CYBERSECURITY CAPACITY REVIEW

The Bahamas

March 2022

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

CONTENTS

Document Administration 3
List of Abbreviations 4
EXECUTIVE SUMMARY 5

INTRODUCTION 14

Dimensions of Cybersecurity Capacity 15
Stages of Cybersecurity Capacity Maturity 17

CYBERSECURITY CONTEXT IN THE BAHAMAS 18

REVIEW REPORT 20

Overview....20

DIMENSION 1 CYBERSECURITY STRATEGY AND POLICY 21

D 1.1 National Cybersecurity Strategy 22
D 1.2 Incident Response and Crisis Management 24
D 1.3 Critical Infrastructure (CI) Protection 24
D 1.4 Cybersecurity in Defence and National Security 27
Recommendations....27

DIMENSION 2 CYBERSECURITY CULTURE AND SOCIETY 32

D 2.1 Cybersecurity Mindset 33
D 2.2 Trust and Confidence in online services 34
D 2.3 User Understanding of Personal Information Protection Online 36
D 2.4 Reporting Mechanisms 37
D 2.5 Media and online platforms....38
Recommendations....38

DIMENSION 3 BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES 32

D 3.1 Building Cybersecurity Awareness 43
D 3.2 Cybersecurity Education 45
D 3.3 cybersecurity Professional Training 47
D 3.4 Cybersecurity Research and Innovation 49
Recommendations....50

DIMENSION 4 LEGAL AND REGULATORY FRAMEWORKS.... 55

D 4.1 Legal and Regulatory Provisions 56
D 4.2 Related Legislative Frameworks..60
D 4.3 Legal and Regulatory Capability and Capacity 62
D 4.4 Formal and Informal Cooperation Frameworks to Combat Cybercrime 64
Recommendations...65

DIMENSION 5 STANDARDS AND TECHNOLOGIES.. 68

D 5.1 Adherence to Standards..69
D 5.2 Security Controls 70
D 5.3 Software Quality 71
D 5.4 Communications and Internet Infrastructure Resilience...72
D 5.5 Cybersecurity Marketplace 73
D 5.6 Responsible Disclosure..74
Recommendations...75
Additional Reflections 78

APPENDICES 79

Methodology - Measuring Maturity..79

DOCUMENT ADMINISTRATION

Lead researchers: Dr Louise Axon, Dr Eva Nagyfejeo

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Dr Jamie Saunders, Professor Federico Varese, Professor Basie Von Solms

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*21/12/2021*	*First draft submitted to Technical Board*
2	*19/01/2022*	*Second draft submitted to Digital Transformation Unit (DTU)*
3	*21/03/2022*	*Comments on draft received from DTU*
4	*29/03/2022*	*Final draft submitted to International Telecommunication Union (ITU) for proofreading*

LIST OF ABBREVIATIONS

CI	Critical Infrastructure
CIRT	Computer Incident Response Team
CMM	Cybersecurity Capacity Maturity Model for Nations
CRDI	Cybersecurity Research, Development and Innovation
CSCF	Customer Security Controls Framework (SWIFT)
CSF	Cyber Security Framework (NIST)
DTU	Digital Transformation Unit
FCDO	Foreign, Commonwealth and Development Office
FIRST	Forum of Incident Response and Security Teams
GCSCC	Global Cyber Security Capacity Centre
HIPAA	Health Insurance Portability and Accountability Act
IDB	Inter-American Development Bank
ITU	International Telecommunication Union
MLAT	Mutual Legal Assistance Treaty
NCEP	National Cybersecurity Education Programme
NCS	National Cybersecurity Strategy
NIST	National Institute of Standards and Technology
OAS	Organisation of American States
RBPF	Royal Bahamas Police Force
SWIFT	Society for Worldwide Interbank Financial Telecommunications
UB	University of The Bahamas
UN	United Nations
URCA	Utilities Regulation and Competition Authority

EXECUTIVE SUMMARY

In collaboration with the International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in The Bahamas at the invitation of the Digital Transformation Unit (DTU). The objective of this review was to enable The Bahamas to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity capacities.

Over the period October-December 2021, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies, and the banking sector as well as international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cybersecurity Culture and Society*
- *Building Cybersecurity Knowledge and Capabilities*
- *Legal and Regulatory Frameworks*
- *Standards and Technologies*

Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in The Bahamas and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

[1] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition," February 2017, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

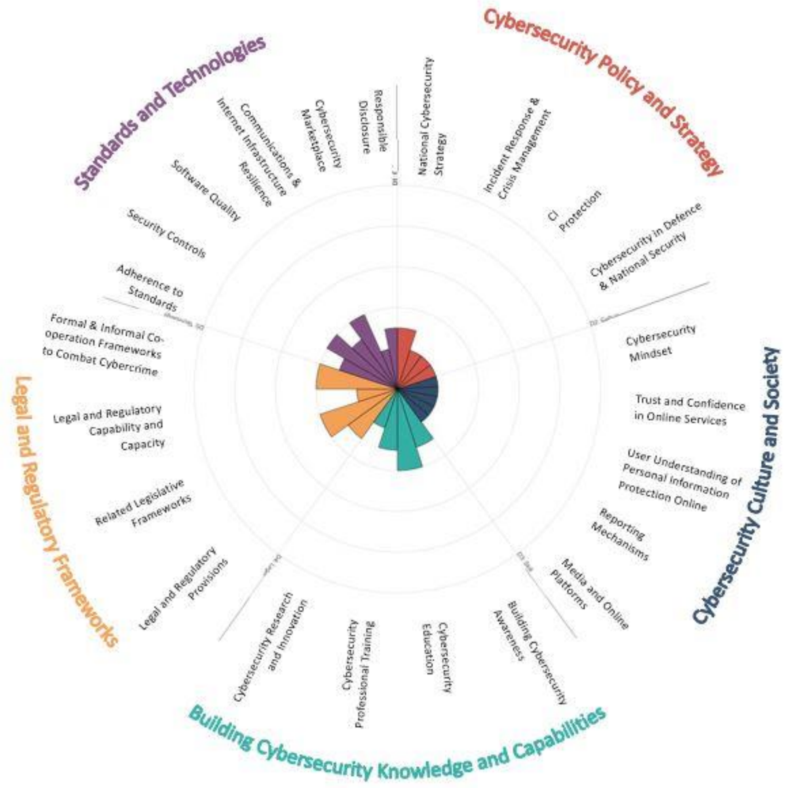


Figure 1: Overall representation of the cybersecurity capacity in The Bahamas

Cybersecurity Policy and Strategy

A national cybersecurity strategy (NCS) for The Bahamas has not yet been published. During the CMM assessment period, the Bahamas was in the process of developing its NCS, with the support of the International Telecommunication Union (ITU). Consultations with key stakeholders from the private and public sector, academia, telecommunications and ICT sector, financial sector, and other infrastructure operators took place in the fourth quarter of 2021 as part of the NCS development. A draft NCS was articulated and approved in early 2022 and provided to the CMM review team. The development of the NCS is part of the Bahamas National Cybersecurity Project ("Government Digital Transformation to Strengthen Competitiveness") led by the Digital Transformation Unit (DTU), which began in January 2021[2].

No overarching national cybersecurity implementation programme has yet been developed. An Action Plan for the 2022 NCS is planned to be drafted; this is a specified objective of the ongoing Bahamas National Cybersecurity Project, and the intention to develop an Action Plan is also referenced in the 2022 NCS draft.

In The Bahamas, there is no process for identifying and categorising national-level cybersecurity incidents, however, this is under development with the creation of the new national Computer Incident Response Team (CIRT). As such, there is no central registry of

[2] https://cybilportal.org/projects/bahamas-national-cybersecurity-project/

cybersecurity incidents in place. The country is in the process of establishing a national CIRT as part of the Bahamas National Cybersecurity Project. The project aim is to perform all necessary capacity building and service upgrades to activate the national CIRT. A CIRT Readiness Assessment has been carried out with the support of the ITU, and a detailed plan is in place for establishing the CIRT.

Since the national CIRT is not yet operational, coordination of incident response within organisations with the national CIRT has not yet been established or tested. While there are mechanisms in place to deal with a range of national crisis scenarios such as hurricanes[3], it is not clear what role they would play (if any) in the event of a significant cyber-related crisis.

The CI has not been formally identified, although it was reported that there is an informal understanding of which sectors form the CI, and this allowed invitation of the CI to this review as well as to the recent consultations for the development of the NCS. Reportedly, one of the objectives of the currently developing CIRT and NCS will be to identify the CI and to provide a level of cybersecurity support for them.

There are no existing regulatory requirements specific to the cybersecurity of the CI in general. There is no baseline of cybersecurity standards to govern CI assets, there is no governance of incident and vulnerability disclosure, and there are no formal processes in place to evaluate CI operator compliance with regulatory standards. Currently, there is some informal collaboration within and between CI sectors.

The Bahamas does not have a standalone cyber-defence strategy; however, a strategy is currently under development. Discussions on the potential impact of cybersecurity on national security and defence have started as part of the Bahamas National Cybersecurity Project. Reportedly, the intention is that a cyber-defence strategy will be an output of the project alongside the new NCS. Specialist cybersecurity capability within the national security establishment is limited.

Cybersecurity Culture and Society

Overall, the cyber-ecosystem in The Bahamas is still in its early stages. The review found that cybersecurity has not yet become a priority across the public and private sectors or among end-users. Some participants indicated that concern about cybersecurity risks is low because people often consider that it is the IT providers' job to protect, not the responsibility of the user.

With regards to small and medium-sized enterprises (SMEs), the review confirmed that there is some level of awareness of cybersecurity risks since they know that in order to be successful SMEs need an online presence (e.g., using emails and social media). However, SMEs often lack the resources to protect themselves properly online.

Large corporations usually have the resources available to protect themselves from most general cyber-attacks. However, they need comprehensive guidelines and cybersecurity

[3] National Emergency Management Agency (NEMA), https://www.bahamas.gov.bs/wps/portal/public/About%20NEMA/The%20National%20Emergency%20Management%20Agency/

policies on what the industry and government requires of them in order to be compliant both locally and internationally (e.g., privacy requirements like GDPR).

The general level of cybersecurity awareness within government agencies remains low. However, more government employees have started reporting illegitimate-looking emails.

A limited proportion of Internet users critically assess what they see or receive online in Bahamas. Based on the review, a very limited proportion believe that they have the ability to use the Internet and protect themselves online.

The government has begun to build a core set of e-services, for which they recognise the need to apply more rigorous security measures in order to establish trust in their use. The Bahamas e-Government Portal Services is a government initiative aimed at making doing business with government easier by providing online access to a range of services.[4] Participants confirmed that various ministries and multiple agencies are planning to put their services online and have at least 200 e-government services operating by April 2025. Based on desk research, e-commerce is becoming increasingly important in The Bahamas.[5] Shopping portals such as eBay and Amazon are regularly accessed by customers where they can use locally issued credit cards to make purchases.[6]

The Office of the Data Protection Commissioner is the national data protection authority of Bahamas with responsibility for the protection of personal data online.[7] Unfortunately, private companies can freely collect and use personal data for their own purposes with no consideration to data protection and privacy. Therefore, there is a need to develop legislation and guidelines at the national level in order to ensure the safety of the clients' personal data used by private entities.

There are no official channels in The Bahamas for users to report computer-related or online incidents.

Cybersecurity issues are reported in an ad-hoc manner by the media in The Bahamas, with insufficient coverage in mass media both online and offline. Participants indicated that there are usually articles within local daily newspapers that cover information about cybersecurity or report on issues such as security breaches or cybercrime.

Building Cybersecurity Knowledge and Capabilities

There is no overarching national cybersecurity awareness-raising programme, coordinating the efforts of relevant stakeholders. Greater national-level coordination of cybersecurity awareness-raising efforts within the country is under development as part of the development of the National Cybersecurity Strategy (NCS). There are indications that various stakeholders in the country realise they can play a role in cybersecurity awareness-raising: it was reported

[4] Government of The Bahamas, E-services, https://www.bahamas.gov.bs/wps/portal/public/gov/government/eServices/eservices/eservices/

[5] U.S. Department of Commerce, International Trade Administration, Bahamas - Country Commercial Guide, eCommerce, https://www.trade.gov/country-commercial-guides/bahamas-ecommerce

[6] Ibid.

[7] Office of the Data Protection Commissioner, https://www.bahamas.gov.bs/wps/portal/public/About%20Us/

that a limited number of cybersecurity-awareness webinars and seminars have been run free for the general public, with the involvement of representatives from government, the private sector, regulators and civil society.

The Get Safe Online Bahamas project provides cybersecurity awareness-raising for personal and business contexts, and has been running in The Bahamas for the past four years. A Cybersecurity Ambassadors programme is run as part of this project. The project portal is the primary site for cybersecurity awareness in the Bahamas, with high levels of interaction from Bahamians.

In terms of awareness-raising by the media, it was reported that articles appear in local newspapers following major cybersecurity incidents. This may help to raise awareness but is currently reactionary. Some proactive awareness-raising news releases are made, for example by the Office of the Data Protection Commissioner, and some insurance companies and banks reportedly run cybersecurity awareness-raising advertisements on the radio. Participants were not aware of any awareness-raising initiatives aimed specifically at executives, although some organisations may conduct such initiatives internally.

No specialised degrees in cybersecurity are currently offered and accredited at university level by a Bahamian institution. Certain courses at the University of The Bahamas (UB) currently include a security-related short module, which reportedly has a high level of uptake and has recently been oversubscribed, indicating demand for cybersecurity education. While no specialised cybersecurity degrees are offered currently, UB have developed a fully accredited Bachelors degree in Cybersecurity and Information Assurance, which is soon to be offered. There was no evidence of cybersecurity offerings in the curriculum at primary- or secondary-school level, and participants were not aware of any such offerings. In 2019, the DTU was commissioned to develop a cybersecurity programme for high-school students and find educators to deliver it; however, this was halted by the COVID-19 pandemic. There was recognition from participants of the need to continue this discussion.

There is some alignment developing between educational offerings and the new NCS, which is currently being drafted: academic stakeholders reported being involved in the recent NCS-development discussions, with a specific meeting having been held on education. A national budget focused on cybersecurity education is not yet established; resources are put towards cybersecurity education, for example by UB, without national-level coordination.

Some private firms offer cybersecurity-training courses online and in-person in The Bahamas. Stakeholders noted that opportunities are readily available to undertake cybersecurity professional training in local training centres, and via regional and international offerings. It was reported that there is uptake of the training courses, but fewer people are taking the examinations to become certified.

There has not yet been an effort to analyse the need for cybersecurity professionals at the national level, or to measure the supply and demand for cybersecurity training courses, and statistical data relative to cybersecurity skills in The Bahamas has not been collected. It was reported by those stakeholders responsible for the development of the NCS that this is a planned objective of the strategy. While the supply and demand for cybersecurity professionals has not been measured, a number of stakeholders noted challenges observed in the availability of, and opportunities for, local cybersecurity professionals.

There is currently no, or only very limited, cybersecurity research and development (R&D) activity taking place in The Bahamas. Participants in the review sessions were not aware of any such activity, but noted that some cybersecurity R&D activity may be carried out by private companies. No doctoral-level students are researching cybersecurity topics yet. As such, research outputs are not yet being produced that address cybersecurity issues within the particular context of the country.

Legal and Regulatory Frameworks

The Computer Misuse Act (2003) is the only legislation in The Bahamas that directly addresses cybercrime.[8] With regards to procedural cybercrime legislation, the Criminal Procedure Code is the main general framework that applies to all cybercrime related investigations.[9] There are limited cybersecurity requirements set out in regulation or law. The need to create legal and regulatory frameworks on cybersecurity have been recognised by participants.

The Data Protection (and Privacy) Act was endorsed in 2003 that includes provisions on privacy, data protection, data subject rights, enforcement, and penalties.[10] The protection of children online, is covered in the Sexual Offences and Domestic Violence Act (2010) that contains provisions on child pornography transmitted by electronic means. With regards to consumer protection, the Consumer Protection Act was passed by the Parliament in 2006.[11] The legislation provides consumers a forum to have their complaints addressed on a timely basis.[12]

Law enforcement officers lack sufficient capacity to prevent and combat cybercrime in The Bahamas. In 2010, a dedicated cybercrime unit (8 people) was created under the Criminal Investigations Department of the Royal Bahamas Police Force (RBPF) and trained by U.S. federal law enforcement agencies.[13] [14]

Law enforcement officers receive ad-hoc training on cybercrime and digital evidence provided by the U.S. State Department, U.S. Department of Defence, INTERPOL[15] and OAS. Participants

[8] Computer Misuse Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

[9] Criminal Procedure Code (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1968/1968-0038/CriminalProcedureCodeAct_1.pdf

[10] Data Protection (and Privacy) Act (2003) http://www.lexbahamas.com/Data Protection 2003.pdf

[11] Consumer Protection Act (2006) http://extwprlegs1.fao.org/docs/pdf/bha78749.pdf

[12] The Government of The Bahamas, Consumer Protection Information and Complaints, https://www.bahamas.gov.bs/wps/portal/public/Consumers/

[13] The Bahamas Police Force, https://www.royalbahamaspolice.org/aboutus/index.php?aboutus_id=1

[14] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

[15] INTERPOL (2016) INTERPOL boosts cybercrime policing capacity in Latin America and the Caribbean, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2016/INTERPOL-boosts-cybercrime-policing-capacity-in-Latin-America-and-the-Caribbean

expressed concern that the trainings lack consistency and are not sufficiently advanced to deal with emerging threats. There is no local institution or consistent programme of specialised training for law enforcement officers, prosecutors or judges in The Bahamas. The Bahamas Bar Association does not offer specialised training on cybercrime in the country. However, there are some opportunities for specialised training abroad (e.g., in the U.S.). In 2021, the Council of Europe, through its Octopus Project, offered a series of EU funded online cybercrime trainings for the Caribbean countries including The Bahamas.[16]

The authorities in The Bahamas have recognised the need to improve both formal and informal cooperation mechanisms, domestically and across borders, but these mechanisms remain ad hoc. Participants described the operational cooperation and exchange of information between the government and criminal justice actors (police, prosecutors and judiciary) as adequate.

There is ad-hoc co-operation between Internet service and other technology providers and law enforcement. The police first has to obtain a court order or a warrant in order to access information from internet service providers (ISPs). A participant described the challenges of cooperating with foreign ISPs such as Facebook.

The existing provisions under the Mutual Legal Assistance Act (2002) facilitates international assistance in criminal matters and criminal investigations between The Bahamas and foreign states.[17] Currently, The Bahamas has mutual legal assistance treaties (MLATs) only with the U.S., Canada and the UK.

Standards and Technologies

No national baselines for the implementation of cybersecurity standards, standards in procurement (from a cybersecurity perspective), or standards for provision of products and services (from a cybersecurity perspective) exist in The Bahamas. In some industries, some organisations may follow certain cybersecurity standards and best practices, but this is not overseen or mandated.

The Finance sector is relatively advanced in this area, as is broadly the case around the world: while adherence to standards is not mandated, it is promoted and expected by the Central Bank, who provide an operational risks guideline that includes compliance with international cybersecurity standards. In summary, the implementation of cybersecurity-related standards is ad-hoc, and there has as yet been no concerted endeavour on a national level to change existing practice in a measurable way. The owners of the current NCS development noted that part of the strategy will focus on regulation of the CI in regard to cybersecurity.

Since there is no national baseline of cybersecurity standards, and application of standards by organisations is ad-hoc and relatively limited, there is significant variation in the application of security controls, both technological and cryptographic, by organisations. Organisations in

[16] Council of Europe (2021) Octopus Project Activities: CARICOM IMPACS and Octopus Project: EU funded online cybercrime trainings for the Caribbean, https://www.coe.int/en/web/cybercrime/-/caricom-impacs-and-octopus-project-eu-funded-online-cybercrime-trainings-for-the-caribbean

[17] BAHAMAS. Mutual Legal Assistance (Criminal Matters) (2002) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1988/1988-0002/MutualLegalAssistanceCriminalMattersAct_1.pdf

some industries, including Finance, Telecommunications, Utilities and Healthcare, reported applying various technological and procedural cybersecurity controls. However, participants felt that there is a lack of focus on administering cybersecurity controls by many organisations in The Bahamas; a key reason for this is that many organisations have no or very limited staff in cybersecurity roles.

Software quality and functional requirements are identified in some sectors, but not in a strategic manner. No catalogue of assured software platforms and applications exists within the public or private sectors. There is currently no support or guidance from the government for organisations on procuring or maintaining secure software. Some organisations, for example in the Finance and Healthcare sectors, reported having policies and processes in place for assessing software quality and monitoring its lifecycle.

Internet services are widely available and used in The Bahamas. There are two ISPs operating in the Bahamas and three submarine Internet cables, offering some redundancy. Representatives from the ISPs described measures taken to increase redundancy (running servers on other islands) and protect downstream users from security risks (e.g., network-security monitoring). It was noted that the level of security risk-management may not be consistent across ISPs, and some concerns were expressed by participants about the reliability of these Internet services from a consumer perspective. Participants felt that there is a need for more consistent redundancy and security across ISPs in The Bahamas, to prevent issues for downstream services.

Most cybersecurity technologies are developed outside The Bahamas; participants were not aware of any such technologies developed locally. There is therefore a high level of dependence on foreign cybersecurity technologies. There was no evidence that the implications of this dependence had been considered systematically, and doing so will be important to ensure that associated risks are identified and mitigated.

There are a limited number of local cybersecurity consultancy services available in the country, and cybersecurity consultancy services are also available internationally. It was reported that due to proximity to nations such as the US, and also due to globalisation broadly, there is sufficient access to cybersecurity consultancy firms by organisations in The Bahamas. Some participants noted that a stronger local offering might be beneficial to prevent outsourcing risks and reap the economic and skills benefits of a local market.

No evidence was provided of risk assessments conducted by organisations to determine how to mitigate the risks of outsourcing IT to a third party or cloud provider, although it is likely that this takes place in some organisations from sectors more advanced in terms of cybersecurity, such as Finance. Cyber-insurance is available to companies in The Bahamas via international providers that are brokered locally. Some organisations, for example in the Telecommunications sector, reported having purchased cyber-insurance.

There are no formal information-sharing mechanisms or channels in place locally for stakeholders to share technical details of vulnerabilities. Some organisations, such as in the Finance sector, participate in regional and international information-sharing groups. No evidence was provided of informal sharing of information on vulnerabilities, although it is likely that some occurs on an ad-hoc basis. Participants from the CI expressed the view that improved information-sharing within and between sectors would be highly beneficial, to improve the awareness of current threats to specific industries and in general, and of vulnerabilities in technologies. Most public and private sector organisations do not yet have responsible-disclosure policies guiding the processes they follow to receive and disseminate vulnerability information responsibly.

INTRODUCTION

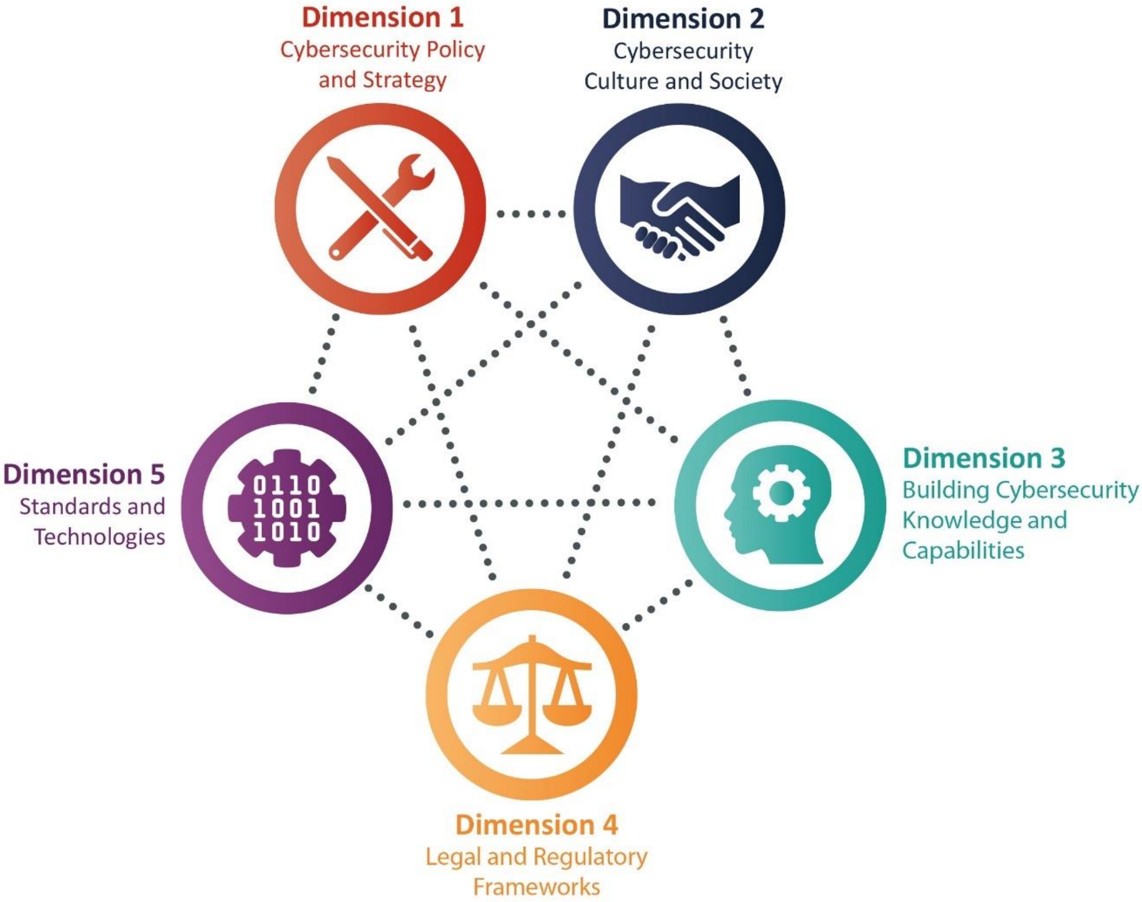
At the invitation of the Digital Transformation Unit (DTU) and in collaboration with the International Telecommunication Union (ITU), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity of The Bahamas. The objective of this review was to enable The Bahamas to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

Over the period October-December 2021, stakeholders from the following sectors participated in a three-day consultation process:

- Public-sector entities:
    - Digital Transformation Unit (DTU)
    - Office of the Data Protection Commissioner
    - Royal Bahamas Police Force, including Cybercrime Unit
    - Defence Force
    - Office of the Attorney General
    - Ministry of National Security
- Universities
- Telecommunications and Internet service providers
- Operators of Critical Infrastructures (CI) (Finance sector, Utilities sector)
- Central Bank
- Insurance providers
- IT consultancy firms
- Software-development firms
- Organisation of American States (OAS)

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were based around the GCSCC Cybersecurity Capacity Maturity Model (CMM)[18] which is composed of five distinct *dimensions* of cybersecurity capacity.


Dimension 1
Cybersecurity Policy and Strategy
Dimension 2
Cybersecurity Culture and Society
Dimension 5
Standards and Technologies
0110
1001
1010
Dimension 3
Building Cybersecurity Knowledge and Capabilities
Dimension 4
Legal and Regulatory Frameworks

[18] Global Cybersecurity Capacity Centre, "Cybersecurity Capacity Maturity Model for Nations (CMM), 2021 Edition," March 2021, https://gcscc.ox.ac.uk/the-cmm#/.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions together with the factors which each presents:

DIMENSIONS	**FACTORS**
Dimension 1 **Cybersecurity Policy and Strategy**	D1.1 Strategy Development D1.2 Incident Response and Crisis Management D1.3 Critical Infrastructure (CI) Protection D1.4 Cybersecurity in Defence and National Security
Dimension 2 **Cybersecurity Culture and Society**	D2.1 Cybersecurity Mindset D2.2 Trust and Confidence in Online Services D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Online Platforms
Dimension 3 **Building Cybersecurity Knowledge and Capabilities**	D3.1 Building Cybersecurity Awareness D3.2 Cybersecurity Education D3.3 Cybersecurity Professional Training D3.4 Cybersecurity Research and Innovation
Dimension 4 **Legal and Regulatory Frameworks**	D4.1 Legal and Regulatory Provisions D4.2 Related Legislative Frameworks D4.3 Legal and Regulatory Capability and Capacity D4.4. Formal and Informal Co-operation Frameworks to Combat Cybercrime
Dimension 5 **Standards and Technologies**	D5.1 Adherence to Standards D5.2 Security Controls D5.3 Software Quality D5.4 Communications and Internet Infrastructure Resilience D5.5 Cybersecurity Marketplace D5.6 Responsible Disclosure

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension contains a number of *factors* which describe what it means to possess cybersecurity capacity. Each factor presents a number of *aspects* grouping together related *indicators*, which describe steps and actions that, once observed, define the stage of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **start-up:** at this Stage, either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There may be an absence of observable evidence at this Stage;

- **formative:** some features of the Aspect have begun to grow and be formulated, but may be ad hoc, disorganised, poorly defined or simply new. However, evidence of this activity can be clearly demonstrated;

- **established:** the Indicators of the Aspect are in place, and evidence shows that they are working. There is not, however, well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in the various elements of the Aspect. But the Aspect is functional and defined;

- **strategic:** choices have been made about which parts of the Aspect are important, and which are less important for the particular organisation or nation. The strategic Stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances; and

- **dynamic:** at this Stage, there are clear mechanisms in place to alter national strategy depending on the prevailing circumstances, such as the technology of the threat environment, global conflict, or a significant change in one area of concern (e.g. cybercrime or privacy). There is also evidence of global leadership on cybersecurity issues. Key sectors, at least, have devised methods for changing strategies at any stage during their development. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this Stage.

The assignment of maturity stages is based upon the evidence collected, including the general or consensus view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of The Bahamas and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN THE BAHAMAS

The Bahamas, known officially as The Commonwealth of The Bahamas, is a sovereign island country in the Caribbean region.[19] The Bahamas is home to a population of approximately 398,000.[20]

Internet penetration has been rising in the Bahamas throughout recent years. In January 2021, there were 335,800 Internet users, an Internet penetration rate of 85%, which was a 0.9% increase since 2020.[21] Similarly, the number of social media users in 2021 was 260,000, a penetration rate of 65.8%, which was a 4% increase since 2020. There were 333,800 mobile connections in 2021 (84.5% penetration), a 4.9% decrease since 2020.

The Inter-American Development Bank (IDB) is currently providing technical and financial support to streamline government procedures and make them available online; increase use of IT in the public sector; increasing transparency of government activities and strengthening auditing and control mechanisms[22]. This is being carried out through a loan operation titled Government Digital Transformation to Strengthen Competitiveness, approved in 2018.

The Bahamas took part in the ITU's Global Cybersecurity Index 2020 (GCI Fourth Edition), and based on the information provided the country ranked 147th in the global rankings out of 182 countries that took part, and 24th out of 35 participating countries in the Americas region, with a score of 13.37. This was a lower ranking than in the previous GCI edition, largely due to the absence of regulations, a National Cybersecurity Strategy (NCS), or a Computer Incident Response Team (CIRT). The GCI report highlights "Legal Measures" as an area of relative strength, while Technical, Organizational, Cooperative Measures and Capacity Development are all areas for potential growth. The gaps noted in this study have been used as drivers for recent cybersecurity projects.

In 2020 The Bahamas took part in the Cybersecurity Regional Study for Latin America and the Caribbean by the IDB and Organisation of American States (OAS).[23] The maturity scores given according to the CMM were Start-Up or Formative for most Factors, with relatively higher maturity in Dimension 4: Legal and Regulatory Frameworks.

[19] Michigan State University, Bahamas: Introduction, https://globaledge.msu.edu/countries/bahamas

[20] World Population Review, The Bahamas Population 2021, https://worldpopulationreview.com/countries/bahamas-population

[21] Datareportal (2021) Digital 2021: The Bahamas, https://datareportal.com/reports/digital-2021-bahamas

[22] https://www.iadb.org/en/project/BH-L1045

[23] https://publications.iadb.org/publications/english/document/2020-Cybersecurity-Report-Risks-Progress-and-the-Way-Forward-in-Latin-America-and-the-Caribbean.pdf

The country has close proximity to the US geographically, and also in terms of business collaboration and support, particularly since a number of Bahamian companies are subsidiaries of US parent companies. This has an impact in terms of cybersecurity, advancing cybersecurity capacity to some extent. Some cybersecurity practices and policies within local organisations are inherited from, or informed by, US parent companies, or influenced by business relationships. It also impacts on the availability of US offerings of cybersecurity consultancy, managed cybersecurity services, and training courses.

The Bahamas National Cybersecurity Project began in January 2021. This project is led by the Digital Transformation Unit (DTU) and supported by the International Telecommunication Union (ITU). The objectives of the project are to develop a National Cybersecurity Strategy (NCS) and Action Plan; carry out a National Computer Incident Response Team (CIRT) Readiness Assessment as well as all necessary capacity building and service upgrades to activate the national CIRT; and review cybersecurity capacity using the CMM through this review.

The CMM, CIRT establishment, and NCS are expected to be completed by the end of 2022, but the implementation is expected to continue until 2026. The recommendations we make in this report, alongside the other objectives of the project, will help The Bahamas to reach a higher level of cybersecurity capacity maturity over the coming years. It is important to note that, as part of these ongoing projects, there is already progress being made towards some of the recommendations in this report.

REVIEW REPORT

OVERVIEW

This section provides an overall representation of the cybersecurity capacity in The Bahamas. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

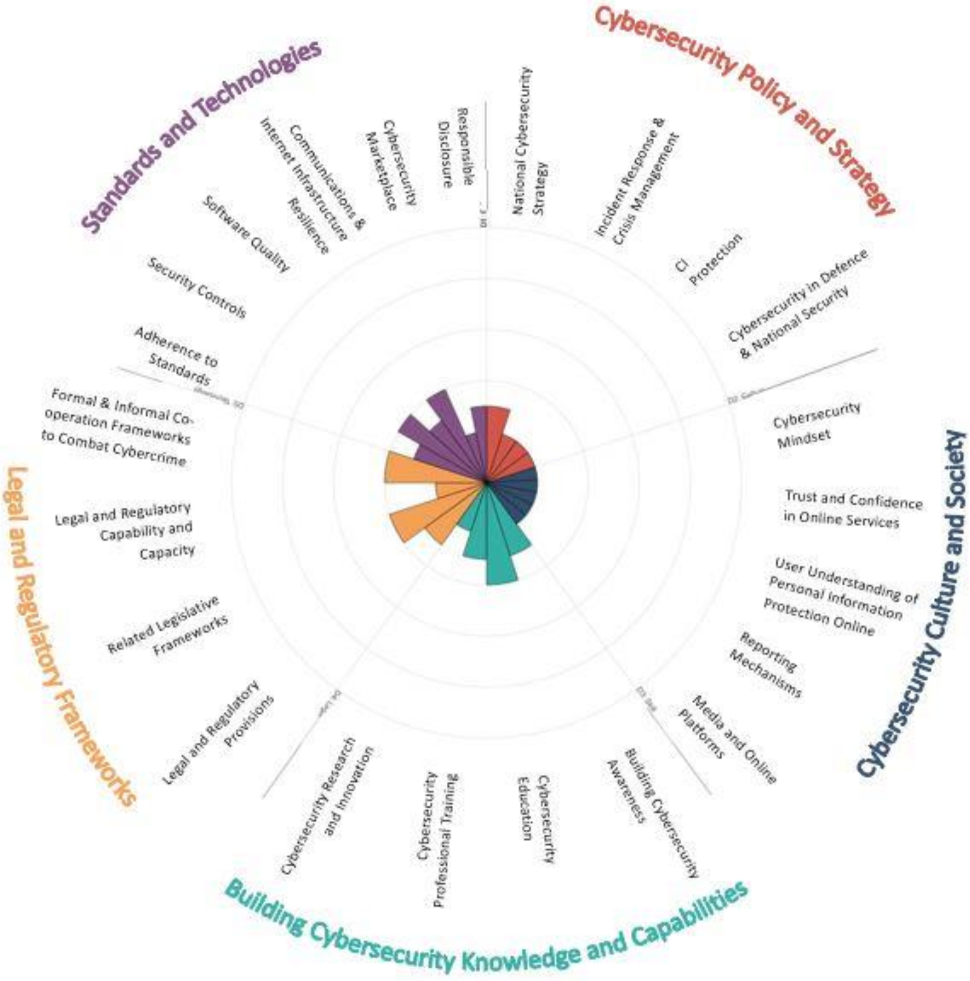
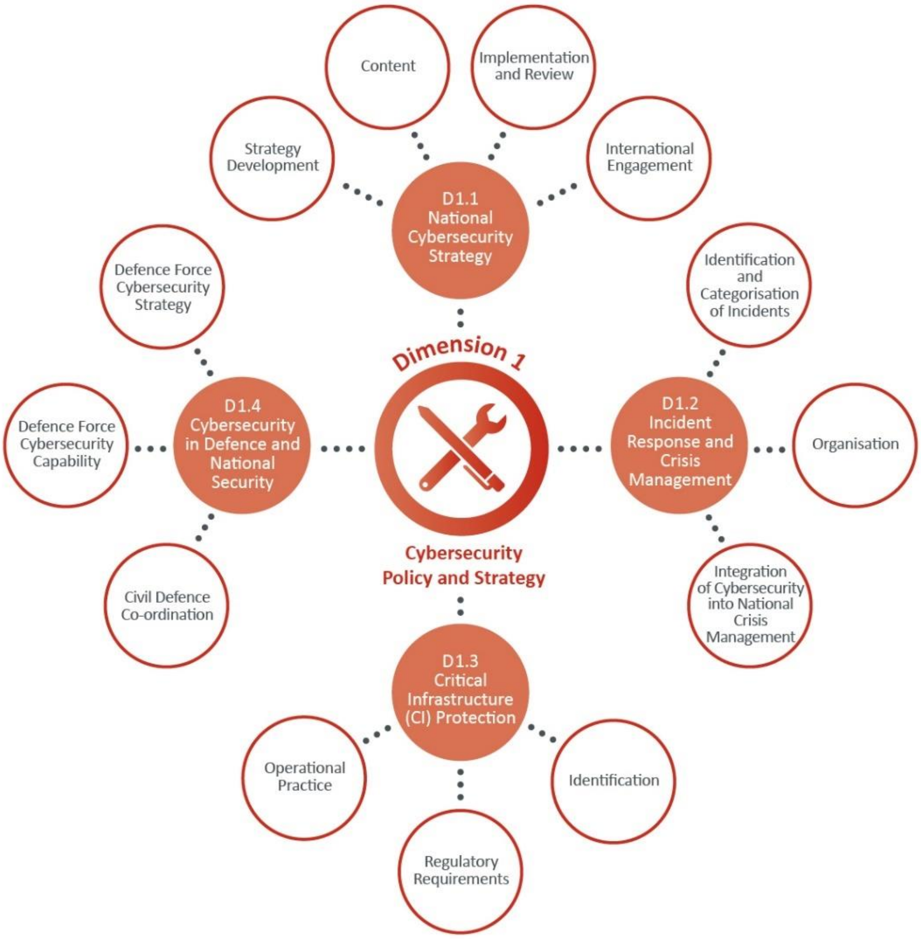


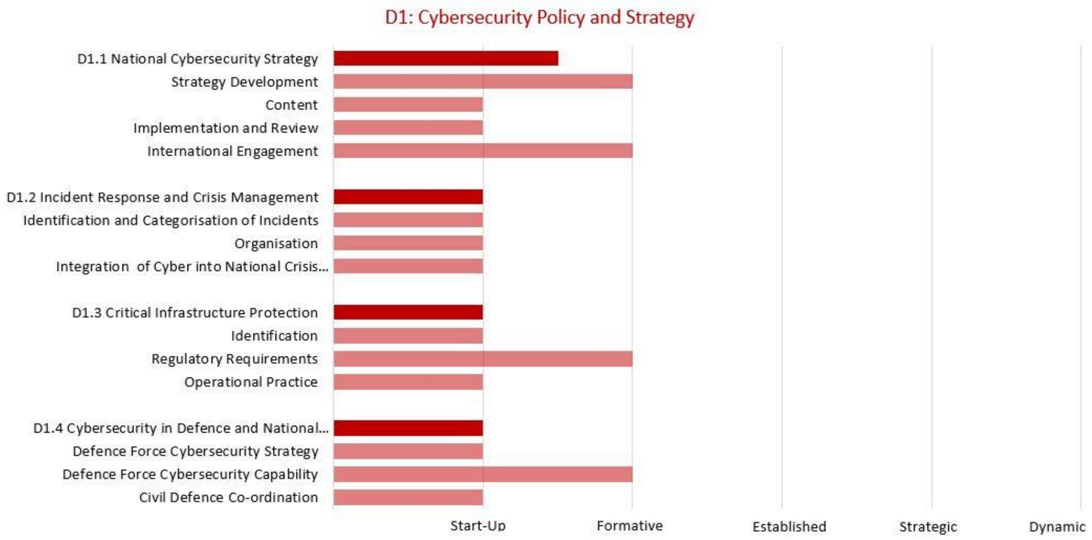
Figure 2: Overall representation of the cybersecurity capacity in The Bahamas

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

This Dimension explores The Bahamas' capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, cyber defence and critical infrastructure protection capacities. This Dimension considers effective strategy and policy in delivering national cybersecurity capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.


Content
Implementation and Review
Strategy Development
International Engagement
D1.1 National Cybersecurity Strategy
Defence Force Cybersecurity Strategy
Identification and Categorisation of Incidents
Dimension 1
D1.4 Cybersecurity in Defence and National Security
D1.2 Incident Response and Crisis Management
Defence Force Cybersecurity Capability
Organisation
Cybersecurity Policy and Strategy
Civil Defence Co-ordination
Integration of Cybersecurity into National Crisis Management
D1.3 Critical Infrastructure (CI) Protection
Operational Practice
Identification
Regulatory Requirements

OVERVIEW OF RESULTS



D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: Start-up to Formative

A national cybersecurity strategy (NCS) for The Bahamas has not yet been published. During the CMM assessment period, the Bahamas was in the process of developing its NCS, with the support of the International Telecommunication Union (ITU). A draft NCS was articulated and approved in early 2022 and provided to the CMM review team.

The development of the NCS is part of The Bahamas National Cybersecurity Project ("Government Digital Transformation to Strengthen Competitiveness") led by the Digital Transformation Unit (DTU), which began in January 2021[24]. The objectives of the project are to develop a National Cybersecurity Strategy and Action Plan; carry out a National Computer Incident Response Team (CIRT) Readiness Assessment as well as all necessary capacity building and service upgrades to activate the national CIRT; and review cybersecurity capacity

[24] https://cybilportal.org/projects/bahamas-national-cybersecurity-project/

using the CMM through this review. The project is planned to be completed by the end of 2022, with interim support from the ITU including support to help the CIRT reach maturity.

Consultations with key stakeholder groups from the private and public sector, academia, telecommunications and ICT sector, financial sector, and other infrastructure operators took took place in the fourth quarter of 2021 as part of the NCS development. The new NCS takes as input the findings from these stakeholder consultations, elements of the content of the 2014 NCS draft which was not published[25] (but the new NCS is not based directly on this earlier effort) and the results of this CMM assessment. The Bahamas has not yet conducted a national-level cybersecurity risk assessment, although identification of the threat and risk to national cybersecurity to inform a risk-based approach is a key focus of the new 2022 NCS draft (and was also referenced in the 2014 NCS draft). Such an assessment would help to strengthen the case for investment and enable prioritisation of the actions within the strategy against the country's specific needs.

No overarching national cybersecurity implementation programme has yet been developed. An Action Plan for the 2022 NCS is planned to be drafted; this is a specified objective of the ongoing Bahamas National Cybersecurity Project. The Action Plan is referenced in the 2022 NCS draft, which states that it will contain "specific tasks, their owners and contributors, deadlines and performance metrics for responsible entities". To ensure that the strategic tasks outlined in the NCS are accomplished, it is important that this Action Plan is published, and includes identification of the necessary resources to carry out each action.

The key focus areas of the 2022 NCS draft are: "Cybersecurity governance framework"; "Effective Incident Prevention and Response"; "Protecting critical information infrastructure"; "Cybersecurity awareness and skills"; and "Improving law enforcement capabilities to better fight cybercrime". The NCS draft also identifies objectives and tasks within each of these strategic areas. These objectives and tasks cover many of the areas of focus of the CMM, and provide a strong basis for building the cybersecurity maturity of the country.

The content of NCS draft clearly reflects the country-specific priorities and circumstances: in particular noting that the NCS objectives are guided by the following vision: "The Bahamas is a secure and trusted digital society, benefiting its citizens' daily lives, sustaining economic competitiveness, and recognised as a reliable partner regionally and globally." This provides a strong basis for ensuring that the NCS aligns with national priorities.

The Bahamas benefits from support from international partners including the ITU (who are supporting The Bahamas National Cybersecurity Project, as described) and Organisation of American States (OAS) (who supported the development of the 2014 NCS draft, for example[26]). The Bahamas government is aware of the existence of international discussions on cybersecurity policy and related issues, and the country participates in international discussions related to cybersecurity issues on occasion, for example through cybersecurity events organised by the OAS, UN and IDB. The government also participates in operational bodies such as international information-sharing networks. Participants noted that, as the ongoing National Cybersecurity Project drives a higher level of cybersecurity activity in the country, participation in international debates and operational bodies will increase. For

[25] http://www.thebahamasweekly.com/publish/bis-news-updates/New_Cyber_Security_Strategy_to_strengthen_data_protection_capabilities34602.shtml
[26] https://www.oas.org/en/media_center/press_release.asp?sCodigo=E-173/14

example, it is planned that the new CIRT will be a member of international bodies such as the Forum of Incident Response and Security Teams (FIRST).

One of the objectives of the 2022 NCS draft is to strengthen international cooperation, including participating in cybersecurity fora locally and internationally. This is important to enable The Bahamas to keep up-to-date with international cybersecurity discussions and make an active contribution to international policy debates. It may be beneficial to conduct an assessment of how the international debates on cybersecurity policy and related issues affect the country's interests and international standing, and define specific engagement objectives accordingly.

D 1.2 INCIDENT RESPONSE AND CRISIS MANAGEMENT

This Factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, co-ordinate, and operationalise incident response, and whether cybersecurity has been integrated into the national crisis management framework.

Stage: Start-up

In The Bahamas, there is no process for identifying and categorising national-level cybersecurity incidents, however, this is under development with the creation of the new national Computer Incident Response Team (CIRT). As such, there is no central registry of cybersecurity incidents in place.

The country is in the process of establishing a national CIRT as part of the Bahamas National Cybersecurity Project. The project aims to perform all necessary capacity building and service upgrades to activate the national CIRT. A CIRT Readiness Assessment has been carried out with the support of the ITU, and a detailed plan is in place for establishing the CIRT. This process has not yet been completed and the CIRT is not yet operational but the project is planned to complete by the end of 2022, including the hiring of personnel, implementation of technologies and processes, and training and knowledge transfer for the new CIRT analysts. It will act as a focal point for information-sharing and coordination for both the public and private sector. It is planned that support will be received from the ITU to help the CIRT reach maturity.

Regulatory requirements for cybersecurity are currently limited, and there are no formal requirements for incident-response plans in any sector. Systematic incident-response mechanisms only appear to exist in the Finance and Telecommunications sectors; for example, some banks and ISPs have put in place formal cybersecurity incident-response plans that are scheduled to be tested via tabletop exercises on an annual basis. Incident-response plans include roles and escalation procedures developed using well-recognised international guidelines such as the National Institute of Standards and Technology (NIST) Computer

Security Incident Handling Guide[27]. These organisations also have their own internal incident-response teams.

The Central Bank of The Bahamas promotes incident response within the Finance sector and expects licensees to have been properly developed and tested business-continuity plans, and to report incidents, including cybersecurity incidents, to the bank supervision unit. The Central Bank reported that if a significant cybersecurity incident was not reported to the regulator, this could result in fines. An attestation framework is in place that requires financial organisations interacting with the Bahamas Automated Clearing House (BACH) to have a tested cybersecurity incident-response plan. As a result, incident-response plans are generally in place within the Finance sector.

While the Telecommunications sector regulator - the Utilities Regulation and Competition Authority (URCA)[28] - does not set specific requirements for cybersecurity incident response, its requirements do cover eventualities that imply liability for cybersecurity incidents. For example, if any incident (including a cybersecurity incident) were to lead to a major outage, fines would be imposed. This drives the implementation of incident-response policies in this sector to some extent.

Since the national CIRT is not yet operational, coordination of incident response within organisations with the national CIRT has not yet been established or tested. Similarly, bilateral cooperation of the national incident-response structures with international partners has not yet been tested. Establishing and testing the relevant coordination mechanisms and protocols will be an important activity to include in the development of the CIRT.

While there are mechanisms in place to deal with a range of national crisis scenarios such as hurricanes[29], cybersecurity is not currently part of national crisis management, and it is not clear what role current crisis-management mechanisms would play (if any) in the event of a significant cyber-related crisis. It is also not clear whether the people involved are equipped to deal with such a crisis, and their readiness to do so has not been exercised. It is important that mechanisms for responding to national-level crises resulting from cybersecurity incidents are put in place, given the growing potential for cybersecurity threats to impact the Critical Infrastructure (CI) and cause national crisis scenarios.

An exercise programme that includes cybersecurity-based scenarios has not been organised within The Bahamas yet but there has been participation in some international drills (such as cyber exercises run by Tradewinds). Emergency communication capabilities for cyber disruptions are limited, and their resilience to cyber disruption has not been fully addressed or tested.

[27] https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

[28] Utilities Regulation and Competition Authority, https://www.urcabahamas.bs/wp-content/uploads/2020/12/Disaster-Management-Regulations-for-the-Electronic-Communications-Sector-in-The-Bahamas_Final-07122020.pdf

[29] National Emergency Management Agency (NEMA), https://www.bahamas.gov.bs/wps/portal/public/About%20NEMA/The%20National%20Emergency%20Management%20Agency/

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This Factor studies the government's capacity to identify CI assets, the regulatory requirements specific to the cybersecurity of CI, and the implementation of good cybersecurity practice by CI operators.

Stage: Start-up

The CI has not been formally identified, although it was reported that there is an informal understanding of which sectors form the CI, and this allowed invitation of the CI to this review as well as to the recent consultations for the development of the NCS. Reportedly, one of the objectives of the currently developing CIRT and NCS will be to identify the CI and to provide a level of cybersecurity support for them.

There are no existing regulatory requirements specific to the cybersecurity of the CI in general. There is no baseline of cybersecurity standards to govern CI assets, there is no governance of incident and vulnerability disclosure, and there are no formal processes in place to evaluate CI operator compliance with regulatory standards. Stakeholders involved in the development of the NCS did acknowledge the need for baseline standards to govern CI assets. The preparation of a regulatory framework for identification and protection of CI, including implementation of specified cybersecurity measures, is an objective of the 2022 NCS draft. Participants from the CI expressed the view that guidance on cybersecurity and monitoring of practices would be beneficial, which suggests that this would be received in a positive way.

A few CI operators are implementing good cybersecurity practices and self-assessing against recognised industry standards such as the Heath Insurance Portability and Accountability Act (HIPAA), Society for Worldwide Interbank Financial Telecommunications (SWIFT) Customer Security Controls Framework (CSCF) and NIST Cyber Security Framework (CSF), but in most sectors this is ad-hoc. In the Finance sector, the Central Bank of The Bahamas sets expectations of its licensees in terms of application of cybersecurity standards and incident-response planning. While compliance with cybersecurity standards is not a regulatory requirement, this drives a higher level of cybersecurity in this sector. Furthermore, the Central Bank provides a technology risk-management guideline to financial institutions, which is being updated to reflect additional concerns related to cybersecurity.

Currently, there is some informal collaboration within and between CI sectors. The example of the Healthcare sector was given: participants reported that incidents, particularly those that result in data leakage, may be kept private due to concerns about reputation, and as such there is only minimal sharing of information on threat and risk between relevant stakeholders. Multiple CI stakeholders expressed the view that it would be beneficial to strengthen processes for incident reporting and communications within and between CI sectors.

D 1.4 CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

Stage: Start-up

This Factor explores whether the government has the capacity to design and implement a strategy for cybersecurity within national security and defence. It also reviews the level of cybersecurity capability within the national security and defence establishment, and the collaboration arrangements on cybersecurity between civil and defence entities.

The Bahamas does not have a standalone cyber-defence strategy; however, a strategy is currently under development. Discussions on the potential impact of cybersecurity on national security and defence have started as part of the Bahamas National Cybersecurity Project. Reportedly, the intention is that a cyber-defence strategy will be an output of the project alongside the new NCS.

Specialist cybersecurity capability within the national security establishment is limited. The Royal Bahamas Defence Force has recently created a cyber team, the goal of which is to defend the information infrastructure and networks of the Defence Force. The newly established cyber team will aim to improve the overall risk-management and defences against new and evolving threats, the protection of critical information, effective distribution of information through networks, the development and implementation of network mapping, conducting vulnerability assessments and encourage the adoption of cybersecurity best practices across all of the organisation. In early 2021, introductory trainings were conducted with a U.S. partner - the Florida National Guard - that covered incident-response processes, MITRE ATT&CK Techniques and Capture-the-Flag (CTF) exercises.

There is no collaboration on cybersecurity between civil and defence entities. This leaves open the questions of how the military might support civil authorities in the event of a major national cyber incident, and how the military might manage its own cyber dependencies on civil infrastructure. The respective roles are yet to be defined within the country's crisis management procedures. There is no formal body for information-sharing relating to cyber-threat intelligence.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of The Bahamas. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

Given the early stage of NCS development, a number of aspects of the CMM involving the strategy content and plans for implementation have not yet been finalised by those responsible for the NCS development. This review report is a good opportunity to make recommendations to inform the NCS development in line with the requirements of the CMM model:

R1.1.1 **(High priority)** Publish the NCS 2022, based on the findings from stakeholder consultations; international resources (such as the ITU's NCS guide), aspects of the 2014 NCS draft, and the recommendations from this CMM review.

R1.1.2 Conduct an assessment of country-specific national cybersecurity risk, including specific links to wider national-level economic and political policies and strategies, in order to ensure that strategy content reflects country-specific priorities and circumstances.

R1.1.3 Ensure that the strategy clearly reflects the needs and roles of relevant stakeholders across government, business and civil society.

R1.1.4 **(High priority)** Develop and publish an implementation plan, describing an implementation programme that covers the scope of the strategy. This plan should assign actions within the programme to specific "owners" (relevant stakeholders across government and other sectors), and define budgets for implementing the actions of the strategy.

R1.1.5 **(High priority)** Identify how to put in place the resources required to deliver the actions of the programme. Ensure that budget shortfalls are identified and escalated to the relevant authority.

R1.1.6 **(High priority)** Assign a coordinating body for the national strategy implementation programme, and ensure that this body has sufficient authority to ensure that action "owners" are held to account.

R1.1.7 Define within the strategy key outcomes against which success can be measured.

R1.1.8 Put in place review processes and mechanisms to enable strategy 'owners' to monitor achievement of outcomes, address implementation issues and escalate risks, issues and dependencies to the relevant authorities. Ensure that these processes are adequately funded.

R1.1.9 Ensure that links between the strategy and priorities such as national security, digital strategy and economic development, as well as wider online policy objectives such as child protection, the promotion of Human Rights, the promotion of Equality, Diversity and Inclusion, and managing disinformation, are clearly indicated.

R1.1.10 Include within the strategy actions to raise public and business awareness, mitigate cybercrime, establish incident-response capability, promote public-private partnership, and protect critical infrastructure and the wider economy.

R1.1.11 Ensure that there are processes in place for strategy review and renewal.

R1.1.12 Consider conducting an assessment of how the international debates on cybersecurity policy and related issues affect the country's interests and international standing. Define specific engagement objectives accordingly.

INCIDENT RESPONSE AND CRISIS MANAGEMENT

The below recommendations will help drive the alignment of the currently developing CIRT with the indicators of the CMM:

R1.2.1 **(High priority)** When developing the CIRT, ensure that it has the sufficient resources, skills, documented process and legal authorities required to address the range of cyber incident scenarios they are likely to face. The risk assessment recommended in R1.1.2 should support this.

R1.2.2 Develop and document processes for identifying, categorising and managing national-level incidents. Create a central registry that categorises the identified national-level incidents according to severity, and develop procedures that can be used to allocate resources according to this categorisation.

R1.2.3 The CIRT should publish clear procedures for incident reporting, publicise the range of support services that it can provide, encourage private-sector entities to adopt their own internal incident-management procedures, and document and test protocols for the coordination of incident management between the CIRT and the relevant other elements of the public and private sectors (including the impacted organisations, law enforcement and ISPs).

R1.2.4 Develop and test processes for bilateral cooperation of the CIRT with international counterparts in the case of responding to cross-border incidents. This should include considering how to broaden the CIRT's contacts with international networks of incident responders.

R1.2.5 Ensure that cybersecurity is fully integrated into the national crisis management framework[30] (NEMA), by developing preparedness plans for responding to national-level crises resulting from cybersecurity incidents. Ensure that the organisation responsible for crisis management is equipped to deal with a range of cybersecurity-related scenarios.

R1.2.6 Develop a national crisis-management exercise programme including cybersecurity-based scenarios.

R1.2.7 Identify which emergency communications systems already exist in the country, test their resilience to cyber disruption, and take action to address weaknesses identified.

R1.2.8 Consider increasing active participation in relevant operational collaboration and policy bodies (such as regional and international CERT bodies).

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.3.1 **(High priority)** Specify which organisations are considered "critical infrastructure" and outline the kinds of risks that these organisations face. Ensure that the list is kept up to date to reflect changes in the country's circumstances.

R1.3.2 **(High priority)** Allocate an agency responsible for overseeing the cybersecurity of the CI. This role could be centralised (e.g., through the CIRT) or delegated to individual sector-regulating agencies.

R1.3.3 **(High priority)** Ensure that CI operators are mandated by regulation to meet appropriate cybersecurity standards, and establish processes for evaluating compliance.

R1.3.4 Consider how to strengthen processes for incident-reporting and communications within and between CI sectors. This may include:

- Placing mandatory breach-reporting and vulnerability-disclosure obligations on CI operators.

[30] National Emergency Management Agency (NEMA), https://www.bahamas.gov.bs/wps/portal/public/About%20NEMA/The%20National%20Emergency%20Management%20Agency/

- Establishing and promoting mechanisms for CI operators to share threat and vulnerability information, best practices and lessons learned.

R1.3.5 Put in place mechanisms to ensure that the CI operators are consistently implementing recognised industry standards and the effectiveness of their cybersecurity controls is regularly assessed.

CYBERSECURITY IN DEFENCE AND NATIONAL SECURITY

R1.4.1 **(High priority)** Assess the potential impact of cybersecurity on national security and Defence and develop a strategy for addressing these risks.

R1.4.2 Ensure that the strategy is supported by appropriate legal authorities and relevant operational doctrine and rules of engagement, and that these are consistent with The Bahamas' human rights and other international humanitarian law obligations.

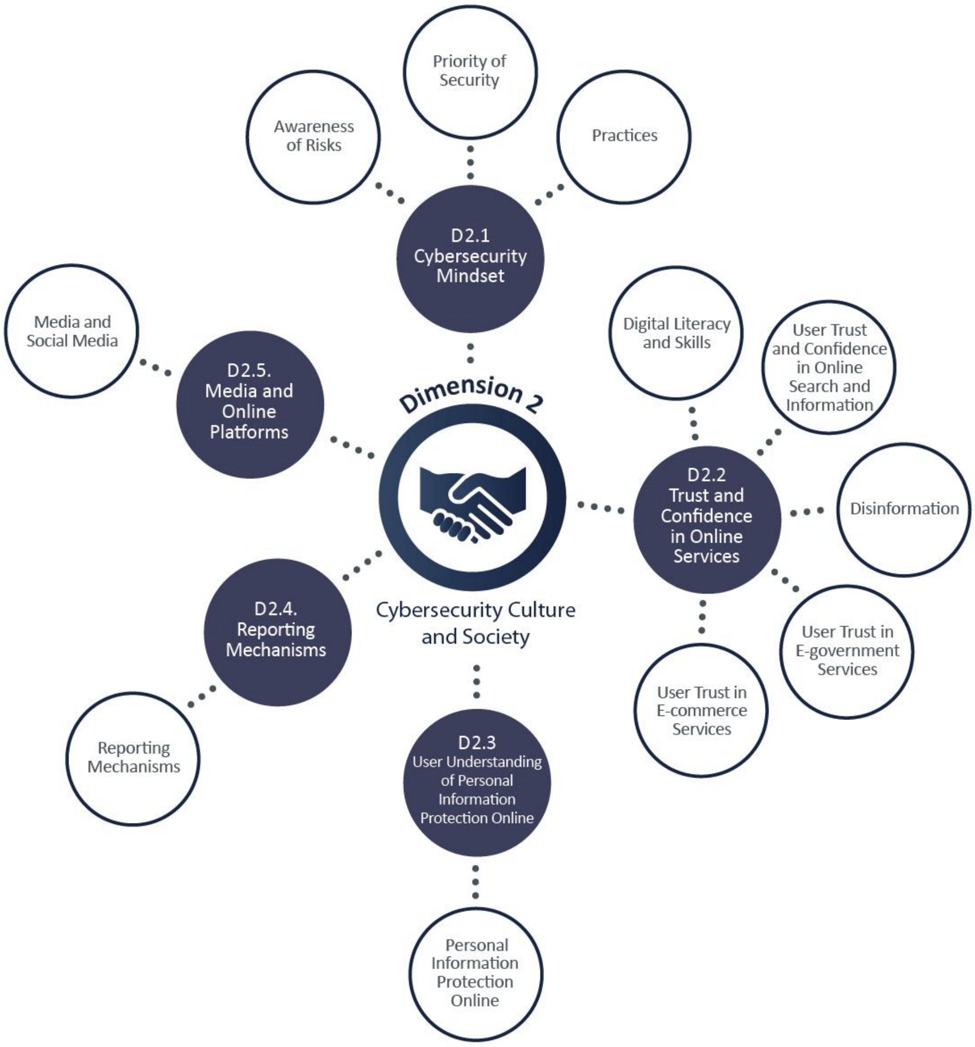
R1.4.3 **(High priority)** Ensure that the resources allocated to the relevant Defence organisations are sufficient to fulfil the outcomes of the strategy.

R1.4.4 Ensure that the role of the national security and defence community in supporting civil authorities in the event of a major national cyber incident, as well as how the military might manage its own cyber dependencies on civil infrastructure, is clear. Test the relevant roles and procedures against plausible cybersecurity crisis scenarios.

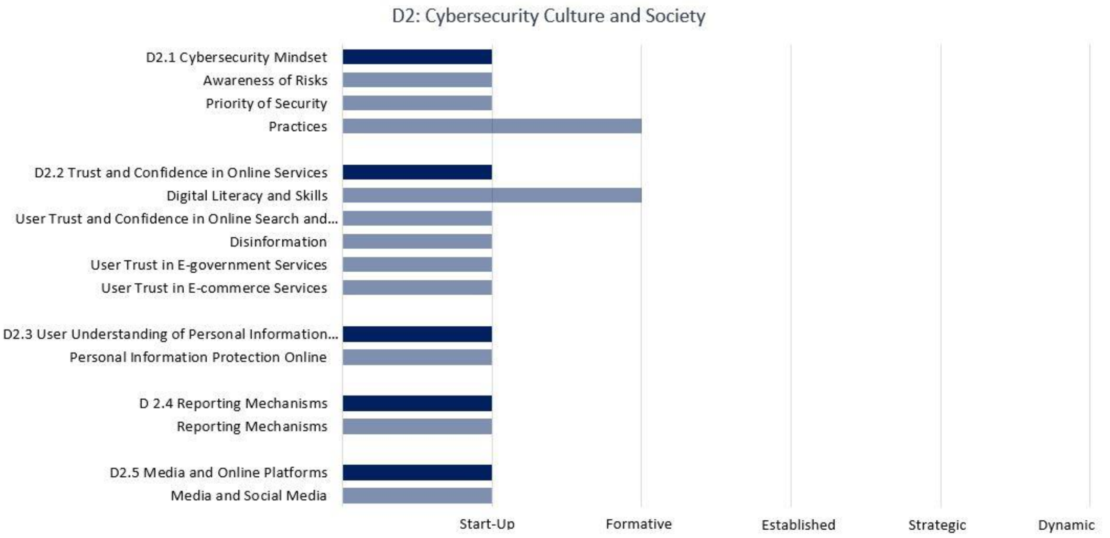
R1.4.5 Establish how the CIRT and the military cyber team can support one another (through liaison between the two entities), and whether there are opportunities to increase efficiency and effectiveness by taking a more integrated approach.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

This dimension reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this Dimension explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this Dimension reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour.


Dimension 2
Cybersecurity Culture and Society
D2.1 Cybersecurity Mindset
Awareness of Risks
Priority of Security
Practices
D2.2 Trust and Confidence in Online Services
Digital Literacy and Skills
User Trust and Confidence in Online Search and Information
Disinformation
User Trust in E-government Services
User Trust in E-commerce Services
D2.3 User Understanding of Personal Information Protection Online
Personal Information Protection Online
D2.4. Reporting Mechanisms
Reporting Mechanisms
D2.5. Media and Online Platforms
Media and Social Media

OVERVIEW OF RESULTS



D 2.1 CYBERSECURITY MINDSET

This Factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society at large. A cybersecurity mindset consists of values, attitudes and practices–including habits of individual users, experts, and other actors–in the cybersecurity ecosystem that increase the capacity of users to protect themselves online.

Stage: Start-up

Overall, the cyber-ecosystem in The Bahamas is still in its early stages. The review found that cybersecurity has not yet become a priority across the public and private sectors or among end-users. Some participants expressed the view that the reason for the minimal recognition of the need to prioritise cybersecurity could be related to many Bahamians perceiving cybersecurity as a fictional problem (e.g., something that happens in the movies) or a problem that occurs only abroad (e.g., in the U.S.). Because of that, citizens may not realise how vulnerable they are and may not take the necessary precautions to protect themselves (e.g., still sharing passwords, not setting the right privacy-protection on social media) and to follow safe cybersecurity practices. This indicates that very few Internet users are following safe cybersecurity practices or taking protective measures to ensure their security. No surveys or metrics exist to document cybersecurity in government, the private sector, or across internet users as a whole.

On a personal level, there is some prominence to a belief that Bahamians would use any means that would give them the least resistance possible to receive the information online.

Some participants indicated that concern about cybersecurity risks is low because people often consider that it is the IT providers' job to protect, not the responsibility of the user. Therefore, it was suggested that there is a need to raise awareness of cybersecurity risks within the public by reminding them of their responsibility in protecting their passwords, not clicking on malicious email subjects and to explain the consequences of their actions. However, there is no capacity to focus on awareness-raising from the government side.

With regards to small and medium-sized enterprises (SMEs), the review confirmed that there is some level of awareness of cybersecurity risks since they know that in order to be successful SMEs need an online presence (e.g., using emails and social media). However, SMEs often lack the resources to protect themselves properly online. Participants acknowledged the need to offer SMEs more resources and help in learning simple practical techniques that they can use in order to protect themselves, either through third parties or themselves.

Large corporations usually have the resources available to protect themselves from most general cyber-attacks. However, they need comprehensive guidelines and cybersecurity policies on what the industry and government requires of them in order to be compliant both locally and internationally (e.g., privacy requirements like GDPR).

The general level of cybersecurity awareness within government agencies remains low. However, more government employees have started reporting illegitimate-looking emails. Especially, government employees working in the finance areas (e.g., finance departments and officers, accountants) are reporting and forwarding suspicious-looking invoices or strange emails suspected to be phishing attempts. Suspicious emails are currently managed by IT Security in the Department of Transformation and Digitization.

D 2.2 TRUST AND CONFIDENCE IN ONLINE SERVICES

This Factor reviews critical skills, the management of disinformation, the level of users' trust and confidence in the use of online services in general, and of e-government and e-commerce services in particular.

Stage: Start-up

A limited proportion of Internet users critically assess what they see or receive online in Bahamas. Based on the review, a very limited proportion believe that they have the ability to use the Internet and protect themselves online. Since June 2021, the Avasant Foundation in collaboration with the Inter – American Development Bank Labs has been piloting the 'Digital Skills and Employment Opportunities for the Displaced Workforce in The Bahamas'.[31] The programme aims to 'develop the digital capabilities of the country's human capital ensuring

[31] Avasant Foundation (2021) Avasant Digital Skills: Re-tooling and Up-skilling – The Bahamas, https://avasant.com/foundation/avasant-digital-skills-re-tooling-and-up-skilling-the-bahamas/

they are adequately equipped with the skills necessary to thrive in the digital age and meet the digital talent requirements of business enterprises.'[32]

Most Internet users exhibit a blind trust in websites and what they see or receive online. Very few Internet users feel confident in using the Internet. However, systematic sample surveys or other metrics to assess users' trust and confidence online are not available.

Participants acknowledged that government agencies and actors have not addressed disinformation online. Whilst others noted that disinformation is managed in a sector specific way (for example, in the banking sector). According to one participant, the root of much of disinformation is anchored in the use of social media. Bahamas is such a small nation that officials do not believe it is possible to modify the behaviours of social-media companies on the basis of their problems.

The government has begun to build a core set of e-services, for which they recognise the need to apply more rigorous security measures in order to establish trust in their use. The Bahamas e-Government Portal Services is a government initiative aimed at making doing business with government easier by providing online access to a range of services.[33] The Inter-American Development Bank is currently providing technical and financial support to make more government services available online through a loan operation titled Government Digital Transformation to Strengthen Competitiveness.[34] The use of digital signatures in e-government and e-commerce services and applications is covered by the Electronic Communications and Transactions Act (2003).[35]

Participants confirmed that various ministries and multiple agencies are planning to put their services online and have at least 200 e-government services operating by April 2025. The objective is to enhance the ease of doing business and to fully digitise the process by having an end-to-end application for a new business or renewal of a business (regardless of business type). One participant advocated the creation of a one-stop shop for government services. As of March 2022, 45 e-government services were delivered to 70,000 registered persons. By the end of 2021, the plan was to be able to process e-government services for children. The review suggested that a relatively high number of people are using them and there is a belief that a growing number of Internet users are developing a greater level of trust in the use of these e-government services. At this stage, there are no surveys or metrics to show the extent Internet users trust e-government services. Also, there was a no information about the levels of e-government security and security breaches.

Based on desk research, e-commerce is becoming increasingly important in The Bahamas.[36] Shopping portals such as eBay and Amazon are regularly accessed by customers where they

[32] Ibid.

[33] Government of The Bahamas, E-services, https://www.bahamas.gov.bs/wps/portal/public/gov/government/eServices/eservices/eservices/

[34] https://www.iadb.org/en/project/BH-L1045

[35] Electronic Communications and Transactions Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf

[36] U.S. Department of Commerce, International Trade Administration, Bahamas - Country Commercial Guide, eCommerce, https://www.trade.gov/country-commercial-guides/bahamas-ecommerce

can use locally issued credit cards to make purchases.[37] Many local companies do not provide online shopping, but more maintain an internet presence through social media pages and a static website.[38] The ongoing COVID-19 pandemic put pressure on many domestic businesses to provide goods and services electronically and to implement systems which allow money and data transfer to carry out these transactions.[39] The Bahamas has implemented the following bills, acts and policies to regulate e-commerce activity in the country: 1) E-Commerce Policy Statement; 2) Electronic Communication and Transaction Bill (2003); Computer Misuse Bill (2003); Data Protection Act (2003); and Unfair Terms in Consumer Contracts Bill (2003).[40] There are no surveys or metrics to show how Internet users trust e-commerce services. It was not clear to what extent private sector recognises the need for the application of security measures to establish trust in e-commerce services.

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

This Factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protecting personal information online, and whether they are sensitive of their privacy rights.

Stage: Start-up

The Office of the Data Protection Commissioner is the national data protection authority of The Bahamas with responsibility for the protection of personal data online.[41] It lists in its missions that it administers and enforces the provisions of the Data Protection Act, promotes the observance of good practice by data controllers within the requirements of the Act, influences thinking on privacy and processing of personal information matters on a local and global basis, discharges various functions relating to or arising from any international obligations.[42] In addition, any Bahamian national who feels that his or her data privacy rights have been infringed upon by any data collector or controller has the opportunity to seek redress by contacting the Data Protection Commissioner and may file a complaint online (or in person, if sensitive).[43]

[37] Ibid.

[38] Ibid.

[39] Ibid.

[40] Ministry of Finance, E-Commerce and The Bahamas Government, https://www.bahamas.gov.bs/wps/portal/public/Government%20Initiatives%20and%20Policies/E-Commerce%20in%20the%20Bahamas/

[41] Office of the Data Protection Commissioner, https://www.bahamas.gov.bs/wps/portal/public/About%20Us/

[42] Office of the Data Protection Commissioner, https://www.bahamas.gov.bs/wps/portal/public/About%20Us/

[43] Government of the Bahamas, Making Data Protection Complaints, https://www.bahamas.gov.bs/wps/portal/public/gov/government/services/

Nevertheless, participants admitted that the protection of personal information online has not been a priority. Unfortunately, private companies can freely collect and use personal data for their own purposes with no consideration to data protection and privacy. Therefore, there is a need to develop legislation and guidelines at the national level in order to ensure the safety of the clients' personal data used by private entities.

Also, participants believed that public awareness of the issues surrounding the protection of personal information and the relationships between privacy and security concerns regarding personal data is low. Mobile internet users are not aware of the kinds of data they share with operators, nor do they know what is done with the information they do provide on popular social media channels such as Facebook or Twitter. Further discussions proposed that the majority of users are too willing to give away personal details, and also remain unaware and not alert to such issues such as the privacy settings they use, or the terms and conditions of the websites.

D 2.4 REPORTING MECHANISMS

This Factor explores the existence of reporting mechanisms that function as channels for users to report Internet-related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Start-up

There are no official reporting mechanisms available in The Bahamas for users to report computer-related or online incidents.

If it is related to privacy, citizens can contact the Data Protection Commissioner and file a complaint online (dataprotection@bahamas.gov.bs) by completing the Privacy Complaint Form.[44] Sometimes, the Data Protection Commissioner collaborates with the Cybercrime Unit of the Royal Bahamas Police Force and with other third parties to investigate and address a complaint. There are instances where direct reporting and complaints are made to the Cybercrime Unit of the Royal Bahamas Police Force and may not get the attention of the Data Protection Commissioner until it is made necessary because feedback is not fast enough. Metrics of reported incidents were not available. Participants acknowledged that users do use social media channels to raise concerns over cyber harms and problems (for example, via Facebook or WhatsApp).

[44] Government of the Bahamas, Making Data Protection Complaints, https://www.bahamas.gov.bs/wps/portal/public/gov/government/services/

D 2.5 MEDIA AND ONLINE PLATFORMS

This Factor explores whether cybersecurity is a common subject of discussion across mainstream media, and an issue for broad discussion on social media. Moreover, this Factor looks at the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up

Cybersecurity issues are reported in an ad-hoc manner by the media in The Bahamas, with insufficient coverage in mass media both online and offline.

Participants indicated that there are usually articles within local daily newspapers that cover information about cybersecurity or report on issues such as security breaches or cybercrime. The articles tend to be reactionary based on a cyber incident that has occurred, but some other news releases seek to raise awareness on cybersecurity and are not related to specific incidents. Some participants noted that they saw cases related to financial fraud where there was an awareness posting specific to this incident. Sometimes banks and companies (e.g., Deloitte) organise conferences and webinars that are free to the public. Some insurance companies and banks run advertisements on the radio (cybersecurity awareness).

Participants further indicated that they believe discussions on social media about cybersecurity are present but only to a very limited extent. There was no information whether whistle-blower protection is provided and if there were any cases of a positive impact of whistle-blower intervention.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *Cybersecurity Culture and Society*. These aim to provide possible next steps to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MINDSET

R2.1.1 **(High priority)** Intensify efforts in leading government agencies to prioritise cybersecurity and enhance efforts at all levels of government to promote understanding of cyber-risks and threats.

R2.1.2 Design coordinated training programmes for employees in the public organisations in cooperation with the private sector. Training should include the following cybersecurity practices:

a) web security (for e.g.: protection of personal information online, social media, social engineering, secure web browsing, malware, passwords)
b) email security (for e.g.: identify a phishing email, sending an email securely)
c) data security (for e.g.: handling and classifying sensitive information, back-up and recovery)
d) mobile device security (for e.g.: portable data storage)
e) remote access security (for e.g.: working from home/while travelling)

R2.1.3 Ensure that risk awareness and secure practices are known also to smaller businesses and adopted by society-at-large.

R2.1.4 In collaboration with NGOs, consider providing the youth social programmes (for e.g.: in schools and universities) that will teach students about safe and responsible behaviour online (for e.g.: the risks of using social media), including how to prevent any uncompromising behaviour.

R2.1.5 Launch a government initiative that assists and provides SMEs with sufficient resources to protect themselves online.

R2.1.6 **(High priority)** Ensure that surveys and metrics are conducted, in order to evaluate the level of cybersecurity knowledge and practice within the nation.

TRUST AND CONFIDENCE IN ONLINE SERVICES

R2.2.1 **(High priority)** Consider improving digital literacy among all demographic groups, including older generations. For example, develop and implement campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content they consume social media or smart-phone applications.

R2.2.2 Promote the implementation of user-consent policies by Internet operators.

R2.2.3 Encourage ISPs to establish programmes that promote trust in their services based on measures of effectiveness of these programmes.

R2.2.4 **(High priority)** Ensure that surveys or other metrics are conducted to assess users’ trust and confidence online.

R2.2.5 Encourage civil society and Internet platform providers to develop approaches to address issues of disinformation.

R2.2.6 Government and/or private entities should consider regularly funding user metrics on trust in e-government services, promoting privacy and security and proactive communication of breaches.

R2.2.7 Encourage the development of e-commerce services with emphasising the need for a security (e.g.: use of encryption, post trust certificates/logos of third-party authentication services on the homepage) in order to establish trust.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.3.1 **(High priority)** Consider implementing broader campaigns in order to improve user practice, and mechanisms to evaluate the current state of user practices. These campaigns should also focus on fostering a public debate about personal information protection online and an adequate balance between security and privacy.

R2.3.2 Encourage a public debate on social media platforms (also in the traditional media) regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.3.3 Develop a Code of Practice on Protecting Personal Information Online in consultation with multiple stakeholders that can be distributed within the public (for e.g.: in primary and secondary schools).

The Code of Practice should include:

a) guidelines regarding Internet safety and the dangers of misuse of personal information online
b) why personal data is important, how it is processed and how can users protect their privacy

REPORTING MECHANISMS

R2.4.1 **(High priority)** Establish coordinated mechanisms within the public and the private sectors that allows citizens to report cybercrime cases, including online fraud, cyber-bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular for women and other vulnerable groups.

R2.4.2 Provide manuals to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it.

R2.4.3 Consider turning the Cybercrime Unit of the Royal Bahamas Police Force into the country's national fraud and cybercrime reporting centre, providing a central point of contact for citizens and businesses.

R2.4.4 Ensure that the Cybercrime Unit has a secure website where victims of cybercrime can report to the police by choosing different options: 1) dialling a number in case it is an emergency or the crime is in progress 2) completing an online form for non-emergency crimes or reporting via social media/email. It is important that all reporting channels should offer the victim the option to report anonymously (for e.g.: anonymous online forms).

MEDIA AND ONLINE PLATFORMS

R2.5.1 **(High priority)** In cooperation with civil society and media organisations develop programmes and campaigns to raise awareness among media providers and leading social media actors, for instance during the dedicated cybersecurity awareness month or dedicated web or social media sites on this topic.

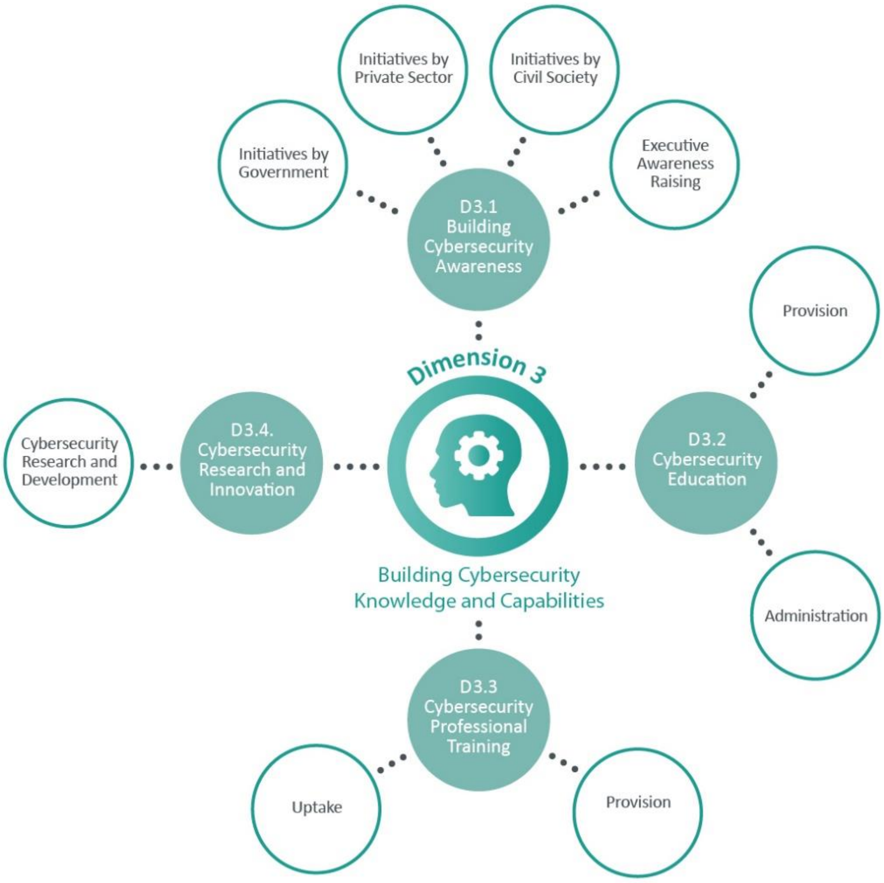
R2.5.2 Enhance the understanding of cybersecurity among media providers (for e.g.: journalists) and facilitate a more active role of media in conveying information about cybersecurity to the public.

R2.5.3 Encourage media content providers to disseminate information on good (proactive) cybersecurity practice that users can pursue to protect themselves or to respond to cyber-incidents. This could stimulate social media discussions on the topic.

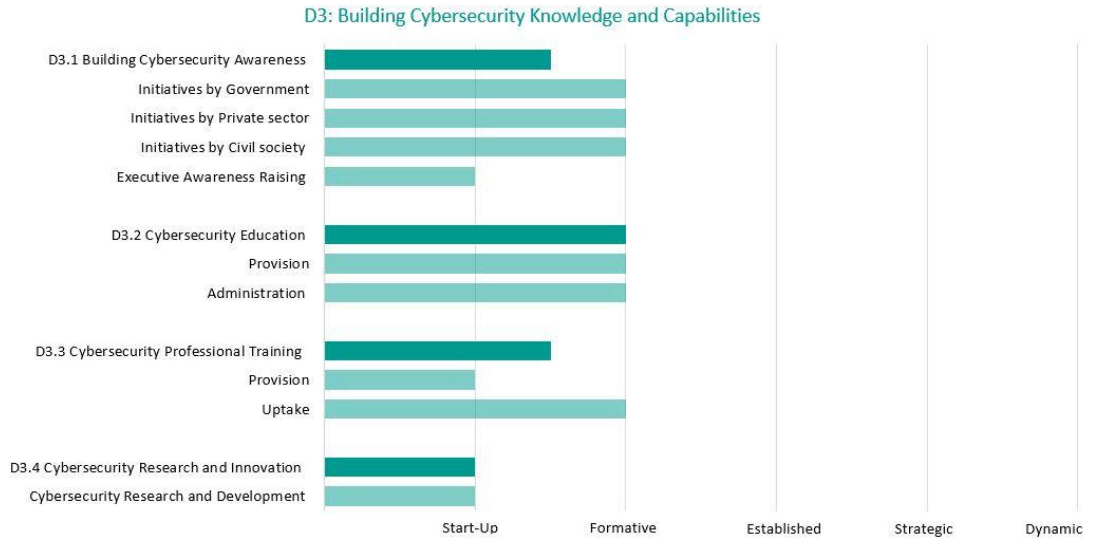
R2.5.4 Establish constructive mechanisms for whistleblowers in the public and private sectors and promote their existence.

DIMENSION 3
BUILDING CYBERSECURITY KNOWLEDGE AND CAPABILITIES

This Dimension reviews the availability, quality and uptake of programmes for various groups of stakeholders, including the government, private sector and the population as a whole, and relate to cybersecurity awareness-raising programmes, formal cybersecurity educational programmes, and professional training programmes.


Initiatives by Private Sector
Initiatives by Civil Society
Initiatives by Government
Executive Awareness Raising
D3.1 Building Cybersecurity Awareness
Provision
Dimension 3
Cybersecurity Research and Development
D3.4. Cybersecurity Research and Innovation
D3.2 Cybersecurity Education
Building Cybersecurity Knowledge and Capabilities
Administration
D3.3 Cybersecurity Professional Training
Uptake
Provision

OVERVIEW OF RESULTS



D 3.1 BUILDING CYBERSECURITY AWARENESS

This Factor focuses on the availability of programmes that raise cybersecurity awareness throughout the country, concentrating on cybersecurity risks and threats and ways to address them.

Stage: **Start-Up to Formative**

There is no overarching national cybersecurity awareness-raising programme, coordinating the efforts of relevant stakeholders. Greater national-level coordination of cybersecurity awareness-raising efforts within the country is under development as part of the development of the National Cybersecurity Strategy (NCS). Metrics to review awareness-raising efforts at the national level do not yet exist. Reportedly, some organisations conduct cybersecurity-awareness training for their internal staff. It was reported that organisations within the financial sector tend to be more mature than other sectors in terms of awareness raising for staff. In these cases, some metrics to review the effectiveness of efforts may be being applied on an ad-hoc basis.

There are indications that various stakeholders in the country realise they can play a role in cybersecurity awareness-raising and some have been involved in ad-hoc initiatives. It was reported that a limited number of cybersecurity-awareness webinars and seminars have been run free for the general public, including as part of Cybersecurity Awareness Month (October 2021). This has included efforts by some representatives from government, the private sector, regulators and civil society. The parties involved in these initiatives reportedly included the Office of the Data Protection Commissioner, Critical Infrastructure (CI) organisations and private-sector companies, civic groups, and URCA (the Telecommunications sector regulator).

It was reported that there has been an increase in uptake of such offerings by the general public.

Other fora and seminars held to raise cybersecurity awareness have included the Cyber Security Forum held by the Bahamas Chamber of Commerce and Employers Confederation (BCCEC) in May 2018; a seminar to increase cybersecurity and cybercrime awareness held by the Central Bank of the Bahamas in 2019; and a joint conference held by the Government of the Bahamas and the International Development Bank (IDB) in December 2019 to share international experiences in cybersecurity. These are annual events that were not conducted in the past two years due to the restrictions of the Covid-19 pandemic.

Some stakeholders described intentions to increase their awareness-raising activity. For example, university representatives stated they do not currently get involved in awareness-raising for the community (such as running public seminars or giving talks to schools, for example), but intend to begin doing so by sending out advisories to sensitise users to risks such as phishing and to the need to protect passwords, for example.

The Get Safe Online Bahamas project provides cybersecurity awareness-raising for personal and business contexts, and has been running in The Bahamas for the past four years. The project is part of the international Get Safe Online project[45], and funded by the UK Foreign, Commonwealth and Development Office (FCDO)[46]. The Get Safe Online Bahamas portal[47] is the primary site for cybersecurity awareness in the Bahamas, with high levels of interaction from Bahamians (verified by statistics provided to the CMM review team by the hosts). It is directly linked to from the Bahamas Government website.

The portal provides cybersecurity awareness content specific to The Bahamas, including personal advice (protecting computers and devices; e-commerce; safeguarding children and social networking); advice for businesses (hardware and devices; information security; online safety and security; rules, guidelines and procedures; software). The site also includes a glossary of information-security terms, and a very limited set of locally-produced audio and video advice clips are available. This represents a good central online resource for cybersecurity awareness-raising, that can now be built out with further resources. Involving a larger number of stakeholders in awareness-raising activities coordinated via the Get Safe Online project and portal may be an effective way of building a more coordinated national-level awareness-raising effort.

A Cybersecurity Ambassadors programme is also run as part of the Get Safe Online project and described in the portal; the portal can be used to apply to become a Cybersecurity Ambassador[48]. Through this scheme, local people are trained to share cybersecurity knowledge with local groups, for example businesses, churches and schools. Reportedly, there are currently three active ambassadors in the Bahamas; eight were trained originally. As part of the international Ambassadors Day (February 2021)[49], which focused on giving advice on the safer use of the Internet, representatives from the Bahamas were involved in providing in-depth online sessions.

[45] https://cybilportal.org/actors/get-safe-online/

[46] https://cybilportal.org/projects/cyber-awareness-campaign/

[47] https://www.getsafeonline.bs/

[48] https://www.getsafeonline.bs/landing-pages/ambassadors/

[49] https://www.getsafeonline.to/wp-content/uploads/2021/04/v2-Final-GSO_Ambassador_Day_Infographic.pdf

In terms of awareness-raising by the media, it was reported that articles appear in local newspapers following major cybersecurity incidents. This may help to raise awareness but is currently reactionary. Some proactive awareness-raising news releases are made, for example by the Office of the Data Protection Commissioner, and some insurance companies and banks reportedly run cybersecurity awareness-raising advertisements on the radio. The government stated an intention to make efforts to increase the coverage and reach of cybersecurity awareness issues in the media.

Participants were not aware of any awareness-raising initiatives aimed specifically at executives, although some organisations may conduct such initiatives internally. As a result, it may be that only a limited number of executives are aware of their responsibilities to shareholders, clients, customers and employees in relation to cybersecurity.

D 3.2 CYBERSECURITY EDUCATION

This Factor addresses the availability and provision of high-quality cybersecurity education programmes and sufficient qualified teachers and lecturers. Moreover, this Factor examines the need to enhance cybersecurity education at national and institutional levels and the collaboration between government and industry to ensure that educational investments meet the needs of the cybersecurity education environment across all sectors.

Stage: Formative

No specialised degrees in cybersecurity are currently offered and accredited at university level (Bachelors or Masters) by a Bahamian institution. Certain courses at the University of The Bahamas (UB) currently include security-related short modules[50]. An Introduction to Information Security module has been offered as an elective, originally to Computer Science students only, and more recently to Business students. The module is also included in the core requirements for the Bachelor of Business Administration in Accounting, and the Bachelor of Business Information in Computer Information Systems. The module includes key principles of information security and risk awareness, as well as practical tasks, for example using Kali Linux to gain experience of practical cyber-attacks. Reportedly, the course has a high level of uptake and has been oversubscribed since being opened up to Business students. There is therefore some evidence of demand for cybersecurity education.

There are some cybersecurity educational offerings from other institutions; for example, a three-month programme has previously been offered by the Bahamas Institute of Financial Services to obtain an Advanced Certificate in Cyber Security[51]. Stakeholders noted that citizens

[50] https://www.ub.edu.bs/wp-content/uploads/2016/11/Academic-Catalogue-2021-2022-FINAL.pdf

[51] https://www.bifs-edu.com/cyber-security-

of The Bahamas are able to access online and international Cybersecurity education courses, although the extent of uptake is unclear and statistics were not provided.

While no specialised cybersecurity degrees are offered currently, UB have developed a fully accredited Bachelors degree in Cybersecurity and Information Assurance, which is soon to be offered. The course has been approved, and it is anticipated that the course will be offered beginning in the fourth quarter of 2022, with the first modules being offered as electives from early 2022. The course reportedly covers topics including information security and assurance, business processes, computer forensics, malware analysis, social engineering and psychology. Stakeholders responsible for developing the course noted that the intention behind including not only technical modules such as malware analysis, but also modules such as business processes, is to produce graduates who are well-suited to employment by Bahamian organisations, who will need experts in information security who understand factors such as privacy policies and compliance with international laws.

This Bachelors course has been in development for around two years, and during the development process it was reviewed informally by a range of stakeholders including cybersecurity experts on the international stage (the organisers of well-recognised international cybersecurity conferences); and experts from industry. International initiatives such as the US NIST National Initiative for Cybersecurity Education (NICE)[52] were used to inform the development of the course and the selection of modules.

Academic stakeholders reported plans to increase cybersecurity-related educational offerings at university level in the future, to include topics such as security of the Internet-of-Things and smart cities. It was noted that a key challenge will be finding the right educators with the skillsets to teach such programmes: a shortage of local educators is a barrier to building out the educational offering. It was reported that there have already been some discussions with other universities (e.g., in the US) to share skills or create hybrid programmes to teach some of these more specialised courses. It may also be valuable to bring in collaboration from government and industry experts.

There are currently no cybersecurity educational or awareness offerings aimed at non-specialists. Consideration should be given to how to build such offerings into broader education programmes; for example by incorporating cybersecurity into general education programmes such as the one offered by UB, which is followed by almost all Bachelors students.[53] It was reported that there is a plan to offer the introduction to information security elective, currently offered to Computer Science and Business students only, more widely to students throughout the university, as a module of the general education programme.

There was no evidence of cybersecurity offerings in the curriculum at primary- or secondary-school level, and participants were not aware of any such offerings. In 2019, the DTU was commissioned to develop a cybersecurity programme for high-school students and find educators to deliver it; however, this was halted by the COVID-19 pandemic. There was recognition from participants of the need to continue this discussion with the Ministry of Education and secondary schools on how to develop such courses, in order to develop cybersecurity skills from an early age. Participants stated that they would like to see a national

[52] https://www.nist.gov/itl/applied-cybersecurity/nice

[53] https://www.ub.edu.bs/wp-content/uploads/2016/11/Academic-Catalogue-2021-2022-FINAL.pdf

curriculum for cybersecurity education and awareness from school to higher-level learning that is implemented and measured.

There is some alignment developing between educational offerings and the new NCS, which is currently being drafted: academic stakeholders reported being involved in the recent NCS-development discussions, with a specific meeting having been held on education. Furthermore, “Cybersecurity Awareness and Skills” (education and training at all academic levels to build the skilled pool of professionals needed to protect the nation’s information systems) in an objective of the 2022 NCS draft.

A national budget focused on cybersecurity education is not yet established; resources are put towards cybersecurity education, for example by UB, without national-level coordination. Establishing a national budget should form part of the ongoing national-strategy development, which should have a focused section on education with actions identified, and an implementation plan should identify the necessary budget as well as metrics for reviewing the supply and demand for cybersecurity education and the effectiveness of the offerings.

D 3.3 CYBERSECURITY PROFESSIONAL TRAINING

This Factor addresses and reviews the availability and provision of affordable cybersecurity professional training programmes to build a cadre of cybersecurity professionals. Moreover, this Factor reviews the uptake of cybersecurity training, and horizontal and vertical cybersecurity knowledge and skills transfer within organisations, and how this transfer of skills translates into a continuous increase of cadres of cybersecurity professionals.

Stage: Start-Up to Formative

Some private firms offer cybersecurity-training courses online and in-person in The Bahamas. Stakeholders noted that opportunities are readily available to undertake cybersecurity professional training in local training centres. This includes preparation courses and examinations for internationally recognised certifications such as Certified CISO training, Certified Ethical Hacker, CISSP and CompTIA Security[54,55]. There are also regional cybersecurity professional training offerings available within The Bahamas[56].

Reportedly there have been instances of international companies coming to The Bahamas to offer professional training locally, for example to banks, as well as organisations (such as some government departments) subscribing to international training offerings[57]. Some local

[54] https://mildaintrainings.com/loc/cyber-security-training-in-bahamas/

[55] https://www.synergybahamas.com/course-details/?course_id=33360&course_type=p

[56] https://www.nhcaribbean.com/training-and-certifications/technical-courses/cybersecurity

[57] https://www.udemy.com/topic/cyber-security/

offerings support organisations in offering training to their employees: through informative videos and simulated phishing campaigns, for example[58].

In terms of uptake of professional training, it was reported that there is uptake of the training courses, but fewer people are taking the examinations to become certified. It was noted that some companies, particularly those that have a parent company abroad governing information security, have a roadmap for cybersecurity training for their staff; in local companies training tends to be more ad-hoc. In sectors with higher cybersecurity maturity – Finance in particular – more internal training occurs, as well as processes such as shadowing to facilitate the transfer of cybersecurity skills and progression of cybersecurity careers.

There has not yet been an effort to analyse the need for cybersecurity professionals at the national level, or to measure the supply and demand for cybersecurity training courses, and statistical data relative to cybersecurity skills in The Bahamas has not been collected. It was reported by those stakeholders responsible for the development of the NCS that this is a planned objective of the strategy. The collection and analysis of such data would enable better understanding of the supply and demand for cybersecurity professional training, and documentation of the key training requirements to meet the needs of society.

While the supply and demand for cybersecurity professionals has not been measured, a number of stakeholders noted challenges observed in the availability of, and opportunities for, local cybersecurity professionals.

Firstly, it was noted that a significant proportion of local companies may not fully understand the need to hire cybersecurity professionals (and it was noted that this stems from companies' lack of awareness of the cybersecurity risk and their responsibility to mitigate it in general). There may be a need to educate companies on cybersecurity, and of particular relevance to this issue on the need to hire staff to work in cybersecurity roles, and on the certifications they should expect those they hire to possess. This currently results in reduced opportunity for trained cybersecurity professionals to fill cybersecurity roles within The Bahamas.

It was reported by numerous participants that this issue is exacerbated by a tendency by some organisations in both the public and private sectors to hire cybersecurity professionals from abroad, rather than hiring local professionals. There may be a perception, stemming from negative perceptions of the level of cybersecurity in the nation, that experts from abroad are better than local experts. This may mean that qualified Bahamians miss out on local cybersecurity roles, that the incentive for Bahamians to train as cybersecurity professionals is reduced, and that insufficient effort is invested in developing a cadre of local experts that can fill cybersecurity positions.

In support of this point, it was noted that some companies have senior cybersecurity roles (e.g., CISOs) filled by remote workers in the US, for example, and that in some companies the entire IT department is working remotely from abroad. It was noted that some employers craft role requirements (e.g., requirements for international experience) that locals are less likely to meet. Participants qualified these points, noting that while assistance from abroad is welcome and may be particularly appropriate and cost-effective for some cases such as contracting US companies for one-time architectural engagements, in order to build cybersecurity programmes, companies need on-the-ground personnel to implement controls

[58] https://www.bahamascybershield.com/

and develop frameworks, and there is a need to invest locally to build these skillsets and ensure the opportunities are given to qualified local experts.

The issue is two-pronged: it was noted that there is indeed a shortage of local qualified professionals in cybersecurity, but that even those qualified are not necessarily being offered the roles locally. This in turn leads to reduced career-progression opportunity for local experts, and lower incentive for local people to train to become cybersecurity professionals.

In response to these issues, participants felt that there is a need for focus investment on improving the local cadre of cybersecurity professionals. This means creating a pipeline that raises awareness amongst young people (in schools and universities) of cybersecurity career paths, makes clear the opportunities to achieve the necessary qualifications, and makes available opportunities to gain industry experience. It will clearly be important that the developing national cybersecurity strategy identifies actions to tackle this issue. Of course, the cybersecurity skills gap is not an issue unique to The Bahamas but a challenge around the world. Participants noted that a dedicated centre for training and certification in cybersecurity (particularly encouraging enrolment from younger people) could be beneficial, as well as initiatives to retain these experts in the country.

There is also a need to make local companies aware of the availability of local qualified experts that can carry out cybersecurity roles. It may be valuable to consider whether any government interventions (such as job-creation initiatives for cybersecurity) or incentives schemes are needed to encourage companies to invest in local talent rather than hiring externally.

D 3.4 CYBERSECURITY RESEARCH AND INNOVATION

This Factor addresses the emphasis placed on cybersecurity research and innovation to address technological, societal and business challenges and to advance the building of cybersecurity knowledge and capabilities in the country.

Stage: Start-Up

There is currently no, or only very limited, cybersecurity research and development (R&D) activity taking place in The Bahamas. Participants in the review sessions were not aware of any such activity, but noted that some cybersecurity R&D activity may be carried out by private companies. No doctoral-level students are researching cybersecurity topics yet. As such, research outputs are not yet being produced that address cybersecurity issues within the particular context of the country.

Academic stakeholders reported an interest in carrying out increased research activity and empirical studies in cybersecurity. Currently, there is no collaboration in regional or international cybersecurity research networks or projects; however academic stakeholders reported that there have been discussions with some foreign universities around cybersecurity research collaboration.

Some examples of broader technology research activity were noted; for example in the FinTech space, Project Sand Dollar was a project developed by the Central Bank of the Bahamas as part of the Bahamian Payment Systems Modernisation Initiative[59]. It was inaugurated in October 2020, to offer a Central Bank Digital Currency (the first launched anywhere in the world) with a view to furthering objectives of financial inclusion and transaction efficiency.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *Building Cybersecurity Knowledge and Capabilities*, the following set of recommendations are provided to The Bahamas. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

BUILDING CYBERSECURITY AWARENESS

R3.1.1 **(High priority)** Assign a dedicated body, for example the body responsibly for the GetSafeOnline Bahamas project, or any other relevant body, to take responsibility to coordinate all Cybersecurity Awareness activities in The Bahamas. The dedicated body should take ownership for all the Recommendations below.

R3.1.2 **(High priority)** Ensure that the concept of a national cybersecurity awareness-raising programme is solidly included in the NCS under development.

R3.1.3 **(High priority)** Develop the content for an overarching national cybersecurity awareness-raising programme which is linked to the draft NCS.

R3.1.4 The programme referred to in R3.1.3 should have an action plan which:

- consolidates and coordinates, as far as possible, all existing awareness-raising initiatives by various stakeholders (including those not currently involved, such as universities)
- identifies how such existing programmes can synergistically contribute to the national awareness-raising effort, and suggest improvements where necessary
- identify further efforts and stakeholder involvement relevant to the national programme

[59] https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2021/the-bahamas/trends-and-developments

R3.1.5 Identify the resources necessary to implement the national awareness-raising programme, specifically as far as financial support is concerned, and ensure that all resources needed are put in place.

R3.1.6 Develop the GetSafeOnline portal into a national cybersecurity awareness portal.

- The Portal should be a single point of access to all aspects of Cybersecurity Awareness, covering the cybersecurity awareness needs of the various sectors of society.
- The Portal should be used to advance and promote the national Cybersecurity Awareness programme, and vice versa.

R3.1.7 Develop and maintain an outcome-oriented system of metrics to allow the effectiveness of the national cybersecurity awareness-raising programme to be measured, and use the metrics to review and improve the national programme. Ensure adequate funding is available for this task.

R3.1.8 Work with relevant stakeholders to create a national cybersecurity awareness-raising programme for executives across the public and private sectors and civil society. The programme should raise executives' awareness of their responsibilities to shareholders, clients, customers and employees in relation to cybersecurity.

CYBERSECURITY EDUCATION

R3.2.1 **(High priority)** Task a dedicated body, for example the Ministry of Education, or another suitable body, to take responsibility for a National Cybersecurity Education Programme (NCEP) in the country. The dedicated body should take ownership for all the Recommendations below.

R3.2.2 Ensure that the NCEP is based on international best practices, and is informed by broad consultation across government, the private sector, academia and civil society.

R3.2.3 **(High priority)** Ensure that the new NCS contains a focused section on cybersecurity education.

R3.2.4 **(High priority)** Ensure that a national budget for implementing the NCEP is available.

R3.2.5 Develop accredited degrees in cybersecurity at university level.

R3.2.6 Ensure that the availability of cybersecurity modules within universities is expanded by offering such modules to students studying a wider range of courses, or making them part of the General Education offering.

R3.2.7 Promote cybersecurity education for non-specialists, by encouraging universities and other bodies to include cybersecurity-related modules in course and hold seminars or lectures for these audiences.

R3.2.8 Investigate the supply of local cybersecurity educators in the country and ensure it meets the growing need for cybersecurity education at all levels (schools, universities, and vocational level).

R3.2.9 Ensure that cybersecurity modules are included in school curricula at primary and secondary level.

R3.2.10 Work with relevant stakeholders to create and promote competitions, initiatives and funding schemes for students in order to increase the attractiveness of cybersecurity careers.

R3.2.11 Initiate the development and funding of an outcome-oriented metrics system to determine data regarding the supply and demand for cybersecurity degree offerings and to measure the effectiveness of such offerings.

R3.2.12 Implement initiatives to raise awareness amongst young people (in schools and universities) of cybersecurity career paths, make clear the opportunities to achieve the necessary qualifications, and make available opportunities to gain industry experience.

CYBERSECURITY PROFESSIONAL TRAINING

R3.3.1 **(High priority)** Assign a dedicated body, in cooperation with relevant stakeholders, to take responsibility to coordinate all Cybersecurity Professional Training activities in The Bahamas, and to take responsibility and ownership of the Recommendations listed below.

R3.3.2 **(High priority)** Ensure that the concept of a National Cybersecurity Professional Training programme is solidly included in the NCS under development.

R3.3.3 **(High priority)** Create a comprehensive metrics system to determine and analyse the needs at the national level in regard to cybersecurity professionals. The system should include programme-review processes and metrics to assess the supply and demand for cybersecurity-skilled workers in both public and private environments, and allow progress to be measures. Ensure proper funding for the system.

R3.3.4 Develop structured cybersecurity training programmes to develop skills towards building a cadre of cybersecurity professionals. In developing these programmes, take into account international cybersecurity vocational-based frameworks and best practices.

R3.3.5 Ensure that cybersecurity professional certification is offered across sectors within the country and encourage formal certification after completion.

R3.3.6 Ensure that relevant cybersecurity training programmes for non-cybersecurity professionals are offered.

R3.3.7 Develop government initiatives to retain trained cybersecurity professionals in the country after successful completion of training programmes.

R3.3.8 Consider creating a dedicated centre for training and certification in cybersecurity (which might particularly encourage enrolment from younger people).

R3.3.9 Ensure that organisations are made aware of the need to hire staff to work in cybersecurity roles, and the certifications they should expect those they hire to possess.

R3.3.10 Consider whether any government interventions or incentives schemes are needed to encourage companies to hire locally qualified experts for cybersecurity roles, rather than hiring from abroad.

R3.3.11 Establish job-creation and career-path initiatives and incentives for cybersecurity professionals within organisations to encourage employers to train staff to become cybersecurity professionals.

CYBERSECURITY RESEARCH AND INNOVATION

R3.4.1 **(High priority)** Assign a dedicated body, in cooperation with relevant stakeholders, to take responsibility to coordinate and expand all Cybersecurity Research and Innovation activities in The Bahamas, and to take ownership of the Recommendations listed below.

R3.4.2 **(High priority)** Ensure that the concept of Cybersecurity Research and Innovation is solidly included in the NCS under development.

R3.4.3 **(High priority)** Together with relevant stakeholders, identify cybersecurity R&D activities that would be beneficial to the nation, and ensure that these activities are emphasised in the new NCS. Consider developing a separate Cybersecurity Research, Development and Innovation (CRDI) strategy with links to the NCS.

R3.4.4 Identify and put in place the resources and processes necessary to deliver the CRDI strategy.

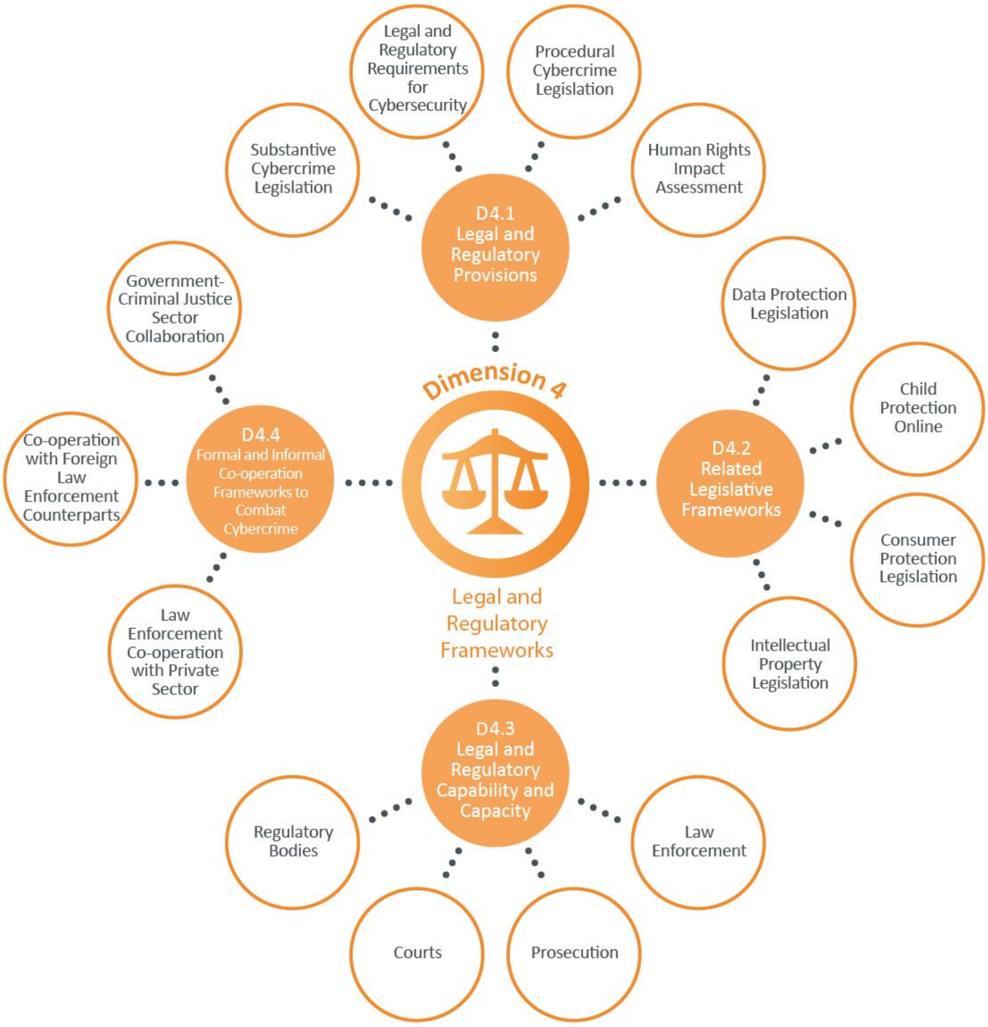
R3.4.5 Ensure that the CRDI strategy coordinates and expands participation, collaboration and partnerships between relevant university and industry stakeholders. Also ensure that it extends such collaboration and partnerships with regional and international cybersecurity-related research networks.

R3.4.6 Put in place a system of metrics to determine, measure and monitor aspects such as:

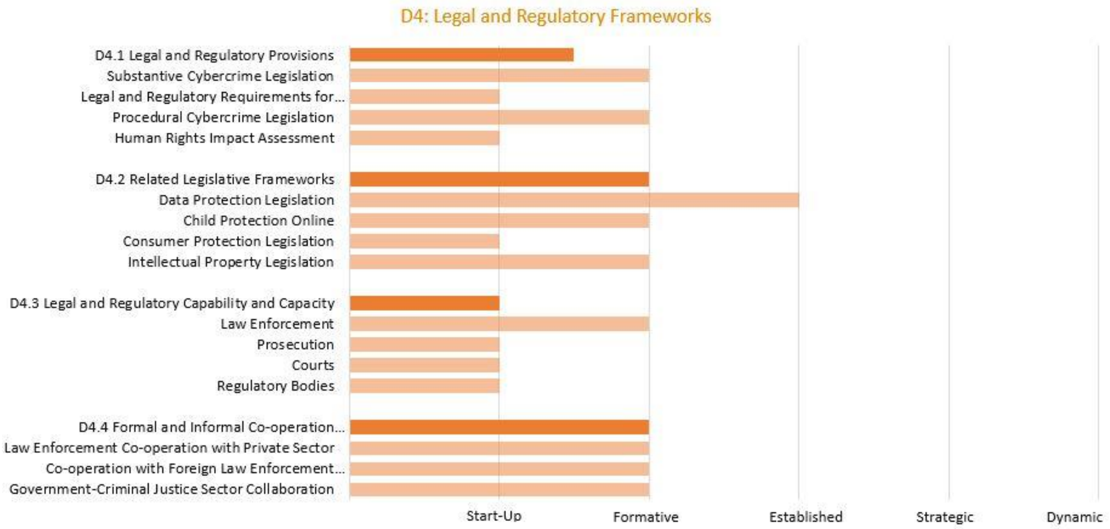
- National R&D requirements, performance, and outputs to allow progress to be measured and improve the cybersecurity R&D capability of the country.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This Dimension examines the government's capacity to design and enact national legislation that directly and indirectly relates to cybersecurity, with a particular emphasis placed on the topics of regulatory requirements for cybersecurity, cybercrime-related legislation and related legislation. The capacity to enforce such laws is examined through law enforcement, prosecution, regulatory bodies and court capacities. Moreover, this Dimension observes issues such as formal and informal co-operation frameworks to combat cybercrime.


Legal and Regulatory Requirements for Cybersecurity
Procedural Cybercrime Legislation
Substantive Cybercrime Legislation
Human Rights Impact Assessment
D4.1 Legal and Regulatory Provisions
Government-Criminal Justice Sector Collaboration
Data Protection Legislation
Dimension 4
Child Protection Online
Co-operation with Foreign Law Enforcement Counterparts
D4.4 Formal and Informal Co-operation Frameworks to Combat Cybercrime
D4.2 Related Legislative Frameworks
Consumer Protection Legislation
Law Enforcement Co-operation with Private Sector
Legal and Regulatory Frameworks
Intellectual Property Legislation
D4.3 Legal and Regulatory Capability and Capacity
Regulatory Bodies
Law Enforcement
Courts
Prosecution

OVERVIEW OF RESULTS



D 4.1 LEGAL AND REGULATORY PROVISIONS

This Factor addresses various legislation and regulatory provisions relating to cybersecurity, including legal and regulatory requirements, substantive and procedural cybercrime legislation, and human rights impact assessment.

Stage: Start-up to Formative

The Computer Misuse Act (2003) is the only legislation in The Bahamas that directly addresses cybercrime.[60] The act defines 'computer' very broadly:

> **Chapter 107A**
> **Computer Misuse Act**
>
> Part I
> Preliminary
> (1) In this Act —"computer" means an electronic, magnetic, optical, electrochemical, or other data processing device, or a group of such interconnected or related devices, performing logical, arithmetic, or storage functions, and includes any data

[60] Computer Misuse Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

storage facility or communications facility directly related to or operating in conjunction with such device or group of such interconnected or related devices. [61]

(Extract from the Computer Misuse Act)

Potentially, a 'computer' under the act would refer to devices such as smart TVs, smart phones, tablets and smart watches. It criminalises the following actions:

Part II
Offences

- Using a computer to secure unauthorised access to any program or data held in a computer;
- Using a computer to secure access to any program or data held in any computer with intent to commit an offence involving property, fraud or dishonesty, or which causes bodily harm;
- Doing any act which you know will cause unauthorised modifications in the contents of any computer;
- Knowingly (i) securing access without authority to any computer for the purpose of obtaining any computer service, or (ii) intercepting without authority any computer functions using any device, or (iii) using or causing a computer to be used directly or indirectly for the purpose of committing an offence;
- Knowingly and without authority or lawful excuse interfering with, interrupting or obstructing the lawful use of a computer; or impeding or preventing access to, or impairing the usefulness or effectiveness of, a computer;
- Knowingly and without authority disclosing any password, access code or other means of access to any program or computer data for wrongful gain or an unlawful purpose or knowing that it would cause wrongful loss to any person; and
- Obtaining access to any protected computer in the course of commission of an offence.[62]

(Extract from the Computer Misuse Act)

This suggests that the Computer Misuse Act (CMA) criminalises the most common forms of cybercrime, including hacking, phishing scams (e.g., entering bank accounts) and spoofing emails (e.g., messages with a forged sender address in order to reveal to the spoofer personal information).[63] The CMA also 'covers offences such as cyberstalking, cyberbullying, unlawful online gaming and online prostitution.'[64] Desk research indicates that the 'CMA applies extraterritorially and empowers the Bahamian courts to exercise jurisdiction in relation to any

[61] Computer Misuse Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

[62] Ibid.

[63] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

[64] Ibid.

offence committed outside of The Bahamas.'[65] It may become necessary to update the legislation as new technologies and new forms of criminality emerge.[66]

With regards to procedural cybercrime legislation, the Criminal Procedure Code is the main general framework that applies to all cybercrime related investigations.[67] Furthermore, desk research suggests that the Computer Misuse Act also includes some procedural powers related to the offenses listed, under Article 15 (Police powers) and Article 16 (Power of police officer to access computer and data):

> **Article 15**. (1) A police officer may arrest without warrant any person who has committed or is committing, or whom the police officer with reasonable cause suspects to have committed, or to be committing, an offence under this Act.
>
> **Article 16**. (1) A police officer or a person authorised in writing by the Commissioner of Police, pursuant to a warrant under section 70 of the Criminal Procedure Code, shall —
> (a) be entitled at any time to —
> (i) have access to and inspect and check the operation of any computer to which this section applies;
> (ii) use or cause to be used any such computer to search any data contained in or available to such computer; or
> (iii) have access to any information, code or technology which has the capability of retransforming or unscrambling encrypted data contained or available to such computer into readable and comprehensible format or text for the purpose of investigating any offence under this Act or any other offence which has been disclosed in the course of the lawful exercise of the powers under this section.[68]

(Extract from the Computer Misuse Act)

Articles 15 and 16 refer specifically to search and seizure procedures.[69] Based on desk research, the Computer Misuse Act does provide for a form of data retention, however, it does not serve the same purposes as data preservation, that is not present.[70]

Other relevant legislative frameworks related to The Bahamas' Internet landscape are:

[65] Higgs & Johnson (2017) Cybercrime Under Bahamian Law, https://higgsjohnson.com/cybercrime-under-bahamian-law/

[66] Ibid.

[67] Criminal Procedure Code (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1968/1968-0038/CriminalProcedureCodeAct_1.pdf

[68] Computer Misuse Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0002/ComputerMisuseAct_1.pdf

[69] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

[70] Ibid.

- **Electronic Communications and Transactions Act**[71] (2003) – includes provision on electronic communications data retention, electronic communications as evidence, and electronic signatures;
- **Interception of Communications Act**[72] (2017) – includes provision on the authorised interception of all communication networks, which would include public telecommunication operators and Internet providers and also provides for the use of certain devices for listening to private conversations;
- **Data Protection (and Privacy) Act**[73] (2003) – contains provisions on privacy, data protection, data subject rights, enforcement and penalties;
- **Sexual Offences and Domestic Violence Act**[74] (2010) – includes provisions on sexual procuration, child pornography, and voyeurism including by electronic means.

There are limited cybersecurity requirements set out in regulation or law. The need to create legal and regulatory frameworks on cybersecurity have been recognised by participants.

The Digital Transformation Unit (DTU) legal consultants advised that no special human-rights impact assessments have been conducted, but the legislators are trained in international human rights and human rights are considered during the drafting of laws. According to the US State Department's 2020 Human Rights assessment report for The Bahamas the government 'did not restrict access to the internet or censor online content, and there were no credible reports the government monitored private online communications without appropriate legal authorisation.'[75] Similarly, the Freedom House's 2021 Freedom on the Net report stated that freedom of expression, belief and right to assembly is protected by the constitution, and the government respects this right in practice.[76]

[71] Electronic Communications and Transactions Act (2003) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/2003/2003-0004/ElectronicCommunicationsandTransactionsAct_1.pdf

[72] Interception of Communications Act (2017) https://www.bahamas.gov.bs/wps/wcm/connect/321b5dd5-6ec0-4497-9742-59ba2c0a93b2/Interception+of+Communication+Bill_2C+2017+(Consol+Cabinet++Amendment)+Feb+7+tr1.pdf?MOD=AJPERES

[73] Data Protection (and Privacy) Act (2003) http://www.lexbahamas.com/Data Protection 2003.pdf

[74] Sexual Offences and Domestic Violence Act (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1991/1991-0009/SexualOffencesAct_1.pdf

[75] US State Department (2020) Country Reports on Human Rights Practices: The Bahamas, https://www.state.gov/wp-content/uploads/2021/03/BAHAMAS-2020-HUMAN-RIGHTS-REPORT.pdf

[76] Freedom House (2021) Freedom on the Net: The Bahamas, https://freedomhouse.org/country/bahamas/freedom-world/2021

D 4.2 RELATED LEGISLATIVE FRAMEWORKS

Stage: **Formative**

This Factor addresses the legislative frameworks related to cybersecurity including data protection, child protection, consumer protection, and intellectual property.

The Data Protection (and Privacy) Act was endorsed in 2003 that includes provisions on privacy, data protection, data subject rights, enforcement, and penalties.[77] Desk research suggests that under Exclusions 5 the act 'contains exemptions for the transfer of data for criminal investigations and prosecutions and permits international transfers of criminal evidence', including when the transfer is pursuant to international legal assistance procedures (MLATs).[78]

The Office of the Data Protection Commissioner is an agency that carries out its role as privacy 'Ombudsman' in The Bahamas.[79] The Commissioner is 'primarily responsible for: 1) Administering and enforcing the provisions of the Data Protection Act; 2) Promoting the observance of good practice by data controllers within the requirements of the Act; 3) Influencing thinking on privacy and processing of personal information matters on a local and global basis; and 4) Discharging, as the national supervisory authority, various functions relating to or arising from any international obligations The Bahamas may have or is seeking to be a party to, in connection with data protection.'[80]

The **protection of children online**, is covered in the Sexual Offences and Domestic Violence Act (2010) that contains provisions on child pornography transmitted by electronic means:

> **16A. Child pornography**
>
> (3) In this section, "child pornography" means —
> (a) a photographic, film, video or other visual representation whether or not it was made or transmitted by **electronic** or mechanical means —
> (i) that shows a person who is, or is depicted as being, under the age of eighteen years engaged in explicit sexual activity; or
> (ii) the dominant characteristic of which is the depiction, of a sexual organ or the buttocks of a person under the age of eighteen years; or

[77] Data Protection (and Privacy) Act (2003) http://www.lexbahamas.com/Data_Protection_2003.pdf

[78] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

[79] Office of the Data Protection Commissioner, https://www.bahamas.gov.bs/

[80] Ibid.

(b) any written material or visual representation that advocates sexual activity with a person under the age of eighteen years.[81]

(Extract from the Sexual Offences and Domestic Violence Act)

With regards to **consumer protection**, the Consumer Protection Act was passed by the Parliament in 2006.[82] The legislation provides consumers a forum to have their complaints addressed on a timely basis.[83] The act focuses on consumer concerns related to the protection from hazards to their health and safety and consumer education.[84] The Consumer Affairs Office is mandated to enforce and monitor the legislation.[85] However, the act's application in the online environment is yet to be considered.

The Bahamas has been a 'member of the World Intellectual Property Organisation (WIPO) since 1977, but has not ratified the WIPO Internet treaties'.[86] The Department of the Registrar General maintains The Bahamas' intellectual property registry.

PART VI
Infringement of Copyright

(7) Where copyright in a work is infringed by a public performance of the work or by the performance of the work in public by means of a machine or device for performing sound recording or motion pictures and other audiovisual works, or receiving visual images or sounds conveyed **by electronic means**, the persons specified in subsection (8) are also liable for the infringement.[87]

(Extract from the Copyright Act)

Article 7 of the Infringement of Copyright section of the Copyright Act (2010) makes references to the law's application in the online environment.

Restitution of stolen property after conviction

113. Any court before which any person is convicted of an offence, under the provisions of the Penal Code, involving **stealing**, taking, obtaining, embezzling,
converting or disposing of or knowingly receiving **any property**, may direct the restitution of such property to the owner thereof or his representative in accordance with and subject to the provisions of section 64 of the Penal Code.[88]

[81] Sexual Offences and Domestic Violence Act (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1991/1991-0009/SexualOffencesAct_1.pdf

[82] Consumer Protection Act (2006) http://extwprlegs1.fao.org/docs/pdf/bha78749.pdf

[83] The Government of The Bahamas, Consumer Protection Information and Complaints, https://www.bahamas.gov.bs/wps/portal/public/Consumers/

[84] Ibid.

[85] Ibid.

[86] U.S. Department of Commerce, International Trade Administration (2021) Bahamas - Country Commercial Guide, Protecting Intellectual Property, https://www.trade.gov/country-commercial-guides/bahamas-protecting-intellectual-property

[87] Copyright Act (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1998/1998-0008/CopyrightAct_1.pdf

[88] Criminal Procedure Code (2010) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1968/1968-0038/CriminalProcedureCodeAct_1.pdf

(Extract from the Criminal Procedure Code)

According to the GCI 2020 survey by the ITU, the copyright infringements are also covered indirectly through the use of the Criminal Procedure Code and it is considered as 'stealing' of any property.[89]

D 4.3 LEGAL AND REGULATORY CAPABILITY AND CAPACITY

This Factor studies the capacity of law enforcement to investigate cybercrime, the prosecution's capacity to present cybercrime and electronic evidence cases, and the court's capacity to preside over cybercrime cases and those involving electronic evidence. Finally, this Factor reviews the existence of cross-sector regulatory bodies to oversee compliance with specific cybersecurity regulations.

Stage: Start-up

In The Bahamas cybercrime is divided into two categories that is not legally written but used for reference and during investigations: 1) *cyber-dependent crime* or 'pure' cybercrime (crimes against computers/information systems, e.g., network hacking, DDoS attacks); and 2) *cyber-enabled crime* (traditional crime that uses the Internet/network to commit a crime, e.g., child pornography, ransomware, scams, defamation usually over social networks). Online scam is the most frequent cyber-enabled crime reported by the public.

Law enforcement officers lack sufficient capacity to prevent and combat cybercrime in The Bahamas. In 2010, a dedicated cybercrime unit (8 people) was created under the Criminal Investigations Department of the Royal Bahamas Police Force (RBPF) and trained by U.S. federal law enforcement agencies.[90] [91]

Law enforcement officers receive ad-hoc training on cybercrime and digital evidence provided by the U.S. State Department, U.S. Department of Defence, INTERPOL[92] and OAS. Participants expressed concern that the trainings lack consistency and are not sufficiently advanced to deal with emerging threats. The last local training was in 2016, in collaboration with the U.S.

[89] ITU, GCI 2020 survey

[90] The Bahamas Police Force, https://www.royalbahamaspolice.org/aboutus/index.php?aboutus_id=1

[91] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

[92] INTERPOL (2016) INTERPOL boosts cybercrime policing capacity in Latin America and the Caribbean, https://www.interpol.int/fr/Actualites-et-evenements/Actualites/2016/INTERPOL-boosts-cybercrime-policing-capacity-in-Latin-America-and-the-Caribbean

Embassy and the FBI, where 16 RBPF officers participated in a cybercrime training workshop through the Caribbean Basin Security Initiative (CBSI).[93]

The RBPF runs a Forensic Science Lab that conducts forensic computer examination such as 'computer data evidence recovery and examination of digital/electronic evidence'.[94] However, participants acknowledged that most of the equipment and technology used in the laboratory are outdated (e.g., from a hardware perspective probably 7-8 years behind) that puts law enforcement at a disadvantage when investigating new incidents. The DTU is reportedly helping the RBPF to update and modernise the laboratory, as part of the ongoing "Government Digital Transformation to Strengthen Competitiveness" project. Participants added that law enforcement relies on international assistance from the FBI and INTERPOL, especially in cases where the government's network has been compromised. With regards to cyber-enabled cases, one of the challenges for law enforcement when providing digital evidence is the need to clarify the evidence to the prosecutor and the judge (e.g., explaining the legal nature of IP addresses).

There is no local institution or consistent programme of specialised training for law enforcement officers, prosecutors or judges in The Bahamas. The Bahamas Bar Association does not offer specialised training on cybercrime in the country (as they do in the United States, Canada, or the UK). However, there are some opportunities for specialised training abroad (e.g., in the U.S.).

In 2021, the Council of Europe, through its Octopus Project, offered a series of EU funded online cybercrime trainings for the Caribbean countries including The Bahamas.[95] It targeted law enforcement and security practitioners and covered sessions on electronic evidence, financial investigations and international cooperation.[96]

During the review, it was not clear to what extent sector-specific regulators (e.g., finance, energy, transport) are equipped with the capability and resources required to oversee compliance with cybersecurity requirements within their sector.

[93] U.S Embassy in the Bahamas, U.S. Embassy Provides Cyber Crime Training for the Royal Bahamas Police Force, https://bs.usembassy.gov/pr-01212016/

[94] The Bahamas Police Force, Forensic Science, http://www.royalbahamaspolice.org/careers/forensic.html

[95] Council of Europe (2021) Octopus Project Activities: CARICOM IMPACS and Octopus Project: EU funded online cybercrime trainings for the Caribbean, https://www.coe.int/en/web/cybercrime/-/caricom-impacs-and-octopus-project-eu-funded-online-cybercrime-trainings-for-the-caribbean

[96] Council of Europe (2021) Octopus Project Activities: CARICOM IMPACS and Octopus Project: EU funded online cybercrime trainings for the Caribbean, https://www.coe.int/en/web/cybercrime/-/caricom-impacs-and-octopus-project-eu-funded-online-cybercrime-trainings-for-the-caribbean

D 4.4 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This Factor addresses the existence and function of formal and informal mechanisms that enable co-operation between domestic actors and across borders to deter and combat cybercrime.

Stage: Formative

The authorities in The Bahamas have recognised the need to improve both formal and informal cooperation mechanisms, domestically and across borders, but these mechanisms remain ad hoc.

Participants described the operational cooperation and exchange of information between the government and criminal justice actors (police, prosecutors and judiciary) as adequate. With regards to more serious crimes, after the investigation is complete, the law enforcement shares the report with the Office of the Attorney General of the Department of Public Prosecutions for review prior to the defendants being charged before the court. In the past, the process of review was not included and once the police officers completed the investigation, the report was taken straight to the magistrates.

There is ad-hoc co-operation between Internet service and other technology providers and law enforcement. The police first has to obtain a court order or a warrant in order to access information from internet service providers (ISPs). A participant described the challenges of cooperating with foreign ISPs such as Facebook. It was not clear to what extent these arrangements are supported by appropriate legislation.

The existing provisions under the Mutual Legal Assistance Act (2002) facilitates international assistance in criminal matters and criminal investigations between The Bahamas and foreign states.[97] Based on desk research, it 'references data and computer systems and could potentially cover some of the international cooperation requirements in Budapest Convention on Cybercrime, but it is not known whether it has been utilised for electronic evidence.'[98] There are no provisions that allow law enforcement to preserve computer data or traffic data on behalf of a foreign state in cybercrime investigations. Furthermore, the act does not cover trans-border access to stored computer data with consent or where publicly available, nor the establishment of a 24/7 network to ensure expeditious assistance of mutual-assistance

[97] BAHAMAS. Mutual Legal Assistance (Criminal Matters) (2002) http://laws.bahamas.gov.bs/cms/images/LEGISLATION/PRINCIPAL/1988/1988-0002/MutualLegalAssistanceCriminalMattersAct_1.pdf

[98] Council of Europe, Octopus Cybercrime Community, The Bahamas, https://www.coe.int/en/web/octopus/country-wiki-ap/-/asset_publisher/CmDb7M4RGb4Z/content/bahamas?_101_INSTANCE_CmDb7M4RGb4Z_viewMode=view/#:~:text=Bahamas%20adopted%20the%20Computer%20Misuse,unauthorised%20disclosure%20of%20access%20code%3B

requests. Currently, The Bahamas has mutual legal assistance treaties (MLATs) only with the U.S., Canada and the UK. Other regional agreements are managed through CARICOM. Among the different available international cooperation channels, the ‘police-to-police’ coordination via INTERPOL was described as an important channel to facilitate cross-border cooperation and information sharing that is handled by the National Central Bureau in Nassau. [99]

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to The Bahamas. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL AND REGULATORY PROVISIONS

R4.1.1 **(High priority)** Consider setting up a periodic process of reviewing and enhancing The Bahamas’ laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: cyber-bullying, hate speech online, sexting and accessing or downloading child-pornography images).

R4.1.2 Revise the Computer Misuse Act (2003) in order to take account of emerging technologies and their use.

R4.1.3 Consider ratifying the Budapest Convention on Cybercrime and update and harmonise existing legislations (e.g.: substantive and procedural laws).

R4.1.4 **(High priority)** Develop legal and regulatory frameworks on cybersecurity requirements in consultation with stakeholders from relevant sectors.

R4.1.5 Ensure that relevant civil and criminal liabilities are clearly articulated and understood by regulated entities.

R4.1.6 Ensure that procedural laws relating to cybercrime permit the exchange of information (and other actions required) to support successful cross-border investigation of cybercrime.

[99] INTERPOL. The Bahamas, https://www.interpol.int/en/Who-we-are/Member-countries/Americas/BAHAMAS

R4.1.7 **(High priority)** Conduct human rights impact assessments of substantive and procedural cybercrime legislation and cybersecurity regulations (including consideration of privacy and freedom of expression implications).

R4.1.8 **(High priority)** Dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation.

R4.1.9 Ensure stronger judicial oversight of lawful surveillance to make it more robust and transparent.

RELATED LEGISLATIVE FRAMEWORKS

R4.2.1 **(High priority)** Develop new or amend existing legislative provisions through multi-stakeholder consultation processes to address children's safety online, data protection online, consumer protection online and intellectual property online.

LEGAL AND REGULATORY CAPABILITY AND CAPACITY

R4.3.1 **(High priority)** Invest in advanced investigative capabilities (by using up-to-date technology) in order to allow the investigation of complex cybercrime cases, supported by regular testing and training of investigators.

R4.3.2 **(High priority)** Allocate resources dedicated to fully operational cybercrime unit based on strategic decision-making, in order to support investigations, both at the institutional and national security level.

R4.3.3 Strengthen national investigative capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.3.4 **(High priority)** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence through international organisations in order to acquire new ICT skills needed for cybercrime investigations (for e.g.: digital evidence gathering) and effective ways of enforcing cyber-laws. Consider making arrangements with academic or industry bodies to support the development and delivery of cybercrime training.

R4.3.5 **(High priority)** Ensure that sector-specific regulators (e.g.: finance, energy, transport) are equipped with the capability and resources required to oversee compliance with cybersecurity requirements within their sector.

R4.3.6 Consider making amendments about the rules so that witnesses can provide evidence in court virtually.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

R4.4.1 **(High priority)** Strengthen formal mechanisms of international law enforcement co-operation including mutual legal assistance, extradition agreements and mechanisms applied to cybercrime cases and enter further bilateral or international agreements.

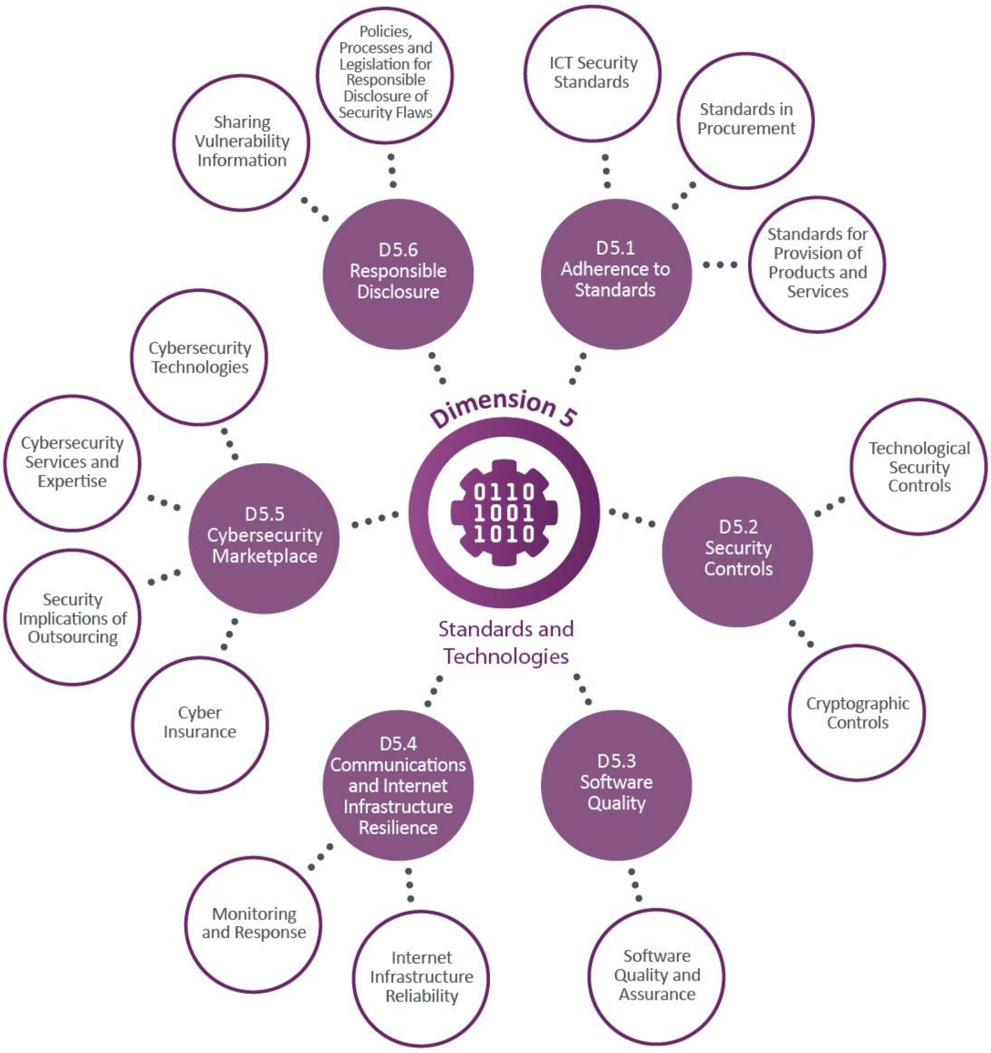
R4.4.2 **(High priority)** Allocate resources to support the exchange of information between public and private sectors domestically, and to enhance the legislative framework and communication mechanisms.

R4.4.3 Facilitate and strengthen informal cooperation mechanisms within the police and criminal-justice system, and between police and third parties, both domestically and across borders, in particular with Internet service and other technology providers.

R4.4.4 Consider establishing a 24/7 point of contact within the Cybercrime Unit of the Royal Bahamas Police Force in order to provide instant assistance for mutual legal assistance requests.

DIMENSION 5
STANDARDS AND TECHNOLOGIES

This Dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The Dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.


Policies, Processes and Legislation for Responsible Disclosure of Security Flaws
ICT Security Standards
Sharing Vulnerability Information
Standards in Procurement
D5.6 Responsible Disclosure
D5.1 Adherence to Standards
Standards for Provision of Products and Services
Cybersecurity Technologies
Dimension 5
0110
1001
1010
Standards and Technologies
Cybersecurity Services and Expertise
D5.5 Cybersecurity Marketplace
Technological Security Controls
D5.2 Security Controls
Security Implications of Outsourcing
Cyber Insurance
Cryptographic Controls
D5.4 Communications and Internet Infrastructure Resilience
D5.3 Software Quality
Monitoring and Response
Internet Infrastructure Reliability
Software Quality and Assurance

D 5.1 ADHERENCE TO STANDARDS

Stage: Start-Up to Formative

This Factor reviews the government’s capacity to promote, assess implementation of, and monitor compliance with international cybersecurity standards and good practices.

No national baselines for the implementation of cybersecurity standards, standards in procurement (from a cybersecurity perspective), or standards for provision of products and services (from a cybersecurity perspective) exist in The Bahamas. Establishing a baseline of cybersecurity standards for the CI was previously an objective of the draft 2014 NCS (but this was not published or implemented) and is an objective of the new 2022 NCS draft. In some industries, some organisations may follow certain cybersecurity standards and best practices, but this is not overseen or mandated. In summary, the implementation of cybersecurity-related standards is ad-hoc, and there has as yet been no concerted endeavour on a national level to change existing practice in a measurable way.

The Finance sector is relatively advanced in this area, as is broadly the case around the world. Although cybersecurity requirements have not yet been mandated by the Central Bank (the regulator of the Finance sector) in the Bahamas, the Finance sector largely comply with international standards including SWIFT cybersecurity requirements, and banks reported that while PCI is not mandated, it tends to be a goal internally.

It was noted that, while they are not mandated, international standards such as ISO 27001, NIST Cyber Security Framework (CSF) are promoted by the Central Bank. The Central Bank provides operational risks guidelines and sets expectations of licensees in terms of application of security standards and incident-response planning, in the form of a cybersecurity-attestation framework for licensees, which has led to Finance organisations having a higher level of maturity. It was noted that there is a technology risk-management guideline for the Bahamas Finance sector, which is being updated to reflect cybersecurity needs.

Certain sector regulators set requirements that are not cybersecurity-specific but cover eventualities related to cybersecurity. The example of the Utilities Regulation and Competition Authority (URCA) was given: for example, if an incident were to lead to a major outage, fines would be imposed according to the regulation, and this would include a cyber-incident. Healthcare entities described seeking to comply with HIPAA.

Some sectors reported needing adherence to other jurisdictions’ cybersecurity regulations due to system outsourcing; the example of the healthcare system was given, some system implementations within which are offered as a service by a US vendor, and as such the vendor has contractual terms in place relating to the relevant regulations.

The owners of the current NCS development noted that part of the strategy will focus on regulation of the CI in regard to cybersecurity; stakeholders from the CI appeared to regard this as a positive change, stating that it would be useful to have more guidance on and regulation of cybersecurity controls in the CI. There was a desire for specific guidelines for CI cybersecurity, noting that not all CI sectors are alike, but there should be some guidelines on general commonalities that can be audited for compliance.

D 5.2 SECURITY CONTROLS

This Factor reviews evidence regarding the deployment of security controls by users and public and private sectors, and whether the technological cybersecurity control set is based on established cybersecurity frameworks.

Stage: Formative

Since there is no national baseline of cybersecurity standards, and application of standards by organisations is ad-hoc and relatively limited, there is significant variation in the application of security controls, both technological and cryptographic, by organisations.

Organisations in some industries, including Finance, Telecommunications, Utilities and Healthcare, reported applying various technological and procedural cybersecurity controls. Examples included incident response, with some organisations having their own internal cybersecurity incident-response teams, and having developed formal cybersecurity incident-response policies and plans including definition of roles and escalation plans, with annual tabletop exercises to test them. Internationally recognised resources such as the NIST Cyber Security Framework[100] were cited as having been used to support the development of these plans. Having an incident-response plan is a key part of the requirements of the Finance sector, including the SWIFT and Central Bank attestation requirements.

Participants noted that the application of security controls largely by organisations depends on their sector and resulting requirements or expectations (for example, in the Finance sector); the organisation's understanding of the cybersecurity risk; and whether the organisation employs staff in cybersecurity roles. It was also noted that some organisations that have parent companies abroad may attain a higher level of security maturity through adoption of the parent company's policies and liaison with the parent company to build security posture, and monitor for and address incidents.

Participants felt that there is a lack of focus on administering cybersecurity controls by many organisations in The Bahamas. A key reason for this, according to participants in the sessions, is that many organisations have no or very limited staff in cybersecurity roles. In government, there is no dedicated information-security department, but responsibility for cybersecurity falls the Department of Transformation and Digitization. In other organisations, responsibility often falls to IT teams to react to cybersecurity incidents, but these teams do not usually have the cybersecurity skill or time to spend on building a security programme proactively. This shortage of skilled cybersecurity staff means that these organisations are not implementing

[100] https://www.nist.gov/cyberframework

cybersecurity controls frameworks effectively, nor are they able to continuously monitor and improve the effectiveness of these controls.

Participants expressed the view that the mindset of company leadership drives this shortage of cybersecurity roles within organisations. Executives within some organisations are not prioritising cybersecurity, and do not understand the need for security officers within their organisations. Awareness-raising and education on cybersecurity for executives is therefore very important.

ISPs participating in the CMM review sessions described security measures in place to manage risks in the services they offer. A participating ISP described monitoring the security of their services to protect customers against DoS attacks, as well as having controls such as incident-response plans in place, with a security team dedicated to these efforts. Tools are being deployed by some service providers to secure communications between servers and users. The application of these security controls by service providers is ad-hoc and varies between providers.

Some participants expressed the view that government agencies and companies are not prioritising the protection of users' data sufficiently. Examples were given of recent breaches of databases holding sensitive personal information[101]. There may be a need to consider how to raise the level of protection of data in transit and data at rest, including using cryptographic controls, through awareness-raising targeted at businesses and government agencies. It was also suggested that further governance is needed in this area.

D 5.3 SOFTWARE QUALITY

This Factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this Factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the critical nature of services.

Stage: Start-Up to Formative

Software quality and functional requirements are identified in some sectors, but not in a strategic manner. No catalogue of assured software platforms and applications exists within the public or private sectors. There is currently no support or guidance from the government for organisations on procuring or maintaining secure software.

Some organisations have policies and processes in place for assessing software quality and monitoring its lifecycle. In the Finance sector, sectoral guidelines cover software security, and

[101] https://practiceguides.chambers.com/practice-guides/data-protection-privacy-2021/the-bahamas/trends-and-developments

software procurement undergoes approval processes including security considerations, along with regular penetration testing and patch management. Some Healthcare organisations described running internal testing processes for software, considering frameworks such as NIST, SANS, HIPAA. Such organisations also reported requesting penetration-testing results from vendors, as well as commissioning penetration tests throughout the software's lifecycle.

It may be valuable to build a centrally managed list of trustworthy and secure software for use. Such a catalogue does not currently exist, and as such companies may not know which software is reliable and secure, or otherwise. Information on software-quality deficiencies is not yet being gathered in a strategic manner to inform users or developers; such information could also be represented in the catalogue.

D 5.4 COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

This Factor addresses the existence of reliable Internet services and infrastructure in the country, as well as rigorous security processes across private and public sectors. Also, this Factor reviews the control that the government might have on its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Formative

Internet services are widely available and used in The Bahamas, at 85% penetration in 2017 according to the ITU[102]. There are two ISPs operating in the Bahamas and three submarine Internet cables (ARCOS, Bahamas Domestic Submarine Network international (BDSNi) and Bahamas Internet Cable System)[103], offering some redundancy.

Representatives from the ISPs described running servers on other islands in the archipelago, to increase their redundancy. These representatives also reported measures in place to manage security risks within the Internet infrastructure. This includes incident-response plans, and network-security monitoring by security-engineering teams, in place within some ISPs, particularly to protect downstream users from attacks such as DoS. It was noted that the level of security risk-management may not be consistent across ISPs, however.

Some concerns were expressed by participants about the reliability of these Internet services from a consumer perspective. One example given was a shortage of static IP addresses, which can reportedly make it difficult to obtain the addresses needed. It was also suggested that on the international stage the Internet in The Bahamas may be perceived to be prone to issues such as botnets and DoS, which can impact on trust in Bahamian digital services from abroad. Participants felt that there is a need for more consistent redundancy and security across ISPs in The Bahamas, to prevent issues for downstream services.

[102] https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BS

[103] https://unctad.org/system/files/non-official-document/dtl_eWeek2017c06-isoc_en.pdf

D 5.5 CYBERSECURITY MARKETPLACE

Stage: Start-Up

This Factor addresses the availability and development of competitive cybersecurity technologies, cyber-insurance products, cybersecurity services and expertise, and the security implications of outsourcing.

Most cybersecurity technologies are developed outside The Bahamas; participants were not aware of any such technologies developed locally. There is therefore a high level of dependence on foreign cybersecurity technologies. There was no evidence that the implications of this dependence had been considered systematically, and doing so will be important to ensure that associated risks are identified and mitigated.

There are a limited number of local cybersecurity consultancy services available in the country, who have reportedly carried out work such as risk assessments with companies and government agencies, for example. Some local providers provide details of the certifications they possess from international bodies such as the Cloud Security Alliance[104]. Cybersecurity consultancy services are also available internationally, for example via the Big Four consultancy firms. Participants were not aware of any guidance available to assist organisations with the selection of consultancy-service providers.

It was reported that due to proximity to nations such as the US, and also due to globalisation broadly, there is sufficient access to cybersecurity consultancy firms by organisations in The Bahamas. However, some participants noted that a stronger local offering would be beneficial, due to concerns about the additional security risks that might be created by outsourcing these services outside the country, as well as recognition of the potential economic benefits of growing this local market and developing a stronger cadre of local experts. Participants again reported the issue of skills from abroad being favoured over local skills in some cases, resulting in international consultancy offerings being used in preference to local consultancy firms in some cases.

No evidence was provided of risk assessments conducted by organisations to determine how to mitigate the risks of outsourcing IT to a third party or cloud provider, although it is likely that this takes place in some organisations from sectors more advanced in terms of cybersecurity, such as Finance. Some participants stated that the maturity of organisations with regards to using cloud providers needs to be improved: in particular the understanding of the potential risks of outsourcing data and business processes to the cloud.

Cyber-insurance is available to companies in The Bahamas via international providers that are brokered locally. Some organisations, for example in the Telecommunications sector, reported having purchased cyber-insurance. There is a need to ensure that the current offerings are sufficient for the country: that they provide the necessary cover to organisations

[104] https://www.cloudcarib.com/about-us/awards-recognition/

in the country, and that they play a role in encouraging positive behaviours such as the sharing of threat information amongst participants of the market.

D 5.6 RESPONSIBLE DISCLOSURE

This Factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors, and whether there is sufficient capacity to continuously review and update this framework.

Stage: Start-Up to Formative

There are no formal information-sharing mechanisms or channels in place locally for stakeholders to share technical details of vulnerabilities. Some organisations, such as in the Finance sector, participate in regional and international information-sharing groups. No evidence was provided of informal sharing of information on vulnerabilities, although it is likely that some occurs on an ad-hoc basis.

Furthermore, it was noted that there may be a lack of willingness to share information on incidents due to concerns about reputation, which results in important information being kept private. There are no fully enforced requirements for any sector to report cybersecurity incidents (as described, the Central Bank does expect Financial institutions to report cybersecurity incidents to its supervision unit, although this is not mandated and enforceable via fines). It was noted that the Office of the Data-Protection Commissioner is supposed to be informed of any breaches relating to personal data, but that in reality this is not sufficiently enforced and does not always happen.

Participants from the CI expressed the view that improved information-sharing within and between sectors would be highly beneficial, to improve the awareness of current threats to specific industries and in general, and of vulnerabilities in technologies. This may require a formal framework or mechanism for information-sharing, including standardisation of the communications protocols between different sectors and of the requirements for reporting on certain types of attack and vulnerability.

Most public and private sector organisations do not yet have responsible-disclosure policies guiding the processes they follow to receive and disseminate vulnerability information responsibly. Such a policy might include disclosure deadlines, scheduled resolution, and the need for acknowledgement, to guide cases in which they identify a security flaw or a security flaw is disclosed to them. There was no evidence provided that the right to legal protections for those disclosing security flaws had yet been discussed, and participants were not aware of any “bug bounty” programmes (through which individuals can receive recognition or compensation for reporting exploits and vulnerabilities) within The Bahamas to encourage responsible disclosure by ethical hackers.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards and Technologies, the following set of recommendations are provided to The Bahamas. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1.1 **(High priority)** Identify a national baseline of cybersecurity-related standards and good practices, and promote broad implementation across the public and private sectors.

- This baseline should include cybersecurity standards and best practices guiding procurement processes (including risk management, lifecycle management, software and hardware assurance, outsourcing, and use of cloud services).
- It should also include cybersecurity standards for the provision of products and services (including software development, hardware-quality assurance, provision of managed services and cloud security).

R5.1.2 In establishing this baseline, consider how standards and best practices can be used to address risk within supply chains, particularly within the CI.

R5.1.3 **(High priority)** Establish an entity within government to assess the use of cybersecurity standards across the public and private sectors.

R5.1.4 Establish government programmes for promoting adherence to the identified cybersecurity standards.

SECURITY CONTROLS

R5.2.1 **(High priority)** Through the identification, promotion and monitoring of cybersecurity standards, as above, ensure that organisations in all sectors are deploying up-to-date technological and cryptographic security controls that conform to internationally-established cybersecurity frameworks, standards and good practice.

R5.2.2 Promote the use of physical security controls by organisations in all sectors to prevent unauthorised personnel from entering computing facilities.

R5.2.3 Consider how to ensure that all Internet-service providers establish policies for the deployment of technical security controls, as well as deploying cryptographic controls to secure communications between servers and users, in order to manage risks in the services they are offering.

SOFTWARE QUALITY

R5.3.1 **(High priority)** Develop a centrally managed catalogue of assured software platforms and applications, to guide the use of software within the public and private sectors.

R5.3.2 **(High priority)** Promote the use of reliable software applications that adhere to international standards and good practices in the public and private sectors.

R5.3.3 Promote the development of policies on and processes for software updates and maintenance by organisations in all sectors (noting that this may form part of the baseline of standards, as above).

R5.3.4 Develop a resource (which may be linked to the catalogue – see R5.3.1) that characterises software applications in regard to their reliability, usability and performance.

COMMUNICATIONS AND INTERNET INFRASTRUCTURE RESILIENCE

R5.4.1 **(High priority)** Ensure that the technology deployed and processes used by all organisations involved in providing Internet infrastructure meet international standards and follow good practices.

R5.4.2 Ensure that all organisations involved in providing Internet infrastructure have mechanisms in place to conduct risk assessments, to monitor and test network resilience and to respond to incidents (including establishing and regularly testing and reviewing incident-response plans).

R5.4.3 Ensure that all organisations involved in providing Internet infrastructure allocate appropriate resources to hardware integration, technology stress testing, monitoring, personnel training, response and drills to test response plans.

R5.4.4 **(High priority)** Establish formal management of the national Internet infrastructure, with documented processes, roles and responsibilities, and redundancy.

CYBERSECURITY MARKETPLACE

R5.5.1 **(High priority)** Convene relevant stakeholders to consider the security implications of using foreign cybersecurity technologies, and consider whether any actions are needed to mitigate potential risks.

R5.5.2 **(High priority)** Develop government guidance to assist organisations in selecting cybersecurity-consultancy providers to meet various needs.

R5.5.3 Convene relevant stakeholders to consider the security implications of using foreign cybersecurity-consultancy services, and consider whether any actions are needed to mitigate potential risks, including developing a stronger local cybersecurity-consultancy market, for example.

R5.5.4 Establish initiatives to raise organisations' awareness of the potential security implications of outsourcing IT to a third party or cloud services, and of how to mitigate these risks.

R5.5.5 **(High priority)** Convene relevant stakeholders to consider whether the current cyber-insurance offerings (in which cyber-insurance is available to companies in the country via international providers that are brokered locally) are sufficient: that they provide the necessary cover to organisations in the country, and that they play a role in encouraging positive behaviours such as the sharing of threat information amongst participants in the market.

RESPONSIBLE DISCLOSURE

R5.6.1 **(High priority)** Establish formal information-sharing mechanisms that stakeholders in the country can use to share the technical details of vulnerabilities, and of threats to specific sectors and across sectors. This may require standardisation of the communications protocols between different sectors, and of the requirements for reporting on certain types of attack and vulnerability.

R5.6.2 **(High priority)** Promote the development of responsible-disclosure policies by public and private-sector organisations, which should include disclosure deadlines, scheduled resolution, and the need for acknowledgement, to guide cases in which they identify a security flaw or a security flaw is disclosed to them.

R5.6.3 Consider whether there is a need to develop legislation to protect those disclosing security flaws responsibly.

R5.6.4 Consider establishing "bug bounty" programmes (schemes which enable individuals to gain recognition or compensation for responsible disclosure of bugs) to encourage the responsible disclosure of security flaws by ethical hackers.

ADDITIONAL REFLECTIONS

This review was carried out remotely under pandemic restrictions, and consequently representation by stakeholders within some groups was somewhat limited. The level of engagement in the review sessions by the stakeholders present was very high, however. The representation and composition of stakeholder groups was, overall, sufficiently balanced to enable the CMM review team to gather the necessary evidence.

APPENDICES

METHODOLOGY - MEASURING MATURITY

Deploying the CMM involves data-gathering both through in-country stakeholder consultation (typically over the course of three days) and remotely through desk research. It is designed to produce an evidence-based report which is submitted to the government representatives for the country being studied and will include recommendations to:

- benchmark the maturity of a country's cybersecurity capacity;
- provide a detailed a set of pragmatic actions to contribute towards the advancement of cybersecurity capacity
- identify maturity gaps; and
- identify priorities for investment and future capacity-building.

During the review of a country, specific dimensions are discussed with relevant groups of stakeholders. Each group of stakeholders is asked to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 'Cybersecurity Culture and Society' and Dimension 3 'Building Cybersecurity Knowledge and Capabilities' of the CMM.

Data collection

The Review Team gathers the evidence necessary to identify the stages of maturity across the CMM through desk research, in-depth interviews, and modified-focus group discussions, utilising the CMM Structured Field Coding (SFC) Tool to capture the results. The functions of the Review Team include that of a facilitator to lead the group sessions, and a note-taker.

The CMM uses a **modified focus-group discussion methodology** that elicits data that complements and helps validate in-depth interviews and desk research.[105] As with interviews, focus-group discussions are an interactive methodology with the advantage that during the process of collecting data, diverse viewpoints and conceptions can emerge as participants follow the discussion. Rather than posing questions to specific participants, the researcher(s) facilitate a discussion among the participants, encouraging them to adopt, defend or explain different perspectives.[106] It is this interaction that offers advantages over other

[105] Williams, M. (2003). Questionnaire design. In *Making sense of social research* (pp. 104-123). SAGE Publications, Ltd, https://www.doi.org/10.4135/9781849209434; Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. (Ed.), *Successful focus groups: Advancing the state of the art* (pp. 35-50). SAGE Publications, Inc., https://www.doi.org/10.4135/9781483349008; Richard A. Krueger, R. A., & Mary Anne Casey, M. A., (2009) Focus-groups: A Practical Guide for Applied Research. SAGE Publications, London.

[106] Kitzinger, J. (1994). The methodology of focus groups: the importance of interaction between research participants. Sociology of health & illness, 16(1), 103-121. https://doi.org/10.1111/1467-9566.ep11347023;

methodologies, making it possible for the participants to reach a mutual understanding and to raise everyone's awareness of cybersecurity practices and capacities.[107] During CMM reviews, the Review Team leads the discussion to get onto all the aspects within the relevant dimensions.

To determine the level of cybersecurity capacity maturity, each *Aspect* has a set of indicators corresponding to all five stages of maturity. A consensus method is used to drive the discussions within sessions, for the stakeholders to provide evidence on how many indicators have been implemented by the country and to determine the maturity level of every aspect of the model. During focus-group discussions, researchers use semi-structured questions to keep discussions around relevant indicators. The discussion among stakeholders provides evidence regarding the implementation of indicators. In gauging the maturity level, if there is no evidence for all the indicators being met at a particular stage, then that country has not yet reached that stage of maturity.

Inconsistencies between stakeholders will inevitably occur. Equally, information known to a stakeholder in one sector might not be familiar in other sectors. Accordingly, it will fall to the Review Team to perceive these information gaps and then investigate them.

Desk research and modified focus groups inevitably raise some additional questions and possible inconsistencies. For this reason, and to a gain more in-depth understanding of key and sometimes unique policies and practices, a set of in-depth interviews are also conducted during and on some occasions following the field research.

Data analysis

With the prior consent of participants, all sessions are recorded. Individual responses are treated as confidential with the Chatham House Rule applied in reporting our results.[108] After conducting a country review, the **data collected during consultations** with stakeholders and the notes taken during the sessions are used to find evidence and **define the stages of maturity** for each *Aspect* of the CMM. The CMM report aggregates this information and determines the maturity for each Factor of the CMM.

In the course of the review further desk research is undertaken to bridge any gaps that emerge during the in-country data-collection process and to validate the evidence provided. While drafting the **CMM report**, further desk research and interviews are often necessary to address any missing information, and to validate and verify the results. For example, stakeholders might not always be aware of recent developments in their country, or if the country has signed a particular convention on personal data protection policy. Therefore, official government or ministry websites, annual reports of international organisations, university websites, in-depth interviews, etc. can be used as supplementary sources for information. This type of additional research helps to ensure that the report accurately reflects the Host

Kitzinger, J. (1995). Qualitative research: introducing focus groups. Bmj, 311(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299; Fern, E. F. (1982). The use of Focus Groups for Idea Generation: The Effects of Group Size, Acquaintanceship, and Moderator on Response Quantity and Quality. Journal of Marketing Research, 19(1), 1–13. https://doi.org/10.1177/002224378201900101

[107] Kitzinger, J. (1995). Qualitative research: introducing focus groups. *Bmj*, *311*(7000), 299-302. https://doi.org/10.1136/bmj.311.7000.299

[108] https://www.chathamhouse.org/about/chatham-house-rule

Country's cybersecurity capacity. In each case, the team does not privilege any particular source of information but seeks to reach a consensus on the most valid status of each indicator of the model.

Developing recommendations

For each *Dimension*, **recommendations** are provided for the next steps to be taken for the country to enhance its cybersecurity capacity. If a country's capacity for a certain *Aspect* is, for example, at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders. The recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the CMM. The recommendations are provided specifically for each *Factor.*

After a review by the GCSCC Technical Board, the draft report is submitted to the Local Host to secure feedback. If new evidence arises, the draft report is revised and the maturity stages of each *Aspect* and *Factor* in the CMM are updated correspondingly. Once all parties approve the draft report, the Local Host will take the lead in the publication process. Publication approval rests with the Host Country and if this is agreed the Local Host is encouraged to publish it via an official government portal or other outlet.

Data management and ethical considerations

Focus-group discussions are conducted online on Microsoft Teams™ and Zoom™ platforms. *(depending on platforms preferred by each nation)* The discussions are recorded using external recorders to guarantee confidentiality of the data and information collected, and for future transcription for the purpose of writing the CMM report. The recordings remain anonymised. The findings from the desktop study, in-depth interviews, and focus group discussions are consolidated during the analysis.

Global Cyber Security Capacity Centre

Department of Computer Science, University of Oxford

Wolfson Building, Oxford OX1 3QD,

United Kingdom

Tel: +44 (0)1865 287434

Email: cybercapacity@cs.ox.ac.uk

Websites: https://gcscc.ox.ac.uk/home-page#/ www.oxfordmartin.ox.ac.uk/cyber-security