National Cybersecurity Strategy - Towards A Secure Cyberspace 2020-2023

GOvernment of belize

Contents

[Glossary of Terms 3](#_Toc26782218)

[Acronyms 3](#_Toc26782219)

[Foreword 4](#_Toc26782220)

[Strategic Vision 4](#_Toc26782221)

[Principles 4](#_Toc26782222)

[Respect for and the promotion of fundamental rights 4](#_Toc26782223)

[Government Led 4](#_Toc26782224)

[Risk based approach 4](#_Toc26782225)

[Shared responsibility 5](#_Toc26782226)

[Fostering an environment for economic growth and innovation 5](#_Toc26782227)

[International Cooperation 5](#_Toc26782228)

[Introduction 5](#_Toc26782229)

[National Context 6](#_Toc26782230)

[Horizon 2030: The National Development Framework for Belize 7](#_Toc26782231)

[National Security and Defence Strategy 2017-2020 8](#_Toc26782232)

[Belize’s Growth and Sustainable Development Strategy (GSDS) 2016-2019 8](#_Toc26782233)

[Baseline Assessment 9](#_Toc26782234)

[Current status of cybersecurity: An overview 10](#_Toc26782235)

[Cybercrime 11](#_Toc26782236)

[Legislative Framework 13](#_Toc26782237)

[Critical Infrastructure 13](#_Toc26782238)

[Priority Areas 14](#_Toc26782239)

[Implementation 15](#_Toc26782240)

[Governance Structure 15](#_Toc26782241)

[Evaluation and Review 16](#_Toc26782242)

[Annex I 17](#_Toc26782243)

[Areas of Priority 17](#_Toc26782244)

[Area of Priority 1: Develop the National Legal Framework to adequately address cybersecurity threats 17](#_Toc26782245)

[Area of Priority 2: Develop a national capacity for incident response and critical information infrastructure protection 20](#_Toc26782246)

[Area of Priority 3: Implement measures to support Education, Awareness and Workforce Development in cybersecurity 22](#_Toc26782247)

[Annex 2 24](#_Toc26782248)

[Cybersecurity Capacity Maturity Model for Nations (CMM) - Belize comparative table 2016 and 2018 24](#_Toc26782249)

[Acknowledgement 28](#_Toc26782250)

# Glossary of Terms

Cybersecurity

Cybercrime

Cyber Incidents

Cyber Attacks

Internet

# Acronyms

BTL

BWL

PUC

CITO

NSCS

# Foreword

*[TO BE COMPLETED]*

# Strategic Vision

*Recognizing the benefits that technologies in this new digital age can bring, the people of Belize will work together to create a safe and trusted digital environment that will promote economic growth and social inclusion for all.*

# Principles

A comprehensive understanding of cybersecurity is paramount to keep pace with emerging technologies and more sophisticated threats. Cybersecurity capacity should not only include the protection of networks and systems, but also take into account the people that rely more and more on internet-enabled devices to conduct basic tasks. In that regard the following principles have guided the development of the Strategy and will further guide its implementation.

## Respect for and the promotion of fundamental rights

This Strategy recognizes that human rights apply online, as well as offline, and that cybersecurity and human rights are mutually reinforcing. Thus this Strategy protects and promotes fundamental rights and freedoms such as the right to privacy, freedom of expression, freedom of association, freedom of assembly among others, in addition to being in line with Part II of the Constitution of Belize and the international instruments to which Belize is party to.

## Government Led

Recognizing that the Government is one of the largest consumers of information technology services, it commits to driving the objectives of this Strategy by adopting best practices in its operations and lead by example in the implementation of the Strategy’s objectives.

## Risk based approach

With the understanding of the importance of Critical Infrastructure to the welfare of Belize, the Strategy seeks to mitigate cybersecurity risks to acceptable levels by encouraging the combination of cost benefit, acceptable risk and other qualitative and quantitative approaches with the desired end result of the protection of Belizean people and economy.

## Shared responsibility

Cybersecurity affects everyone and as a result it is a shared responsibility for all to exercise cybersecurity best practices. Targeted awareness raising initiatives will be implemented through the mobilization and partnership with civil society, academia and other interest groups across Belize, to enable and empower end-users to keep themselves and their organizations safer online.

## Fostering an environment for economic growth and innovation

Recognizing the importance of innovation and business development to our national economy, a cyber-environment that is safe and conducive to such development will be fostered.

## International Cooperation

The age-old statement ‘no-man is an island’ has become such a relevant concept in this digital era. The need for comprehensive stakeholder cooperation has never been greater than it is today. This Strategy focuses on the need to leverage international partnerships to investigate criminal activities, build capacity and protect Belize’s cyberspace.

# Introduction

This Strategy was developed in collaboration with the Government and stakeholders, to address cybersecurity threats facing Belize, so as to provide guidance on key actions to be taken to improve Belize’s overall preparedness and responsiveness to these threats. This Strategy outlines the principles and long-term goals that will form the basis and overall direction for the planning and development of the national cybersecurity posture, including a plan of action outlining various roles and responsibilities for implementation.

Cybersecurity impacts many actors such as, policy-makers, private sector, law enforcement, academia, and civil society, therefore a multi-stakeholder approach was used in the development of this Strategy. Cybersecurity risks[[1]](#footnote-1) in this regard, should therefore be analyzed within a broader context that also encompasses legal, economic and social factors, contributing to a better management of cybersecurity threats and decision-making. Technology is changing exponentially every day, and the threats surrounding these technologies are becoming increasingly sophisticated. Our growing connectivity and dependence on Internet-based platforms and services has significantly increased our exposure to cyber threats. While this growth has brought numerous opportunities for many nations, cyber threats have equally evolved in recent years. This therefore, requires the development of public policies that seek to ensure an open and safe Internet for all. In order to mitigate the impact of these threats, a structural change around cybersecurity is imperative. However, this structural change is only possible with national coordination and international cooperation, as well as with the active participation of different actors of society working in tandem. Globally, there is no one fix for these ever-evolving cyber threats and governments recognize the need for collaboration and cooperation among states, as well as all national cyber actors including the private sector, NGOs, academia, and citizens as a part of the solution. To compound these issues, the trans-border nature of the Internet requires strategic thinking, not only in how we adopt technological solutions for the creation of more efficient services, but also in how we protect them.

## National Context

Similarly, the implementation of cybersecurity measures takes into account many other aspects of a nation’s economic and developmental goals and plans. Therefore, in the development of the Strategy, there was a recognition that cybersecurity considerations cannot be taken in isolation but must be considered in the wider context of other policy decisions and national initiatives such as the National Sustainable Tourism Master Plan 2030[[2]](#footnote-2), the National Growth and Sustainable Development Strategy 2016-2019[[3]](#footnote-3), among others. The graphic below illustrates some of considerations and policies that were taken into account during the development of this Strategy:

### Horizon 2030: The National Development Framework for Belize

The Horizon 2030[[4]](#footnote-4) vision, goals and strategies arose out of an analysis of the current socio-economic situation of Belize, informed by a broad consultation process and review of existing technical and policy studies. The framework included specific vision statements from stakeholders including ‘Belizeans are capable of using state of the art technology which they incorporate into productive enterprise[s].’ Listed among five important cross cutting issues was a need to invest in education and a review of the education system to assess its strength and weaknesses and the development of a long term investment plan. This review, as stated in Horizon 2030, would define the human resources that are critical to closing the resource gaps identified. This approach is critical especially in the field of cybersecurity as it has been reported in several fora that there is a global cybersecurity skills gap, of which Belize is no exception. The gap in Cybersecurity jobs are expected to reach 1.8 million by 2022, up 20% from 1.5 million in 2015, according to the Center for Cyber Safety and Education.[[5]](#footnote-5)

### National Security and Defence Strategy 2017-2020[[6]](#footnote-6)

The vision of the NSDS is for a Belize “*of peace and tranquility, where citizens live in harmony with the natural environment and enjoy a high quality of life. Belizeans are an energetic, resourceful and independent people looking after their own development in a sustainable way”.* Having established itself on three main pillars, namely: 1. Maintain the Sovereignty and Territorial Integrity of Belize; 2. Reduce Local and Transnational Crimes; 3. Provide the necessary environment for a prosperous and stable Belize, the NSDS encompasses all factors identified to be essential to the security, stability and prosperity of Belize and the protection of the geopolitical space of Belize as defined by the Belize Constitution. As a part of the strategic objectives the NSDS states that as an effort to reduce such occurrences and the resulting harm to Belize’s sustainable development aspirations, there will be a provision of basic equipment and capacity to effectively manage and control Belize’s land, sea, air, and **cyber space** (emphasis added). As a nation we recognize cyberspace as a territory for protection. The NSDS further states that ‘in order to build public consensus, multilateral cooperation, and public-private partnerships to defeat transnational organized crime and local gangs, we aim to build new partnerships with industry, private sector, academia, civil society and non-governmental organizations to combat these networks that operate in the illicit and licit worlds...[as well as] ..further international norms against tolerating or sponsoring crime in all its forms, including in **cyberspace** especially as it relates to prostitution and sexual abuse’(emphasis added). This position is not a unique approach as many nations have recognized cyberspace as the fifth domain, and as a nation we will continue to extend our resources to protecting the all the borders of Belize, which is among the reasons for the development a strategic approach to cybersecurity efforts.

### Belize’s Growth and Sustainable Development Strategy (GSDS) 2016-2019

Flowing from Horizon 2030, the GSDS is a strategic plan that places sustainable development as a priority while striving to bring economic, social and environmental policies into balance. The GSDS is based on the principles of sustainable development, and on three notable drivers that are common to successful developing countries: a proactive role for the state, tapping into global markets, and innovative social policy.[[7]](#footnote-7) Among the Critical Success Factors for the GSDS, they identified CSF1, “Optimal National Income and Investment,” and included as an action to *‘Build institutional capacity to encourage technological adaptation and innovation while also taking into account climate change resilience considerations’.* This line of action encourages the adoption of technology to improve efficiency, productivity and competitiveness. As stated in the GSDS, *Capacity development processes will target the technical skills needed to facilitate government’s efforts to encourage innovation and imitation.* Notably, while technology will continue to revolutionize the way we do business, broader and wider-spread use of technology will also bring its vulnerabilities. Therefore the National Cybersecurity Strategy is designed to guide our nation to think of cybersecurity as an automatic consideration for any investment that involves technology.

## Baseline Assessment

It is imperative when designing a strategy at the national level that an assessment is undertaken to ensure, not only that the right areas of focus are identified, but also to determine what is being done well and where the deficiencies lie. As such, in the development of the National Cybersecurity Strategy, the level of connectivity to the internet was considered to determine the scope of the problem, cybersecurity capacities that exists was measured and finally, the volume of cybercrimes that are committed in Belize were taken into account.

In terms of connectivity, there has been a steady growth in the level of Internet penetration and connectivity[[8]](#footnote-8). The more connected people become the more avenues that open for opportunities for cyberattacks. As of 2018, the Internet penetration rate of Belize was recorded as being over 50% of the population, an increase of over 40% since 2000 (See Table and Chart below).

|  |  |  |  |
| --- | --- | --- | --- |
| Year | Population | Users | % Penet. |
| 2000 | 245,800 | 15,000 | 6.10% |
| 2005 | 291,904 | 35,000 | 12.00% |
| 2008 | 301,270 | 32,000 | 10.60% |
| 2012 | 327,719 | 74,700 | 22.80% |
| 2013 | 340,844 | 108,048 | 31.70% |
| 2018 | 382,444 | 200,020 | 52.30% |

Figure 1-Comparative Table with Population and Internet users over the last 5 years

Figure 2- Source: World Bank and ITU

The primary goal of information such as this is to implement measures to reduce risk. Ensuring an understanding of ‘what is at risk’ helps to shape prioritization and resourcing for implementation. Additionally, to measure existing capabilities to address the threats, in 2018, the Cybersecurity Capacity Maturity Model for Nations (CMM)[[9]](#footnote-9) assessment was undertaken, and the results indicated that Belize, since it was last applied in 2016, was still between a start-up and a formative level of maturity in regards to cybersecurity along the five dimensions of capacities that were assessed. Thus, indicating the need for the development of this comprehensive framework.

# Current status of cybersecurity: An overview

With the ever increasing growth in connectivity, the dependence on internet-based platforms has grown simultaneously, along with increased exposure to cyber related crimes. Despite the development and deployment of sophisticated cyber security solutions, patches, and updates, there has been a continuous increase in the number of cyber-attacks globally. For example, in 2018, a series of attacks from a group called ‘Magecart’ took place. This group was responsible for publicized breaches, including Ticketmaster and Feedify. With this, in addition to the recent spate of ransomware attacks on other targets such as FedEx, San Francisco’s light-rail network, and Britain’s National Health Service, it is clear that the frequency and complexity of attacks have increased.

An undeniable fact, is that many nations and organizations are struggling to keep pace with cybercriminal activities. The costs of cybercrime have been estimated to have quadrupled since 2015, reaching $2.1 trillion by the end of 2019 and outpacing spending on cybersecurity by over 16 times.[[10]](#footnote-10) Gartner forecasts that industry spend in 2018 will reach $93 billion, as traditional security measures such as firewalls and anti-virus software prove to be inadequate.[[11]](#footnote-11)

Cybersecurity has now become an increasing part of the national dialogue in Belize, with discussions to address this issue being staged among different sectors of the country. Over the past few years, several government agencies have also been working in order to address cybersecurity. Since 2014, the Ministry of National Security has been working on coordinating this at the national level and had organized a Cybersecurity Ad Hoc Committee, made up of multiple stakeholders, including academia and the private sector, to work together on building awareness about cybersecurity and cybercrime in Belize. Since then the National Cyber Security Task Force comprised a cross section of national stakeholders (both public and private sector, academia and civil society groups) was established in 2018 and was instrumental to the development of this Strategy.

## Cybercrime

The Police Information Technology and Cyber Unit (PITCU) of Belize Police Department (BPD) manages the investigations of cyber-related crimes, as well as those felonies that involve electronic evidence. The PITCU has investigated cases of phishing, credit card and ATM fraud, as well as other crimes that involve electronic evidence, including drug trafficking. They have also received reports of cyberbullying, revenge porn and identity theft. In terms of some international collaboration to counter cybercriminal activities, the PITCU holds a partnership with the Internet Watch Foundation in order to report cases of child pornography[[12]](#footnote-12). Below is a summary of cybercrimes recorded over the last five years.

| CyberCrimes 2013 to 2018 | | | | % per annum |
| --- | --- | --- | --- | --- |
|  | Crimes targeting technology, etc.\* | Crimes committed through technology\*\* |  | Growth |
| Year | Incidents | Incidents | Total # Incidents |  |
| 2013 | 521 | 80 | 601 |  |
| 2014 | 663 | 116 | 779 | 29.62% |
| 2015 | 713 | 166 | 879 | 12.84% |
| 2016 | 818 | 145 | 963 | 9.56% |
| 2017 | 773 | 118 | 891 | -7.48% |
| 2018 | 768 | 136 | 904 | 1.46% |

\* For example cellphones, computers, note books, theft, damage, virus etc.

\*\* For example, social engineering, phishing, texts, emails, etc.

Figure 3-Growth of Cybercrime - 5 year period

As recent as August 2018, it was reported that there were phishing scams targeting the Belizean Public.[[13]](#footnote-13) Given the prevalence of theft of mobile devices in Belize, PITCU has been paying close attention because many cyber-related crimes are being executed through stolen devices.

## Legislative Framework

Given that there is no comprehensive criminal legislation that strictly address cybercrime, the prosecution of these crimes have been difficult. Currently, Belize has four laws that inter-relate to cybercrime[[14]](#footnote-14): the Telecommunications Act-CAP. 229 and 229S[[15]](#footnote-15), the Electronic Evidence Act-CAP. 95:01[[16]](#footnote-16), the Electronic Transactions Act-CAP. 29:01[[17]](#footnote-17), the Intellectual Property Act, the Interception of Communications Act CAP. 229:01[[18]](#footnote-18) and the Mutual Legal Assistance in Criminal Matters Act- CAP. 103:01[[19]](#footnote-19). With this legislative gap, there is a great need for the development of a comprehensive cybercrime bill that is tailored to the reality of Belize.

## Critical Infrastructure

Cyber-attacks against critical infrastructure are a reality. These threats goes well beyond the risk of an information breach or an unavailable information system, but potentially impacts the lives of our citizens should critical infrastructure be impacted. There is a need to begin the dialogue among key stakeholders, which may include but not limited to ministries and other entities with responsibility for energy, banking and finance, communications, transportation, immigration, agriculture, tourism, health and national security.

This is critical as Latin American and Caribbean region is not insusceptible to cyber-attacks. In 2015, the OAS and Trend Micro released a report[[20]](#footnote-20) which highlighted the reality regarding attacks that negatively impact the critical infrastructure of the region. According to the Report, 44 percent of respondents reported being aware of different types of destructive attacks, while 40 percent said they had experienced attempts to shutdown cybernetic systems. In 2018, an updated report [[21]](#footnote-21) was released in collaboration with Microsoft, which indicated that 69 percent of respondents indicated they have noticed an increase in the number of attacks to their computer systems and/or networks over the last 12 months, and 57 percent of the respondents indicated they did not have a dedicated budget for cybersecurity measures, even though in 59 percent of those respondents with a dedicated budget, indicated that their budgets have increased within the last year. This kind of data emphasizes the need to ensure that Critical Infrastructure is addressed directly because of the risk if left unattended.

# Priority Areas

Taking into account the state of cybersecurity readiness of Belize and the developmental goals for the coming years, this Strategy has identified three areas of priority which will be focused on for the next two years. The aim of these priority areas is to build the capacity of Belize to better address cybersecurity threats. Each area identified will include specific activities that address gaps such as the capability to identify and respond to cyber incidents. The other aim would be to increase the overall awareness of not only government personnel on threats and tools needed to counter them but the general citizenry. Additionally, recognizing the need to have a comprehensive legislative framework in place, the Strategy outlines critical steps that can be taken to better enable the legislative posture of Belize to address cybercrime as a security risk.

The following diagram summarizes the areas identified as priority for the Strategy.

# Implementation

Effective implementation can only be achieved if a governance and monitoring process that takes into account all stakeholders, their competencies and contributions is implemented. This collaboration between stakeholders, can take into account all the various areas that impact the successful implementation of the Strategy, this includes sourcing technical capability, budget, talent recruitment, international cooperation. Collaboration and information sharing should be mutually beneficial for all and take into account the objectives the Strategy is aiming to achieve. The diagram below outlines all the various factors that should be taken into account for the implementation and monitoring of the Strategy.

Figure 4-Inter-related considerations for implementing a NCS

## Governance Structure

The incredibly complex challenges inherent to cybersecurity require a whole- of-nation approach guided by multiple agencies and stakeholders. A Governance structure, therefore, is needed for the identification of roles and responsibilities and overall responsibility for the implementation of the areas of priorities identified in this document, as well as related national cybersecurity initiatives. This Strategy recognizes the need to take into account existing governance frameworks, for example, in relation to the areas identified that may require legislative changes, the responsible institutional actors will prepare and submit accordingly (i.e. the Office of the Attorney General and Office of the Solicitor General respectively).

It is essential in this regard to consider who will manage inter-institutional relationships, act as a national and international point of contact, communicate and provide an advisory role in general regulations, follow-up and evaluation of measures. As such this Strategy recommends, that **a National Cybersecurity Coordinator,** under the auspices of the National Security Council be appointed for the coordination of the implementation of actions identified in this Strategy. As a consultative body, the National Cybersecurity Task Force that was established for the development of the Strategy, should also be called upon on a periodic basis to provide advice on the areas of priorities identified in relation to their primary areas of responsibilities.

## Evaluation and Review

Finally, metrics to evaluate the effectiveness of the objectives and activities articulated in this Strategy is needed and as such an evaluation of the Strategy will be undertaken eighteen (18) months after its approval.

## 

# Annex I

## Areas of Priority

The realization of the strategic vision of this Strategy will be based on the strategic objectives below. These objectives and activities have been developed by identifying the most important focal points and articulating a timeline within which they should be completed, broken down as follows:

* Short-Term: 6 months
* Medium-Term: 1 year
* Long-Term: 2 years

### Area of Priority 1: Develop the National Legal Framework to adequately address cybersecurity threats

This component contemplates the review of the existing legal framework that impacts cybersecurity initiatives including legislation related to digital evidence, data protection, etc., with the goal of providing procedural tools for investigators and prosecutors of digital related crimes. Additionally, this priority recognizes the need to provide tools to end-users. Based on the interaction of all relevant stakeholders, minimum security standards must be defined to ensure effective prevention and to achieve a common understanding of current requirements.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Objectives** | | **Activities** | **Coordinating Institutions** | **Timeline** |
| 1. | Feasibility assessment of data retention/digital evidence regulation conducted | * 1. Conduct consultation with all relevant stakeholders with the view of identifying gaps and recommendations for drafting instructions for new legislation | **Lead:** PUC  **Partners:**  IT Service Providers Attorney General’s Ministry  CITO | **Medium Term** |
| 2. | Minimum security standards included for information systems used in critical infrastructure | 2.1 Identify critical information infrastructure for minimum standards – incidents response  2.2 Develop minimum security standards for information systems used in critical infrastructure – incidents response  2.3 Establish a working group with the mandate to review common threats and provide recommendation for standards according to industry. | **Lead**: PUC  **Partners:**  IT Service Providers  CITO  Central Bank  BEL  BWS  Energy  Transport  Health  Communication  Immigration  Tourism  National Security | **Long Term** |
| 3. | Drafting Instruction for Legislation to address cybercrime submitted to Cabinet for approval | 3.1 Establish a legal working group to provide recommendation for drafting instructions for a draft Cybercrime Bill  3.2 Consult with international organizations such as the Council of Europe and Organization of American States for technical assistance for the development of the Cybercrime Bill  3.3 National Security Council Secretariat (NSCS) to request AG to draft cybercrime bill and consult with key stakeholders for input | **Lead:** CITO  **Partners**: NSCS  Attorney General  National Security  PUC | **Medium Term** |
| 4. | Judiciary and Prosecutors sensitized on technical concepts, popular methods of cybercrime, technologies used in committing cybercrime, level of crime | 4.1 National Security Council Secretariat (NSCS) and Police Information Technology and Cyber Unit (PITCU) of Belize Police Department (BPD) to conduct Quarterly briefings  4.2 Consult/dialogue with judiciary for training needs  4.3 Organize training for the judiciary and prosecutors | **Lead:**  Belize Police Department (BPD)  **Partners:**  NSCS  Judiciary  Registrar General | **Medium Term** |
| 5. | Ministry of Foreign Affairs National Security & Attorney General’s Office participate in bilateral and multilateral international cybersecurity agreements | 5.1 Government to review the process for acceding to the Convention on Cybercrime (Budapest Convention)  5.2 Consider signing CARICOM Treaties and other bilateral and multilateral treaties (extradition and evidence sharing) as needed | **Lead:** NSCS  **Partner:** Ministry of Foreign Affairs  Attorney General | **Short Term** |
| 6. | Capacity of Police Information Technology and Cyber Unit (PITCU) of Belize Police Department (BPD) strengthened | 6.1 Source training in investigation of digital crimes  6.2 Leverage international and regional partners to access annual training (e.g. OAS Annual Summer Bootcamp)  6.3 Creation of a manual to provide guidance on:  (i) Evidence collection, (ii) evidence storage and (iii) first responders to a crime scene in digital evidence gathering | **Lead**:  Belize Police Department (BPD)  **Partner:**  Office of the Director of Public Prosecution  Ministry of Foreign Affairs  Attorney General | **Medium Term** |
| 7. | Tracking and Analysis of cybercrime incidents improved | 7.1 Update Belize Police Information Technology and Cyber Unit website to include cybercrime reporting.  7.2 Create an App for reporting cybercrimes e.g. cyberbullying | **Lead:** Belize Police Department (BPD)  **Partner**: CITO | **Medium Term** |

### Area of Priority 2: Develop a national capacity for incident response and critical information infrastructure protection

This component recognizes the need for national coordination of incidents but takes a phased approach to building key relationships with critical sectors such as financial sector. Additionally, it is necessary to build the capability to collect and analyze cyber security incident, alert, and threat information, in order to understand in close to real time the risk to networks, detect incidents, and take immediate actions to mitigate consequences. As such this Area of Priority seeks to ensure there is a continuous enhancement of incident response capabilities and Establish mechanisms and procedures to facilitate timely information sharing and action among stakeholders.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Objectives** | | **Activities** | **Coordinating Institutions** | **Timeline** |
| 1. | National information sharing mechanisms among key sectors developed | 1.1 Develop a dialogue with key sectors in a phased approach to adopt an information sharing protocol. e.g. Central Bank use of Traffic Light Protocol.  1.2 Identify a list of sectorial Cybersecurity Incident Response Teams (CIRT). | **Lead:** CITO  **Partner:** Central Bank  Multi-stakeholder Advisory Group | **Medium Term** |
| 2. | National CIRT developed and institutionalized | 2.1 Develop a roadmap for the establishment of a National CIRT.  2.2 Develop the framework for the CIRT.  2.3Train incident response personnel and develop strategic capacity. | **Lead:** CITO  **Partner:** PUC  Central Bank | **Short-Mid Term** |
| 3. | User-friendly mechanisms for citizens to report incidents developed | 3.1 Develop a publicly available reporting mechanism for citizens to report incidents.  3.2 Establish a Multi-stakeholder Advisory Group (community) focused on community awareness.  3.3 Implement a National Public awareness campaign to sensitize the public on the availability of the reporting tool | **Lead:** Belize Police Department (BPD) | **Medium Term** |
| 4. | International Cooperation and new partnerships established | 4.1 Identify International Partner agencies to help build capacity and collaborate on incidents such as:   * [CSIRTAmericas.org](file:///C:/Users/SICAadminrep/Desktop/CSIRTAmericas.org) * [LACNIC WARP](https://warp.lacnic.net/) * [Commonwealth Telecommunications Organisation](https://cto.int/) | **Lead:** CITO  **Partner:** PUC  **Partner: Central Bank** | **Short-Medium Term** |
| 5. | Measures to protect services defined as critical that are essential for the functioning of the economy established | 5.1 Conduct Risk/Threat Assessment and identify classify all technology assets which support critical information systems  5.2 Obtain full understanding of critical system and information availability requirements based on agency priorities and mandates  5.4 Develop incident response and recovery plans that facilitates the measurement, detection, mitigation, and monitoring of cyber incidents for critical assets.  5.5 Implement an awareness campaign on the importance of standards and their adoption to operators and owners of critical infrastructure | **Lead:** PUC  Central Bank  CITO  **Partner:** National Security – NSCSS | **Long Term** |

## Area of Priority 3: Implement measures to support Education, Awareness and Workforce Development in cybersecurity

The reality is that there are simply not enough skilled personnel available in cybersecurity, and if there is personnel most government employees utilize technology to perform their duties. Therefore, they need to be informed about the severe consequences that may arise from just one mistake. This component seeks to raise the level of national awareness as well, on key cybersecurity issues and focuses on specific messaging for targeted audiences. The importance of security awareness training in government cannot be overemphasized. Just as awareness training in the health sector can help improve the standard of living and avoid certain diseases, so security awareness mitigate consequences of cyber incidents. Everyone needs to have a clear understanding that cybersecurity is a shared responsibility.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Objectives** | | **Activities** | **Coordinating Institutions** | **Timeline** |
| 1. | Mapping of key stakeholders developed and targeted awareness campaigns implemented | 1.1 Undertake consultation with all relevant stakeholders including NGOs, educational institutions, etc. to determine needs of the various target groups for cybersecurity awareness (e.g. indigenous communities, parents, teachers, vulnerable groups, women, etc.)  1.2 Map various initiatives that exists that can be utilized for incorporating or delivering Cybersecurity awareness messaging  1.3 Implement awareness campaigns at the District and Village level taking into account cooperation with town councils, village councils and community councils. | **Lead:** PUC  **Partners:**  Belize Network of NGOs  ADAMScon  Ministry of Education, Ministry of National Security | **Medium Term** |
| 2. | The general public is sensitized, educated and empowered on relevant cybersecurity topics | 2.1 Prepare a Cyber Security Communication Strategy, with a view to improve communication to stakeholders on cyber threats and available tools.  2.2 Develop television ads, jingles and news clips on key cybersecurity messages (Phishing, Grooming, sextortion, Cyberbullying, Privacy ,sexting)  2.3 Issue public facing messages through mediums such as text blasts, with key cybersecurity messages  2.4 Organize competitions among youth, in areas such as visual art, digital, written focused on cybersecurity  2.5 Adopt international cybersecurity awareness messaging services such as Get Safe Online website or STOPTHINKCONNECT  2.6 Collaborate with internet service providers, such as, BTL and Speednet at Expos for distribution of printed cyber awareness information and train-the-trainer initiatives focused on messaging developed.  2.7 Put out information on Large LED TVS and Billboards with Cyber Awareness info and catchy lines such as #beinternet awesome | **Lead:** PUC  **Partners:**  ADAMScon  BTL  Speednet  Ministry of Education  National Security  BTL, Speed net and  CITO | **Short Term**  **Short Term**  **Short Term**  **Medium Term**  **Short Term**  **Long Term** |
| 3. | Youth educated on cybersecurity threats and tips to stay safe online | 3.1 National campaign that goes from the bottom up: include different languages target youths and issues facing them  3.2 Include cyber component to existing forums (e.g. ICT for girls) | **Lead:** Ministry of Education  **Partners:**  Local universities  High Schools  PUC | **Medium Term**  **Short-**  **Medium Term** |
| 4. | Impact of awareness campaigns measured | 4.1 Develop survey to measure the impact of the various awareness campaigns | **Lead:** NSCS  **Partners:**  Ministry of Education | **Long term** |

# Annex 2

## Cybersecurity Capacity Maturity Model for Nations (CMM) - Belize comparative table 2016 and 2018

In that regard the **Cybersecurity Capacity Maturity Model for Nations (CMM)[[22]](#footnote-22)** was implemented in 2016 and again in 2018 for Belize. The assessment tool is used to measure the level of maturity of a nation in regards to cybersecurity across five different dimensions (see sidebar “Dimensions of the Cybersecurity Maturity Model”.) Each dimension provides several indicators of cyber capacity (an average of 10 indicators per dimension) in order for a nation to understand the stage of maturity in each specific consideration. These indicators are measured across five levels of maturity: Start-up, Formative, Established, Strategic and Dynamic. The stages of maturity vary from an initial stage of maturity where a nation may have just begun to consider cybersecurity, through to a dynamic stage where a nation is able to quickly adapt to changes in the cybersecurity landscape, by balancing threat, vulnerability, risk, economic strategy or changing international needs, while at the same time improving its posture and readiness to face new threats.

**Dimensions of the Cybersecurity Maturity Model**

**Cybersecurity Policy and Strategy** Identifying whether countries have comprehensive national cybersecurity policies that identify stakeholders’ roles, responsibilities in order to ensure a coordinate and cohesive cybersecurity framework including their cyber defense outlook.

**Cyber Culture and Society** Understanding the different mind-sets in terms of cybersecurity (government, private sector and society), identifying national cybersecurity awareness campaigns and privacy policies, as well as how is the level of trust in the use of online services (e-government and e-commerce).

**Cybersecurity Education, Training, and Skills** Identifying the availability of training and education in cybersecurity and the availability of skilled labor force in this field.

**Legal and Regulatory Frameworks** Legislation related to information and communications technologies (ICT), privacy, human rights, data protection, as well as substantive and procedural cybercrime law.

**Standards, Organizations and Technologies** The adoption of standards, the presence of incident response teams and command and control centers, national infrastructure resilience, critical national infrastructure protection, crisis management, cybersecurity insurance, and digital redundancy.

| **Dimensions** | | | **2016** | **2018** |
| --- | --- | --- | --- | --- |
| **D1: Cybersecurity Policy and Strategy** | **1-1 National Cybersecurity Strategy** | Strategy Development | 1 | 2 |
| Organization | 1 | 2 |
| Content | 1 | 1 |
| **1-2 Incident Response** | Identification of Incidents | 2 | 2 |
| Organization | 1 | 2 |
| Coordination | 2 | 2 |
| Mode of Operation | N/A | 1 |
| **1-3 Critical Infrastructure (CI) Protection** | Identification | 2 | 1 |
| Organization | 1 | 2 |
| Risk Management and Response | 2 | 1 |
| **1-4 Crisis Management** | Crisis Management | 1 | 1 |
| **1-5 Cyber Defense** | Strategy | 1 | 1 |
| Organization | 1 | 1 |
| Coordination | 1 | 1 |
| **1-6 Communications Redundancy** | Communications Redundancy | 1 | 1 |
| **D2: Cyber Culture and Society** | **2-1 Cyber Security Mind-set** | Government | 2 | 2 |
| Private Sector | 2 | 2 |
| Users | 1 | 2 |
| **2-2 Trust and Confidence on the Internet** | User Trust and Confidence on the Internet | 2 | 2 |
| User Trust in E-government Services | 2 | 2 |
| User Trust in E-commerce Services | 2 | 2 |
| **2-3 User Understanding of Personal Information Protection Online** | User Understanding of Personal Information Protection Online | N/A | 1 |
| **2-4 Reporting Mechanisms** | Reporting Mechanisms | N/A | 2 |
| **2-5 Media and Social Media** | Media and Social Medi | N/A | 2 |
| **D3: Cybersecurity Education, Training and Skills** | **3-1 Awareness Raising** | Awareness Raising Programmes | 1 | 1 |
| Executive Awareness Raising | 2 | 2 |
| **3-2 Framework for Education** | Provision | 1 | 1 |
| Administration | 1 | 2 |
| **3-3 Framework for Professional Training** | Provision | 2 | 2 |
| Uptake | 2 | 2 |
| **D4: Legal and Regulatory Frameworks** | **4-1 Legal Frameworks** | Legislative frameworks for ICT Security | 2 | 2 |
| Privacy, Freedom of Speech and other Human Rights online | 2 | 2 |
| Data Protection Legislation | N/A | 1 |
| Child Protection Online | N/A | 1 |
| Consumer Protection Legislation | N/A | 1 |
| Intellectual Property Legislation | N/A | 1 |
| Substantive cybercrime Legislation | 2 | 2 |
| Procedural cybercrime Legislation | 1 | 1 |
| **4-2 Criminal Justice System** | Law enforcement | 2 | 2 |
| Prosecution | 1 | 1 |
| Courts | 2 | 1 |
| **4-3 Formal and Informal Cooperation Frameworks to Combat Cybercrime** | Formal Cooperation | N/A | 1 |
| Informal Cooperation | N/A | 2 |
| **D5: Standards, Organizations, and Technologies** | **5-1 Adherence to standards** | ICT Security Standards | 2 | 1 |
| Standards in Procurement | 1 | 1 |
| Standards in Software Development | 2 | 1 |
| **5-2 Internet Infrastructure Resilience** | Internet Infrastructure Resilience | 2 | 3 |
| **5-3 Software Quality** | Software Quality | N/A | 1 |
| **5.4 Technical Security Controls** | Technical Security Controls | N/A | 2 |
| **5.5 Cryptographic Controls** | Cryptographic Controls | N/A | 1 |
| **5-6 Cyber Security Marketplace** | Cyber Security Technologies | 2 | 2 |
| Cybercrime Insurance | 1 | 1 |
| **5-7 Responsible Disclosure** | Responsible Disclosure | 1 | 1 |

# Acknowledgement

It is important to acknowledge the contribution of the following entities for their dedication and participation in the development and successful completion of the Strategy:

Attorney General's Ministry

Belize Defence Force

Belize Police Department

Belize Telemedia Limited

Broadband

Central Bank of Belize

Central Information Technology Office

Chamber of Commerce

Cross Design Group Ltd.

Judiciary (Supreme Court)

Ministry of Education

Ministry of Home Affairs

National Security Council Secretariat

Police Information Technology Unit

Public Utilities Commission

XXXXXX

1. This includes threats or vulnerabilities in networks, computers, programs and data, flowing from or enabled by connection to digital infrastructure, information systems, or industrial control systems, the Internet, etc. Cyber risk is commonly defined as exposure to or the potential of harm or loss resulting from breaches of or attacks on information systems or infrastructure (RSA.com) [↑](#footnote-ref-1)
2. <http://tourism.gov.bz/nstmp/> [↑](#footnote-ref-2)
3. <http://cdn.gov.bz/mof.gov.bz/files/FINAL%20GSDS_March_30_2016.pdf> [↑](#footnote-ref-3)
4. <http://med.gov.bz/wp-content/uploads/2016/10/Horizon2030executivesummary.pdf> [↑](#footnote-ref-4)
5. <https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#36f3870c1c30> [↑](#footnote-ref-5)
6. <http://www.bco.gov.bz/docstation/com_docstation/39/national_security_and_defence_strategy_2017_2020.pdf> [↑](#footnote-ref-6)
7. Growth and Sustainable Development Strategy Belize 2016-2019 [↑](#footnote-ref-7)
8. <https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BZ> [↑](#footnote-ref-8)
9. Cybersecurity Capacity Maturity Model for Nations - <https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0> [↑](#footnote-ref-9)
10. <https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/> [↑](#footnote-ref-10)
11. <https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/> [↑](#footnote-ref-11)
12. IWF Belize Reporting Portal - https://report.iwf.org.uk/bz/ [↑](#footnote-ref-12)
13. <https://www.ambergristoday.com/news/2018/08/15/phishing-scams-targeting-belizean-public> [↑](#footnote-ref-13)
14. Cybersecurity- Are we ready in Latin America and the Caribbean 2016 Report <https://publications.iadb.org/en/cybersecurity-are-we-ready-latin-america-and-caribbean> [↑](#footnote-ref-14)
15. <http://www.belizelaw.org/web/lawadmin/index2.html> [↑](#footnote-ref-15)
16. <http://www.belizelaw.org/web/lawadmin/index2.html> [↑](#footnote-ref-16)
17. <http://www.belizelaw.org/web/lawadmin/index2.html> [↑](#footnote-ref-17)
18. <http://www.belizejudiciary.org/download/LAWS%20of%20Belize%20rev2011/Law%20s%20Update%202011/Data/VOLUME%2011/Cap%20229.01%20Interception%20of%20Communications%20Act.pdf> [↑](#footnote-ref-18)
19. <http://www.belizejudiciary.org/download/LAWS%20of%20Belize%20rev2011/Law%20s%20Update%202011/Data/VOLUME%206B/Cap%20103.01%20Mutual%20Legal%20Assistance%20in%20Criminal%20Matters%20(Belize-USA)%20Act.pdf> [↑](#footnote-ref-19)
20. Report on Cybersecurity and Critical Infrastructure in the Americas <https://www.sites.oas.org/cyber/Certs_Web/OAS-Trend%20Micro%20Report%20on%20Cybersecurity%20and%20CIP%20in%20the%20Americas.pdf> [↑](#footnote-ref-20)
21. <https://www.oas.org/es/sms/cicte/cipreport.pdf> [↑](#footnote-ref-21)
22. Cybersecurity Capacity Maturity Model for Nations (CMM) -Belize Summary Assessment – [Annex 2](#_Annex_2) [↑](#footnote-ref-22)