NATIONAL CYBERSECURITY STRATEGY

TOWARDS A SECURE CYBERSPACE

2020-2023

GOVERNMENT OF BELIZE

NATIONAL CYBERSECURITY STRATEGY

TOWARDS A SECURE CYBERSPACE 2020-2023

OAS | More rights for more people

CONTENTS

01

Executive Summary 7

Foreword 9

Glossary of Terms 11

Acronyms 12

Strategic Vision 12

Principles 12

Respect for and the promotion of fundamental rights 12

Government Led 12

Risk based approach 13

Shared responsibility 13

Fostering an environment for economic growth and innovation 13

International Cooperation 13

02

Introduction 14

National Context 15

Horizon 2030: The National Development Framework for Belize 15

National Security and Defence Strategy 2017-2020 16

Belize's Growth and Sustainable Development Strategy (GSDS) 2016-2019 16

Baseline Assessment 17

03

Current status of cybersecurity: An overview 18

Cybercrime 19

Legislative Framework 20

Critical Infrastructure 20

Priority Areas 21

Implementation 22

Governance Structure 23

Evaluation and Review 23

04

Annex I 24

Areas of Priority 24

Area of Priority 1: Develop the National Legal Framework to adequately address cybersecurity threats 24

Area of Priority 2: Develop a national capacity for incident response and critical information infrastructure protection 27

Area of Priority 3: Implement measures to support Education, Awareness and Workforce Development in cybersecurity 29

Annex 2 32

Cybersecurity Capacity Maturity Model for Nations (CMM) - Belize comparative table 2016 and 2018 32

Acknowledgement 35

NATIONAL CYBERSECURITY STRATEGY

TOWARDS A SECURE CYBERSPACE 2020-2023

EXECUTIVE SUMMARY

Cybersecurity impacts many actors within the public domain, including policymakers, the private sector, law enforcement, academia and civil society; therefore, a multi-stakeholder approach was used in the development of this Strategy. Cybersecurity risks[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. As our connectivity and dependence on Internet-based platforms and services increase, so do our vulnerabilities and exposure to cyber threats. While this growth has brought numerous opportunities for many nations, cyber threats have equally evolved in recent years. This reality, therefore, requires the development of public policies that seek to ensure an open and safe Internet for all.

Developed through a multi-stakeholder approach, through the establishment of an Inter-institutional Cybersecurity Task Force, the *National Cybersecurity Strategy* of Belize seeks to establish a vision to enhance the cybersecurity posture of Belize. Considering existing national plans and the level of connectivity of the nation, a tiered approach was used to develop concrete and measurable actions that can be taken to advance the capability of the nation to address cyber threats. As such, in the development of the National Cybersecurity Strategy, the level of connectivity to the Internet, as well as, the volume of cybercrimes that are committed in Belize were considered. These variables were also used to determine the scope of the problem, existing cybersecurity gaps, capacities and opportunities for public-private synergies in Belize.

In terms of connectivity, there has been a steady growth in the level of Internet penetration and connectivity .[2] The more connected people become the more avenues are open 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. With respect to cybercrime, the Police Information Technology and Cyber Unit (PITCU) the 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. The PITCU holds a partnership with the Internet Watch Foundation, which facilitates the international reporting and investigation of cases of child pornography[3].

Acknowledging the evolving dynamics of the cybersecurity landscape in Belize, the strategy addresses three priorities pillars and includes actionable objectives to be realized over a period of three (3) years:

Figure 1-Areas of Priority

It is essential to consider who or what entity will manage the inter-institutional relationships of Belize's cybersecurity landscape, act as a national and international point of contact to facilitate cooperation, provide an advisory role in the development of programmatic interventions, and perhaps most importantly, coordinate the execution, evaluation and reporting of the strategy's action plan. As such, this Strategy recommends, that a National Cybersecurity Coordinator, under the auspices of the Ministry of National Security be appointed for the coordination of the implementation of actions identified in this Strategy.

Finally, the Strategy recognizes the need to undertake a review of its achievements within eighteen (18) months of its approval.

FOREWORD

It is without a doubt that the fourth industrial revolution is here. In the words of Professor Klaus Schwab, Founder and Executive Chairman of the World Economic Forum:

"This Fourth Industrial Revolution is, however, fundamentally different. It is characterised by a range of new technologies that are fusing the physical, digital and biological worlds, impacting all disciplines, economies and industries, and even challenging ideas about what it means to be human. The resulting shifts and disruptions mean that we live in a time of great promise and great peril."

The Internet as a shared global resource encapsulates unimaginable possibilities. As we seek to improve the standard of living of our people, we must harness the potential of this tool to capitalize on the opportunities in the digital economy. However, this cannot be pursued in a vacuum, as securing our engagement online from the onset is a critical first step in ensuring we retain value in whatever digital investments are made.

Why would I say this? Cyberspace has also become the fifth domain, along with air, sea, land and space, requiring defence. With the increased frequency and sophistication of malicious cyber activities, as a developing nation we cannot afford to be complacent. In today's digital age, everyone should care about cybersecurity. With the advancement in mobile technology for example, many Belizeans are engaged online. Personal information on social media sites such as phone number, email address, home address, and credit/debit card numbers and other information like photos and opinions, etc. are being shared. Aside from social media sites, people share their details for business reasons, and many have no idea how their information would be used. Further, another challenge in this area is the global shortage of cybersecurity experts, and Belize is no exception.

With the above in mind, the strategic lines of action articulated in this document demonstrate, among other things, two main concepts:

1. We as a Government recognize our cybersecurity gaps and challenges BUT at the same time, we recognize that everything cannot be all fixed with a stroke of a pen and the articulation of this document, therefore, we have identified three (3) key priority areas to start our journey of building resiliency and protecting the Belizean people.

2. We also recognize that 'no man is an island' and this must be a national effort. Relying on, while cultivating our own homegrown talent, we will face this challenge recognizing the need to institutionalize processes that will improve our overall cyber hygiene.

I must conclude by stating that this National Cybersecurity Strategy demonstrates a commitment to strengthening Belize's capabilities and national coordination to mitigate the impact of cyber threats. It also recognizes the importance of having a strategic vision to address Cybersecurity.

I implore all Belizeans to embrace this new digital era with a consciousness that the protection of the Internet is a shared resource. On behalf of the Government and people of Belize, I take this opportunity to thank everyone that was engaged in the development process and contributed their time, knowledge and talent to make this national cybersecurity framework possible.

Hon. Michael Peyrefitte
Minister of National Security

GLOSSARY OF TERMS

For the purposes of this document:

Critical infrastructure: Includes those sectors whose assets, systems, and networks, whether physical or virtual, are considered so vital that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof.

Digital Assets: Is content that is stored digitally and has value.

Cyber Education: Includes technical and non-technical content at all levels to provide the knowledge and skills necessary to perform cybersecurity functions

Cyber Awareness: Involves providing information about existing threats and takes into account knowledge combined with attitudes and behaviors that serve to protect digital assets and citizens online.

Cybersecurity: Takes into account the continuous and planned activities at the political, legal, economic, educational, awareness raising and technical levels to manage risks in cyberspace to ensure the ensure the confidentiality, integrity and availability of digital assets

Cybercrime: Is a crime that either uses services or applications in cyberspace are to carry out a crime or are themselves the targets of crime

Cyber Incidents: An event or activity that is observable occurrence in a system and/or network that usually indicates some form of interference from an unauthorized source.

Cyber Attack: Is a malicious and deliberate attempt by an individual or organization to breach the information system of another individual or organization[4].

Electronic Evidence: Is the information and data of investigative value that is stored on or transmitted by an electronic device.

Cyber bullying: Is harassment carried out on the Internet, via social networks, video game chat, or instant messaging. This can include direct verbal or emotional abuse, exclusion from social groups, or spreading gossip and rumors, making public content that was intended to be private, embarrassing the victim by impersonating them on social media, Posting embarassing pictures, revenge porn.

Identity theft: is the use of someone's personal information without permission for financial gain. They may get loans, mortgages, or credit cards in the victim's name, or they may make use of the victim's health insurance. Or they may assume the victim's identity in order to avoid arrest.

Phishing: is the use of emails that appear to originate from a trusted source, in order to trick a user into entering valid credentials at a fake website. Typically the email and the web site looks like they are part of a bank the user is doing business with.

Revenge porn: is a form of cyber bullying where nude or sexual photos or videos of someone are publically posted. Often, sexual images exchanged during a relationship are posted by an angry ex when the relationship ends. Other times, accounts of celebrities are hacked and sexual images found there are posted. In a recent case, revenge porn was combined with politics, when the ex of a female politician gave sexual images to the organization of a political rival. The images were published, causing her to resign, which allowed the rival to run in the election to take her place. Another name for revenge porn is Non-Consensual Pornography (NCP).

ACRONYMS

BEL – Belize Electricity Limited
BWS – Belize Water Services
CITO – Central Information Technology Office
NSCS – National Security Council Secretariat
PUC – Public Utilities Commission
OAS– Organization of American States
CICTE– Inter-American Committee Against Terroism
PITCU– Police Information Technology and Cyber Unit
BPD–Belize Police Department
MNS– Ministry of National Security
ATM–Automated Teller Machine
IT–Information Technology
ICT– Information and Communication Technology

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[5] 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.

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[6], the National Growth and Sustainable Development Strategy 2016-2019[7], among others. The graphic below illustrates some of considerations and policies that were taken into account during the development of this Strategy:

Figure 2 - Cybersecurity

Horizon 2030: The National Development Framework for Belize

The Horizon 2030[8] 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[9].

National Security and Defence Strategy 2017-2020[10]

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 is 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 of 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[11]. 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 consider to determine the scope of the problem, cybersecurity capacities that exists was measured and finally, the volume of cybercrimes that are committed in Belize was taken into account.

In terms of connectivity, there has been a steady growth in the level of Internet penetration and connectivity[12]. 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).

Table 1

Year	Population	Users	% Penetration
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%

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)[13] 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[14]. 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[15].

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 an inter-institutional cybersecurity task force, led by the PUC, NSCS, CITO and comprising 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

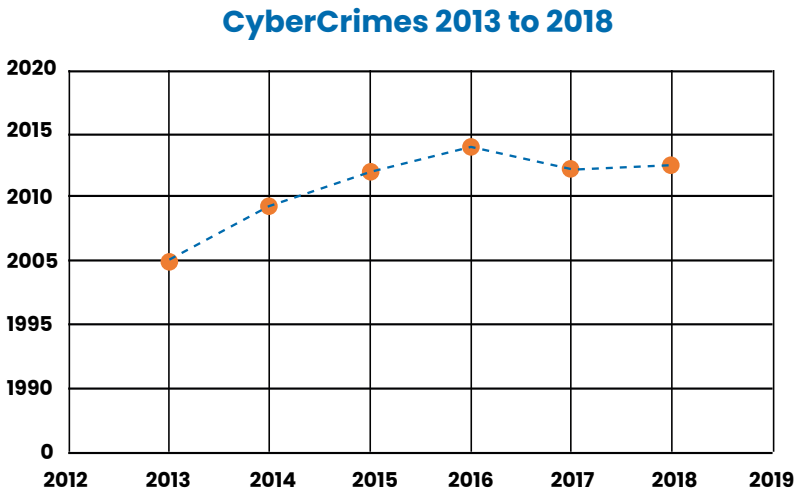
The Police Information Technology and Cyber Unit (PITCU) of Belize Police Department (BPD) manages the investigations of cyber-related crimes, as well as those felonies that involve electronic evidence. The PITCU has investigated cases of phishing, credit card and ATM fraud, as well as other crimes that involve electronic evidence, including drug trafficking. The PITCU have also reported that they have 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[16]. Below is a summary of cybercrimes recorded over the last five years.

Table 2

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 4 – Growth of Cybercrime - 5 year period



As recent as August 2018, it was reported that there were phishing scams targeting the Belizean Public[17]. 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 several legislations that relate to cybercrime[18]: the Telecommunications Act-CAP. 229 and 229S[19], the Electronic Evidence Act-CAP. 95:01[20], the Electronic Transactions Act-CAP. 29:01[21], the Intellectual Property Act, the Interception of Communications Act CAP. 229:01[22] and the Mutual Legal Assistance in Criminal Matters Act- CAP. 103:01[23]. 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, food security, banking and finance, communication, transportation, health and security. For instance, the protection of our democracy as a nation is paramount and in this digital age, the digital assets supporting our democratic processes could be considered a critical infrastructure, given the destabilizing impact on society that could occur if they are rendered inoperable or unreliable.

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[24] 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[25] 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

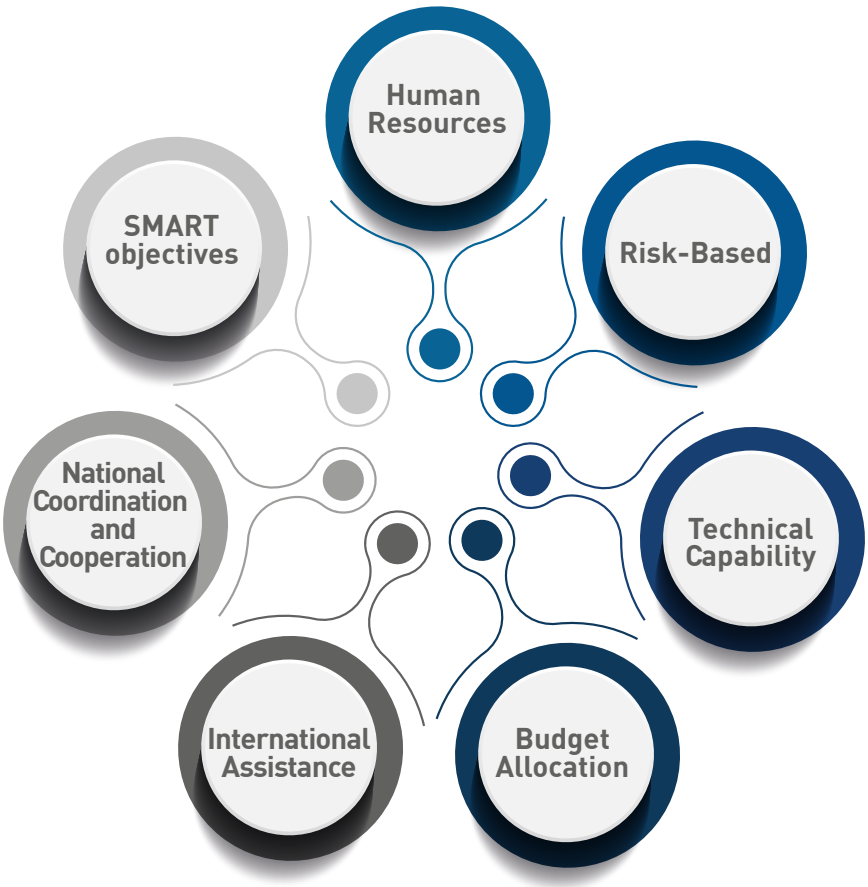
Taking into account the state of cybersecurity readiness of Belize and the developmental goals for the coming years, this Strategy has identified three areas of priority which will be focused on for the next four years. The aim of these priority areas is to build the capacity of Belize to better address 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 is 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 and sense of ownership by 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 5 – 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, partners 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 Ministry of National Security be appointed for the coordination of the implementation of actions identified in this Strategy. As a consultative body, the Inter-institutional 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 are needed and as such an evaluation of the Strategy will be undertaken eighteen (18) months after its approval.

ANNEX 1

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.

1 Objectives:

Feasibility assessment of data retenion/digital evidence regulation conducted

Activities:

1.1 Conduct consultation with all relevant stakeholders with the view of identifying gaps and recommendations for drafting instructions for new legislation

Coordinating Institutions:

Lead: PUC

Partners: IT Service Providers, Attorney General, CITO

Timeline:

Medium Term

2 Objectives:

Minimum security standards included for information systems used in critical infrastructure

Activities:

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.

Coordinating Institutions:

Lead: PUC

Partners: Ministries with responsibility for:

- Immigration
- Tourism
- National Security
- CITO

Central Bank Stakeholders from:

- BEL
- BWS
- Energy
- Transport
- Health
- Communication
- IT Service Provider

Timeline:

Long Term

3 Objectives:

Drafting Instruction for Legislation to address cybercrime submitted to Cabinet for approva

Activities:

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

Coordinating Institutions:

Lead: CITO

Partners: NSCS
Attorney General,
Ministry with responsibility for National Security,
PUC

Timeline:

Medium Term

4 Objectives:

Judiciary and Prosecu-tors sensitized on technical concepts, popular methods of cybercrime, technologies used in committing cybercrime, level of crime

Activities:

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

Coordinating Institutions:

Lead:
Belize Police Department (BPD)

Partners:
NSCS,
Judiciary,
Registrar General

Timeline:

Medium Term

5 Objectives:

Ministry of Foreign Affairs National Security & Attorney General's Office participate in bilateral and multilateral international cybersecurity agreements

Activities:

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

Coordinating Institutions:

Lead: NSCS
Partners: Ministry with responsibility for Foreign Affairs,
Attorney General

Timeline:

Short Term

6 Objectives:

Capacity of Police In-formation Technology and Cyber Unit (PITCU) of Belize Police De-partment (BPD)

Activities:

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

Coordinating Institutions:

Lead: Belize Police Department (BPD)
Partners:
Office of the Director of Public Prosecution,
Ministry with responsibility for Foreign Affairs,
Attorney General

Timeline:

Medium Term

7 Objectives:

Tracking and Analysis of cybercrime incidents improved

Activities:

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

Coordinating Institutions:

Lead: Belize Police Department (BPD)
Partners: CITO

Timeline:

Medium Term

Area of Priority 2:

Develop a national capacity for incident response and critical information infrastructure protection

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.

1 Objectives:

Feasibility assessment of data retenion/digital evidence regulation conducted

Activities:

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).

Coordinating Institutions:

Lead: CITO
Partners: Central Bank, Multi-stakeholder Advisory Group

Timeline:

Medium Term

2 Objectives:

Minimum security standards included for information systems used in critical infrastructure

Activities:

2.1 Develop a roadmap for the establishment of a National CIRT.
2.2 Develop the framework for the CIRT.
2.3 Train incident response personnel and develop strategic capacity.

Coordinating Institutions:

Lead: CITO
Partners: PUC, Central Bank

Timeline:

Short-Mid Term

3 Objectives:

User-friendly mechanisms for citizens to report incidents developed

Activities:

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

Coordinating Institutions:

Lead: Belize Police Department (BPD)

Timeline:

Medium Term

4 Objectives:

International Cooperation and new partnerships established

Activities:

4.1 Identify International Partner agencies to help build capacity and collaborate on incidents such as:

- CSIRTAmericas.org
- LACNIC WARP
- Commonwealth Telecommunications Organisation

Coordinating Institutions:

Lead: Belize Police Department (BPD)

Timeline:

Medium Term

5 Objectives:

Measures to protect services defined as critical that are essential for the functioning of the economy established

Activities:

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
5.3 Develop incident response and recovery plans that facilitates the measurement, detection, mitigation, and monitoring of cyber incidents for critical assets.
5.4 Implement an awareness campaign on the importance of standards and their adoption to operators and owners of critical infrastructure

Coordinating Institutions:

Lead:
Central Bank
CITO

Partner: Ministry with responsibility for National Security – NSCS

Timeline:

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. Additionally, the cybersecurity workforce is a diverse group of practitioners who govern, design, defend, analyze, administer, operate, and maintain the data, systems, and networks, therefore building a pool of talent in Belize, will serve to benefit the country as technology advances. 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. By promoting an awareness of digital rights, recognizing that this issue, if treated as a human right is a concern for everyone, efforts will be made to build campaigns to help the public understand that cybersecurity is a shared responsibility.

1 Objectives:

Initiatives and policies that supports the development of a cybersecurity workforce defend, analyze, administer and maintain the data, systems, and networks developed

Activities:

1.1 Review existing workforce development frameworks such as the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework to identify specialty areas, work roles, tasks, and knowledge, skills, and abilities needed to develop a national cybersecurity workforce survey

1.2 Undertake a cybersecurity workforce study using the survey to determine skills gap needed at the national level

1.3 Undertake consultation with universities including University of Belize and the University of the West Indies, to identify specific course curriculum needed based on cybersecurity workforce study results and create a national training catalog of cybersecurity related courses available nationally

1.4 Develop a national training/workforce development plan that leverages on existing educational of-ferings (certificates, degrees, etc.) and incorporates gaps identified in the cybersecurity workforce study

Coordinating Institutions:

Lead: Ministry with responsibility for Education and Technology

Partners: Belize Chamber of Commerce and Industry, University of Belize Association of Computing Machinery Student Chapter

Timeline:

Long Term

2 Objectives:

Mapping of key stakeholders developed and targeted awareness campaigns implemented

Activities:

2.1 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.)
2.2 Map various initiatives that exists that can be utilized for incorporating or delivering Cybersecurity awareness messaging
2.3 Implement awareness campaigns at the District and Village level taking into account cooperation with town councils, village councils and community councils.availability of the reporting tool

Coordinating Institutions:

Lead: Ministry with responsibility for Education and Technology
Partners: Belize Network of Non-Government Oraganizaitons, AdamsCon,
Ministry with responsibility for Education, Ministry with responsibility for National Security

Timeline:

Medium Term

3 Objectives:

The general public is sensitized, educated and empowered on relevant cybersecurity topics

Activities:

3.1 Prepare a Cyber Security Communication Strategy, with a view to improve communication to stakehold-ers on cyber threats and available tools.
3.2 Develop television ads, jingles and news clips on key cybersecurity messages (Phishing, Grooming, sextortion, Cyberbullying, Privacy, sexting)
3.3 Issue public facing messages through mediums such as text blasts, with key cybersecurity messages
3.4 Organize competitions among youth, in areas such as visual art, digital, written focused on cybersecurity
3.5 Adopt international cybersecurity awareness mes-saging services such as Get Safe Online website or STOPTHINKCONNECT
3.6 Collaborate with Internet service providers, such as, Digi and Speednet at Expos for distribution of printed cyber awareness information and train-the-trainer initiatives focused on messaging developed.
3.7 Put out information on Large LED TVS and Bill-boards with Cyber Awareness info and catchy lines such as #beInternet awesome

Coordinating Institutions:

Lead: Ministry with responsibility for Education and Technology
Partners:
ADAMScon
Speednet
Ministry with responsibility for Education, Ministry with responsibility for National Security
Digi, Speed net and
CITO

Timeline:

Short Term
Short Term
Short Term
Medium Term
Short Term
Long Term

4 Objectives:

Youth educated on cybersecurity threats and tips to stay safe online

Activities:

4.1 National campaign that goes from the bottom up: include different languages target youths and issues facing them

4.2 Include cyber component to existing forums (e.g. ICT for girls)

Coordinating Institutions:

Lead: Ministry with responsibility for Education

Partners:

Local universities

High Schools

NGOs

PUC

Timeline:

Medium Term

Short-Medium Term

5 Objectives:

International Cooperation and new partnerships established

Activities:

5.1 Develop a survey on level of awareness nationally to develop a baseline of the target group

5.2 Develop survey to measure the impact of the various awareness campaigns

Coordinating Institutions:

Lead: NSCS

Partners:

Ministry with responsibility for Education

Timeline:

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)**[26] 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.

BELIZE

D1 Política y Estrategia de Seguridad Cibernética

	2016	2020
1-1 Estrategia Nacional de Seguridad Cibernética		
Desarrollo de la Estrategia	1	2
Organización	1	2
Contenido	1	1
1-2 Respuesta a Incidentes		
Identificación de Incidentes	2	2
Organización	1	2
Coordinación	2	2
Modo de Operación	0	1
1-3 Protección de la Infraestructura Crítica (IC)		
Identificación	1	1
Organización	1	2
Gestión de Riesgos y Respuesta	1	1
1-4 Manejo de Crisis		
Manejo de Crisis	1	1
1-5 Defensa Cibernética		
Estrategia	1	1
Organización	1	1
Coordinación	1	1
1-6 Redundancia de Comunicaciones		
Redundancia de Comunicaciones	1	1

D2 Cultura Cibernética y Sociedad

	2016	2020
2-1 Mentalidad de Seguridad Cibernética		
Gobierno	2	2
Sector Privado	2	2
Usuarios	1	2
2-2 Confianza y Seguridad en Internet		
Confianza y Seguridad en el Internet del Usuario	2	2
Confianza del Usuario en los Servicios de Gobierno Electrónico	2	2
Confianza del Usuario en los Servicios de Comercio Electrónico	2	2
2-3 Comprensión del Usuario de la Protección de la Información en Línea		
Comprensión del Usuario de la Protección de Información Personal en Línea	0	1
2-4 Mecanismos de Denuncia		
Mecanismos de Denuncia	0	2
2-5 Medios y Redes Sociales		
Medios y Redes Sociales	0	2

D3

2016 | 2020

Formación, Capacitación y Habilidades de Seguridad Cibernética

3-1 Sensibilización

- Programas de Sensibilización
- Sensibilización Ejecutiva

3-2 Marco para la Formación

- Provisión
- Administración

3-3 Marco para la capacitación profesional

- Provisión
- Apropiación

D4

2016 | 2020

Marcos Legales y Regulatorios

4-1 Marcos Legales

- Marcos legislativos para la seguridad de las TIC
- Privacidad, libertad de expresión y otros derechos humanos en línea
- Legislación sobre protección de datos
- Protección infantil en línea
- Legislación de Protección al Consumidor
- Legislación de Propiedad Intelectual
- Legislación sustantiva contra el delito cibernético
- Legislación procesal contra el delito cibernético

4-2 Sistema de justicia penal

- Fuerzas del orden
- Enjuiciamiento
- Tribunales

4-3 Marcos de cooperación formales e informarles para combatir el delito cibernético

- Cooperación Formal
- Cooperación Informal

D5

2016 | 2020

Estándares, Organizaciones y Tecnologías

5-1 Cumplimiento de los Estándares

- Estándares de seguridad de las TIC
- Estándares en adquisiciones
- Estándares en el desarrollo de software

5-2 Resiliencia de la infraestructura de Internet

- Resiliencia de la infraestructura de Internet

5-3 Calidad del software

- Calidad del software

5-4 Controles técnicos de seguridad

- Controles técnicos de seguridad

5-5 Controles criptográficos

- Controles criptográficos

5-6 Mercado de Seguridad Cibernética

- Tecnologías de Seguridad Cibernética
- Seguro Cibernético

5-7 Divulgación Responsable

- Divulgación Responsable

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:

Belize Association of ICT Professionals

Belize Port Authority

Attorney General's Ministry

Belize Defence Force

Belize Police Department

Belize Telemedia Limited

Broadband Belize

Central Bank of Belize

Central Information Technology Office

Belize Chamber of Commerce and Industry

AdamsCon

Judiciary (Supreme Court)

Ministry of Education

Ministry of National Security

National Security Council Secretariat

Police Information Technology and Cyber Unit

Public Utilities Commission

FOOTNOTES

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)

2 - https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BZ

3 - IWF Belize Reporting Portal - https://report.iwf.org.uk/bz/

4 - https://www.cisco.com/c/en/us/products/security/common-cyberattacks.html

5 - 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)

6 - http://tourism.gov.bz/nstmp/

7 - http://cdn.gov.bz/mof.gov.bz/files/FINAL%20GSDS_March_30_2016.pdf

8 - http://med.gov.bz/wp-content/uploads/2016/10/Horizon2030executivesummary.pdf

9 - https://www.forbes.com/sites/martenmickos/2019/06/19/the-cybersecurity-skills-gap-wont-be-solved-in-a-classroom/#36f3870c1c30

10 - http://www.bco.gov.bz/docstation/com_docstation/39/national_security_and_defence_strategy_2017_2020.pdf

11 - Growth and Sustainable Development Strategy Belize 2016-2019

12 - https://data.worldbank.org/indicator/IT.NET.USER.ZS?locations=BZ

13 - Cybersecurity Capacity Maturity Model for Nations - https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cybersecurity-capacity-maturity-model-nations-cmm-0

14 – https://www.weforum.org/agenda/2019/01/addressing-the-growing-cybersecurity-skills-gap/

15 – https://www.weforum.org/agenda/2018/06/how-organizations-should-prepare-for-cyber-attacks-noam-erez/

16 – IWF Belize Reporting Portal - https://report.iwf.org.uk/bz/

17 – https://www.ambergristoday.com/news/2018/08/15/phishing-scams-targeting-belizean-public

18 – 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

19 – http://www.belizelaw.org/web/lawadmin/index2.html

20 – http://www.belizelaw.org/web/lawadmin/index2.html

21 – http://www.belizelaw.org/web/lawadmin/index2.html

22 – http://www.belizejudiciary.org/download/LAWS%20of%20Belize%20rev2011/Law%20s%20Update%202011/Data/VOLUME%2011/Cap%20229.01%20Interception%20of%20Communications%20Act.pdf

23 – 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

24 – 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

25 – https://www.oas.org/es/sms/cicte/cipreport.pdf

26 – Cybersecurity Capacity Maturity Model for Nations (CMM) -Belize Summary Assessment – Annex 2

NATIONAL CYBERSECURITY STRATEGY

TOWARDS A SECURE CYBERSPACE 2020-2023

OAS | More rights for more people

NATIONAL CYBERSECURITY STRATEGY

TOWARDS A SECURE CYBERSPACE

2020-2023