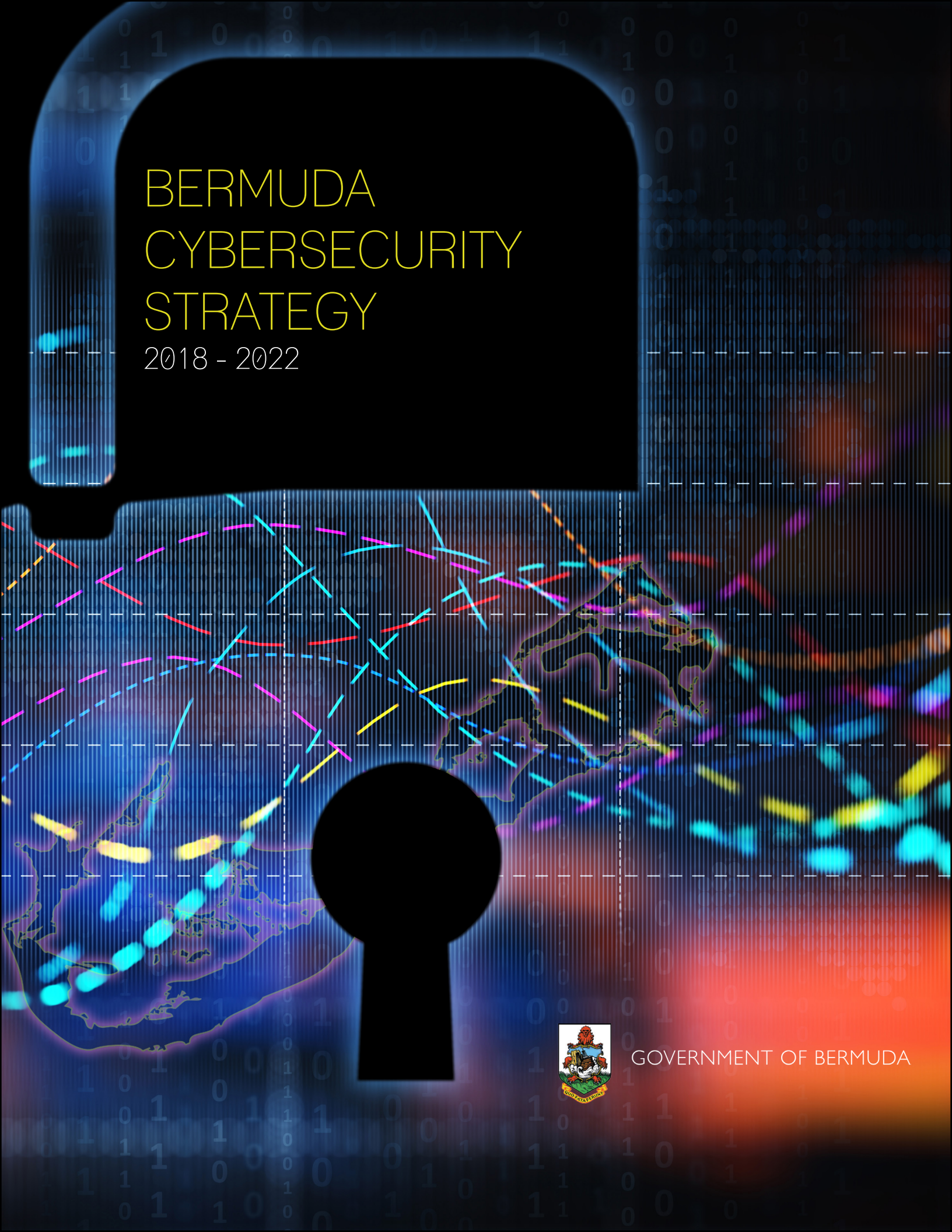
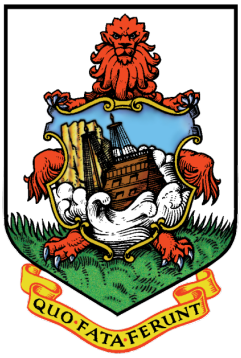


BERMUDA CYBERSECURITY STRATEGY

2018 - 2022

GOVERNMENT OF BERMUDA



BERMUDA CYBERSECURITY STRATEGY 2018 - 2022

CTO

Contents

A Message from the Premier
The Hon. David Burt, JP, MP.

At a time when the Internet continues to rapidly grow in importance by the day, Bermuda is an active and noteworthy player in the global economy, leveraging this tool for many purposes.

Online activity has become a daily part of life in Bermuda. It continues to change how business is managed and transactions are performed. A person from one part of the world can trade, learn from, and work with others from a completely different part of the world in a matter of nanoseconds. Here in Bermuda, the internet and its associated technologies have become the backbone of many transactions, whether with and among banks, government entities, schools and even charities, to name but a few.

The internet comes with many benefits but the risks are just as significant. Cyber-threats are growing as fast as the internet and the cost of a cyber-breach, as well as other implications, could be sizeable for individuals, organisations, and the jurisdiction as a whole.

Bermuda is an economy that leverages the Internet to enable its continued growth in a sustainable way that protects its assets and its global partnerships while guarding the information that the jurisdiction holds and processes. As such the Bermuda Cybersecurity Strategy 2018-2022 was established to develop and sustain a safe environment for anyone with an active online presence: any individual or organisation, who is based in Bermuda.

A Message from the Minister of National Security, the Hon. Wayne M. Caines, JP, MP.

The exchange of information is critical for our prosperity and well-being. Whether in business or in our personal lives, we are highly dependent on information technology to store, process and analyze information, and to communicate with our families, friends, business contacts around the world. It expands our capabilities and provides new opportunities for education, economic prosperity and improved quality of life.

As information technology continues to expand our horizons, opening up new opportunities, it also brings with it new and increasing risks. Cybercriminals seek to use our information and systems against us for their own economic gain. They trade in stolen personal information and use Ransomware and other forms of malware to extort money from individuals and businesses. Nation states engage in cyber-espionage for political and economic gain. Hacktivists deface websites, disrupt operations and expose sensitive confidential information to the world.

In order for Bermuda to continue its social and economic growth, we must ensure the Island is protected from cyber threats. Our critical national infrastructures, vital services and sensitive information must be defended against those who look to profit at our expense or who simply want to damage our pristine reputation as a business jurisdiction.

To that end, the Cybersecurity Governance Board has been established to oversee the implementation of Bermuda's National Cybersecurity Strategy. The Vision for Cybersecurity is attained through the following Strategic Goals:

1. Protect Bermuda's cyberspace,

2. Develop, enact and maintain appropriate legislation, regulation, policies and procedures to enhance cybersecurity and reduce cybercrime,

3. Promote cybersecurity awareness and capacity-building, and

4. Enhance local and international cybersecurity collaboration and co-operation.

With these goals in mind, this public/private partnership will guide the development and implementation of cybersecurity and cybercrime legislation. The Board will establish a National Computer Security Incident Response Team (CSIRT), facilitate threat-sharing and raise cybersecurity awareness across the jurisdiction. The Board will also support the development of educational programmes to build capacity and ensure Bermudians are prepared for the challenges and able to capitalise on the opportunities that lay ahead. Last but not least, the Board will leverage partnerships and external sources to assist where necessary.

The Government recognizes that is must set an example for the jurisdiction by ensuring it follows industry standards and generally accepted good practices for cybersecurity. To make sure that the Critical Information Infrastructures within Government are adequately protected, Cabinet has approved the Information Systems Risk Management Programme Policy. This policy requires the Government to implement and maintain a holistic, risk based cybersecurity programme that protects an organisation from end to end. This includes establishing policies, standards and procedures aligned with internationally recognized standards to secure Government information systems to protect individuals, the Government and Bermuda's reputation against cyber-threats.

I am confident that the steps we are taking will ensure Governments' and businesses' critical information infrastructures are protected, and just as importantly, our local and international community will know that Bermuda continues to be a safe and secure place to live and conduct business.

Executive Summary

The Government of Bermuda ("GoB" or "Government of Bermuda") recognises the major role that Information and Communication Technology ("ICT") plays to ensure growth in Bermuda. Over the last two decades, both private and public businesses across Bermuda have made ICT a key enabler of services and organisations are progressively leveraging ICT's benefits to provide effective, competitive services. Households are increasingly using ICT devices.

The GoB understands that Bermuda needs to be a safe harbour for conducting business, both physically and virtually. It needs to have a secure environment where technology supports economic growth and diversification. The Bermuda Cybersecurity Strategy 2018-2022 therefore takes a proactive approach aimed at maintaining a safe cyberspace for Bermuda, contributing to enhancing the Island's economic resilience while responding to both current and emerging cyber-threats.

The Strategy provides a roadmap for defending Bermuda's cyberspace and builds on several national development priorities identified in the *Speech from the Throne 2017* and the *2018-2019 Budget Statement*. The Strategy uses a sustained multi-stakeholder approach to enhance the collective ability of stakeholders to protect their ICT systems and data against the ever-evolving and borderless scourge of cyber-threats.

As Bermuda embarks on the process of strengthening its cybersecurity posture, the Strategy sets out the following core elements:

(i) The current status of cybersecurity in Bermuda, including both existing and emerging cyber-threats facing it;

(ii) The cybersecurity vision and strategic goals;

(iii) Principles that guide the implementation of the Strategy;

(iv) Roles and responsibilities of relevant stakeholders; and

(v) The methodology for implementing the Strategy and monitoring its progress.

Bermuda's Vision for Cybersecurity is:

A secure, resilient and trustworthy cyberspace that drives socio-economic development which fosters an informed and inclusive society in Bermuda

The Vision for Cybersecurity is attained through the four following Strategic Goals:

- *Strategic Goal 1*: Protect Bermuda's cyberspace
- *Strategic Goal 2*: Develop, enact and maintain appropriate legislation, regulation, policies and procedures to enhance cybersecurity and reduce cybercrime
- *Strategic Goal 3*: Promote cybersecurity awareness and capacity-building
- *Strategic Goal 4*: Enhance local and international cybersecurity collaboration and co-operation

This Strategy provides the appropriate framework for the Government of Bermuda to ensure that Information and Communications Technology (ICT) systems are integrated across all segments of our society and economy, in a safe and secure manner. In turn, this will enable economic diversification and augment Bermuda's prosperity and safety.

1. Introduction

ICTs have transformed people's lives and the way societies operate and have created numerous socio-economic opportunities. In many countries, public and private sectors and individual citizens have become increasingly reliant on ICTs for day-to-day activities. Bermuda is no different: having developed a supportive business legal framework and ICT infrastructure, the country is heavily dependent on technology.

The Government of Bermuda has recognised the need to diversify its economy and the critical role ICT plays in supporting this objective. Bermuda has, in recent years, implemented various measures to expand its economy and stimulate investment.

The need for economic diversification requires that it continue to embrace new technologies. Bermuda must also promote itself as a secure and prosperous environment for conducting business, both in-land and off-shore.

Bermuda's Cybersecurity Strategy describes the approach of the Government of Bermuda in creating a secure cyberspace, which will contribute to the country's economic resilience, responding to both current and emerging cyber-threats. This Strategy considers and builds on several national priorities for Bermuda which are outlined within the *Speech from the Throne 2017* and the *2018-2019 Budget Statement*. The Strategy has been developed through extensive consultation and is based on a multi-stakeholder approach.

This approach requires ongoing investment by all stakeholders to enhance their individual capabilities for protecting ICT systems and data from current and emerging cyber-threats.

1.1 Scope of Strategy

This Strategy describes a coherent, national approach for protecting Bermuda's data, information systems and network infrastructure from cyber-threats. It provides guidelines to all relevant stakeholders on their expected roles and responsibilities in achieving the national Vision and Strategic Objectives of this strategy.

Based on a multi-stakeholder approach, this strategy targets all sectors of Bermuda's economy and society including individuals, public and private sector organisations, academia and civil society organisations. It presents recommended actions to be undertaken across key focus areas identified in consultation with stakeholders.

This Strategy also underpins the international engagements undertaken by Bermuda within the context of ensuring a secure and resilient cyberspace.

The successful implementation of this Strategy will serve as a critical contribution towards achieving the benefits of economic diversification, using ICT, to support the prosperity and wellness of Bermuda's citizens.

To clearly outline the cybersecurity posture of Bermuda, the following core elements were considered:

(i) The current status of cybersecurity in Bermuda, including both existing and emerging cyber-threats facing the Island;

(ii) The cybersecurity vision and strategic goals

(iii) Principles that will guide the implementation of this Strategy;

(iv) Roles and responsibilities of relevant stakeholders; and

(v) The methodology to be followed for implementing the Strategy and monitoring its progress.

1.2 Strategy Context

Bermuda, while small in terms of land mass and with a population of just over 65,000[1] people, had an Internet penetration rate of 95.3% in 2017[2] which was one of the highest in the world. In the *State of ICT in Bermuda 2016* Report, 100% of businesses had Internet access and 90% of businesses had a disaster recovery or business continuity plan in place[3]. 99% of Bermuda residents and 97% of professionals believed that to compete in the global economy, Bermuda must continue to meet or exceed global technology standards. Similarly, 98% of residents and 96% of professionals believed that it was important for Bermuda to continue adopting new technology products and services to remain competitive. It is clear from the Report that ICT is viewed as an important enabler of economic development for individuals and organisations. However, there is a need for greater focus on cybersecurity.

Worldwide, there have been many real examples of cyber-attacks on private and public companies as well as on national infrastructure, which have resulted in significant financial loss or service impact. Locally, the Bermuda Police Service Financial Crime Unit has responsibility relating to fraud and cybercrime.

[1] https://data.worldbank.org/indicator/SP.POP.TOTL?locations=BM
[2] https://www.internetworldstats.com/top25.htm
[3] https://www.gov.bm/sites/default/files/7455-The-State-of-ICT-in-Bda-2016.pdf

While it is evident that cybersecurity events are occurring in Bermuda, there is a lack of information-sharing and established reporting mechanisms. Consequently, it is not clear how often these incidents occur nor the magnitude of their impact. It is therefore critical that Government and private industry work together to share information with the objective of minimizing risk.

Taking the above into consideration, the Government established a Cybersecurity sub-committee through the E-Commerce Advisory Board (ECAB) to assess cybersecurity risk management planning for Bermuda's Critical National Infrastructure (CNI) sectors including health, emergency services, transportation, energy, finance, food, communications and government services. During its work, the ECAB Cybersecurity sub-committee secured Private-sector input on the prevention, preparation, response and recovery from cyber-incidents.

The Cybersecurity Working Group was subsequently created with the mandate or providing strategic insight and recommendations pertaining to the protection of Bermuda's ICT infrastructure. It made several recommendations which included implementing security risk assessment for CNI entities, broadening the Department of ICT Policy and Innovation's Cybertips initiative to include cybersecurity awareness among the general population, building capacity within the Bermuda Police Service, and developing a National Cybersecurity Strategy for Bermuda.

1.2.1 Cyber-Threats and Vulnerabilities

Cybercrime continues to be a persistent threat to governments, businesses and citizens across the world, with Bermuda being no exception. Cybercrime is an evolution of traditional crimes and the rapid adoption of new technology which, coupled with the easy availability of cybercrime tools, has given rise to the number of attacks in recent years.

As is the case for other nations, those who commit cybercrimes within Bermuda's jurisdiction are not necessarily based on the Island. While the Bermuda Police Service does not have a dedicated cybercrime unit, there are IT intelligence officers and digital forensics officers within the Service. There is also recognition of the need for international cooperation with partners such as the National Crime Agency (NCA) in the United Kingdom and the Federal Bureau of Investigation (FBI) in the USA for best practices. Legislatively, one must recognise the limited scope of the Computer Misuse Act which was enacted over two decades ago and therefore does not adequately address the challenges of today's cyber-environment.

Apart from cybercriminals, Bermuda and Bermuda-based organisations are not immune to threats posed by insiders. Employees with access to critical organisational systems and data pose a significant threat as damage can be done either accidentally or deliberately. Employees can unintentionally cause harm especially when unaware of good cybersecurity practices.

Corporate and state-sponsored cyber-espionage has also been identified as a threat to Bermuda, a low-tax jurisdiction that has attracted hundreds of international companies. As Bermuda moves to diversify its economy and looks towards new and emerging technologies and initiatives including FinTech and distributed ledger technologies, there is a need to consider its exposure to related vulnerabilities and risks. With the rise of the Internet of Things, more data is being created and transmitted, which presents new opportunities for compromise as the increased volume of data available across networks means that the risk of breaches is greater for organisations.

Bermuda must therefore implement good practices and procedures across all segments of society to address current and emerging vulnerabilities. Most cyber-attacks involve the exploitation of known but unmitigated vulnerabilities. Bermuda needs to take the necessary actions to encourage individuals and institutions to invest in tools and training and to take adequate measures to address identified vulnerabilities. Investments must focus on key areas including technology, individuals and governance.

1.3 Cybersecurity Capacity Review

In March 2018, with assistance from the Commonwealth Telecommunications Organisation (CTO), Bermuda conducted a cybersecurity capacity assessment for the country. The assessment was based on a Cybersecurity Capacity Maturity Model (CMM) developed by the CTO's implementing partner University of Oxford's Oxford Martin School. The model was used to assess the cybersecurity maturity level for Bermuda based on five key dimensions:

(i) Policy & Strategy;

(ii) Culture & Society;

(iii) Education, Training & Skills;

(iv) Legal & Regulatory Frameworks; and

(v) Standards, Organisations, & Technologies.

In addition, the model enabled stakeholders in Bermuda to identify gaps, challenges and opportunities that Bermuda needed to consider to address in this strategy.

In the following sub-section, this Strategy outlines some of the key findings of the CMM assessment.

1.3.1 Summary of the Key Findings of the Assessment

(i) Bermuda organisations recognise that cybersecurity is a key issue in its drive to embrace future technologies for economic diversification; however, there is no overarching national cybersecurity programme for the country.

(ii) Bermuda does not have a formal framework for monitoring cyber-threats and for preventing, detecting, and mitigating against cyber-attacks.

(iii) Bermuda has identified Critical National Infrastructure entities (CNIs) but has not categorised their respective Critical Information Infrastructures (CII). Also, the list of CNIs is not yet formally approved. There is no formal collaboration framework between CII operators and owners and the Public Sector. In addition, there is no national risk management framework and contingency plans against cyber-attacks to ensure the resiliency of CIIs.

(iv) Bermuda does not have sufficiently adequate and effective legislation, policies and regulations on cybersecurity to address both current and future cybersecurity threats. There currently exists the Computer Misuse Act 1996 though its scope is limited and needs updating.

(v) While the Personal Information Protection Act 2016 is in place, it has not been fully implemented yet.

(vi) There is inadequate training capacity and lack of specialised expertise in cybersecurity.

(vii) There is limited ability to prosecute cybercrimes. Mutual legal assistance for cybercrime has also proven challenging.

(viii) There is awareness for the use of standards in cybersecurity. However, it is not mandated and there is no form of national coordination on it.

a. Bermuda Cybersecurity Strategy Alignment with the National Agenda

Bermuda's Cybersecurity Strategy is aligned with the objectives and aspirations of the national agenda of Bermuda as described below:

(i) The 2017 Speech from the Throne called for a focus on cybersecurity and on ensuring that digital infrastructure is protected and safe.

(ii) 2018/19 Budget Statement reflected the importance of cybersecurity and of emerging technologies.

In addition to the above national guiding documents, this Strategy is aligned with the following CARICOM Frameworks, given Bermuda's affiliate membership status within that community:

(i) CARICOM Crime and Security Strategy 2013 identifies and prioritises the common security risks and threats which CARICOM is facing and is likely to face in the future. It articulates an integrated and cohesive security framework to confront these challenges and guides the coordinated internal and external crime and security policies adopted by CARICOM Member States. The Strategy identifies cybercrime as a "Tier 1 risk and threat" meaning it is of high-probability and high-impact.

(ii) CARICOM Cybersecurity and Cybercrime Action Plan seeks to address the cybersecurity vulnerabilities in each participating Caribbean country and to establish a practical, harmonised standard of practices, systems and expertise for cybersecurity, to which each Caribbean country could aspire in the short and medium terms. It also seeks to build the required capacity and infrastructure to allow for the timely detection, investigation and prosecution of cybercrime and possible linkages to other forms of criminal activity.

b. Cybersecurity Legislation in Bermuda

There may be a need for new cybersecurity legislation and/or regulations to support the strategy. In addition, the following pieces of existing legislation will have to be assessed and updated where appropriate:

(i) Computer Misuse Act 1996: this law criminalises offences such as unauthorised access to computer systems and gives police powers of arrest without a warrant should there be reasonable cause to suspect an offence was committed.

(ii) Electronic Transactions Act (ETA) 1999: The ETA gives legal recognition to electronic records. It provides that information shall not be denied legal effect, validity, admissibility or enforceability solely on the ground that it is in the form of an electronic record. It also addresses various elements of e-commerce such as legal requirements for electronic records including delivery, electronic signatures and certification and standards for electronic transactions to protect consumers and businesses.

(iii) Public Access to Information Act (PATI) 2010: PATI allows citizens and residents to ask a public authority for records to help them understand the work that goes on in the public authority and how it makes decisions.

This makes the entire government more accountable and removes unnecessary secrecy.

(iv) Electronic Communications Act 2011: this law encourages the development and maintenance of resilient and fault-tolerant communications infrastructures and promotes investment in the electronic communications sector and in communications-reliant industries.

(v) Personal Information Protection Act (PIPA) 2016: PIPA has been enacted to impose on data custodians' requirements for protecting personal data. The scope of the work discussed below pertains to cybersecurity events in general whether or not a data breach has occurred.

(vi) Virtual Currencies Business Act 2018: The comprehensive legislation covers the issuing, selling or redeeming of tokens and cryptocurrencies, Initial Coin Offerings (ICO), crypto exchanges, crypto wallets and other crypto service vendors. The Act includes extensive consumer protection so that the BMA can protect its citizens and has enough regulation that allows the ecosystem to flourish in an evolving environment.

(vii) Digital Assets Business Act (DABA) 2018: DABA introduces a supervisory framework for the Bermuda Monetary Authority to regulate persons carrying on digital asset business and for the

protection of the interests of clients or potential clients of persons carrying on the business of digital asset business.

(viii) Initial Coin Offerings Amendment Act 2018: The amended Act treats ICOs as restricted business activities that will require the consent of Bermuda's Minister of Finance prior to an offering being made to the public (an "ICO offering"). The ICO Act regulates all aspects of offering digital assets to the public as a means for a Bermuda company to raise capital.

2. Strategy Approach

Bermuda's National Vision for cybersecurity, together with the core elements of Bermuda's approach for managing the numerous cyber-threats, is outlined in the following sub-sections.

2.1 Vision Statement

A secure, resilient and trustworthy cyberspace that drives socio-economic development which fosters an informed and inclusive society in Bermuda

2.2 Strategic Goals

Bermuda aims to achieve its Vision for Cybersecurity through the attainment of the following four Strategic Goals:

- *Strategic Goal 1*: Protect Bermuda's cyberspace.
- *Strategic Goal 2*: Develop enact and maintain appropriate legislation, regulation, policies and procedures to enhance cybersecurity and reduce cybercrime.
- *Strategic Goal 3*: Promote cybersecurity awareness and capacity building.
- *Strategic Goal 4*: Enhance local and international cybersecurity collaboration and co-operation.

2.3 Guiding Principles

The execution of Bermuda's Strategy will be underpinned by the following principles:

1. ***The rule of law:*** This Strategy will be implemented in accordance with the laws recognized in Bermuda and enshrined in the Bermuda Constitution Order 1968 which protects the fundamental rights and freedoms of all citizens. It will also be implemented in accordance with international instruments which Bermuda has ascended to.

2. ***Shared responsibility:*** The Strategy outlines the roles and responsibilities of individuals and organisations for the protection of systems, networks and data and ensures they are fulfilled. The Strategy will also provide a framework that will drive collaboration and cooperation in this regard.

3. ***Risk-Based approach:*** This Strategy will promote the application of a risk-based approach for managing cyber-threats for prioritising and executing cyber-related activities by individuals and organisations.

4. ***Access to the Internet and cyberspace:*** The Strategy articulates Bermuda's dedication to ensuring access to a safe and secure cyberspace.

5. ***ICT as a key enabler:*** The Strategy will support the digital and economic transformation of Bermuda by ensuring that cybersecurity becomes an integral consideration of all strategies, programmes and capabilities deployed.

6. ***Proactive Action:*** The Strategy details Bermuda's commitment to proactively manage the rapidly-evolving cyber-threat landscape and to ensure individuals and organisations protect their systems, networks and data.

3. Achieving Bermuda's Strategic Goals

The following section outlines the strategic goals, specific objectives, and actions which must be achieved and executed to enable the attainment of Bermuda's national Vision on Cybersecurity 2018-2022. They will be executed in a manner that is consistent with the principles described above.

3.1 Strategic Goal 1: Protect Bermuda's Cyberspace

Effective cybersecurity ensures system availability, integrity, authenticity, confidentiality and non-repudiation. That in effect addresses privacy and enhances trust in related systems, which is vital for encouraging and promoting the use of new technologies.

Bermuda is embarking on a journey of economic diversification and in doing so is embracing ICT to transform its economy and society. Therefore, there is a critical need to secure networks and systems: should there be an attack on critical networks and systems, the country would be severely impacted, particularly from an economic outlook. It is crucial that Bermuda not only identify and address new and existing vulnerabilities to critical systems and infrastructure, but also develop and enforce common standards to secure ICT infrastructure and services, including data repositories. There is a need to promote collaboration and information-sharing among all stakeholders and to ensure coordinated efforts to mitigate and respond to incidents targeting CIIs.

3.1.1 Specific Objective 1.1: Establish a Cybersecurity Governance Structure

To effectively manage Bermuda's response to constantly-evolving cyber-threats and to coordinate the various entities with perceived overlapping authority for the management of these issues, there must be an overarching authority to monitor and oversee all stakeholders. While there currently exists a Cybersecurity Working Group and an E-Commerce Advisory Board, the Working Group should ideally be strengthened to create a formal governance structure which will manage cybersecurity and deliver an effective and coordinated response to all activities.

This body will act as a sustainable structure which can evolve to meet the dynamic realities of cyberspace. It will also allow Bermuda to provide effective governance and leadership on cybersecurity issues and to avoid duplication of efforts.

Actions:

3.1.1.1 Develop legislation which creates the Cybersecurity Governance Board and prescribes the roles, responsibilities and authority for the board.

3.1.1.2 Appoint and operationalise the Cybersecurity Governance Board reporting to the relevant Minister.

3.1.1.3 Develop an implementation, operational and financial plan for the Cybersecurity Governance Board.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.1.1.4 Bermuda will have a cybersecurity governance body which ensures the implementation of a joined-up, national approach for executing cyber-related activities and initiatives across Bermuda.

On-going Initiatives:

Objective 1.1 - Establish a Cybersecurity Governance Structure.

3.1.1.5 There currently exists a Cybersecurity Working Group (CWG) to oversee the development of the current cybersecurity strategy and to advise Cabinet Cybersecurity Committee. The CWG will provide interim governance functions however there may be a need to revisit the membership of the CWG to ensure it is inclusive of all relevant stakeholders.

3.1.1.6 The E-Commerce Advisory Board (ECAB), will also contribute to the above actions in the interim.

3.1.2 Specific Objective 1.2: Identify and protect the critical information infrastructures (CIIs) of Bermuda

Undoubtedly, the Government of Bermuda appreciates the importance of securing its Critical Information Infrastructures (CIIs) which are sub-elements of Critical National Infrastructure (CNI).

Bermuda has begun the process of identifying and classifying its CNIs, deemed to be assets of unique national importance and the loss of which would have national long-term effects and devastating impact on other sectors. There exists a coordination mechanism for disaster management: the Emergency Measures Organisation (EMO). Steps are being taken to draft and enact comprehensive disaster management legislation which will identify and protect CNIs. Existing coordination mechanisms will be strengthened as it is vital to also protect those interconnected information infrastructures (CIIs) which underpin these CNI.

Bermuda will ensure that the public and private organisations which own and operate Critical Information Infrastructure (CII) are able to monitor, detect and manage vulnerabilities and threats to their ICT systems, network and data. Bermuda will also seek to enhance understanding of such threats and vulnerabilities to CIIs and to ensure that measures are implemented to boost their resilience and security.

Actions:

3.1.2.1 Develop and enact comprehensive disaster management legislation which includes detailed provisions relating to the protection of CNI and CII.

3.1.2.2 Develop risk and vulnerability registers and regulations which promote continuous monitoring and risk management across all CIIs.

3.1.2.3 Develop a National CII Governance Framework which would consist of processes, policies, guidelines, good practices, standards, etc. and would be adhered to by CII operators and owners.

3.1.2.4 Undertake continuous monitoring and testing of CII to detect vulnerabilities, risks, threats, etc.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.1.2.5 The Government of Bermuda and CII operators/owners stay up-to-date with and in full understanding of the risks, vulnerabilities, threats and levels of cybersecurity across all of Bermuda's CII. They can therefore develop/deploy the appropriate capacity to ensure the cybersecurity of CII.

3.1.2.6 There is enhanced resilience and security of CII across Bermuda.

On-going Initiatives:

Objective 1.2.1 – develop and enact comprehensive disaster management legislation which includes detailed provisions relating to CNI and CII.

3.1.2.7 National Disaster Coordinator (NDC) – comprehensive Disaster Management legislation is currently being drafted which will identify CNI.

3.1.2.8 The Royal Bermuda Regiment (RBR) has a listing of all key point infrastructure which will need to be reviewed and updated.

Objective 1.2.2 – develop risk and vulnerability registers and regulations which promote continuous monitoring and risk management across all CIIs.

3.1.2.9 The Emergency Measures Organisation (EMO) is already established and has a process in place to meet and coordinate when national emergency/disasters occur.

3.1.3 Specific Objective 1.3: Establish a Bermuda Computer Security Incident Response Team (CSIR)

To secure and strengthen its CII, Bermuda will ensure that coordinated efforts are taken to mitigate and/or respond to incidents in a rapid and effective manner. To accomplish this, there is a requirement to establish an organisation which can serve as the national focal point for incident cautions, reporting, management and response.

The Computer Security Incident Response Team (CSIRT) will not be created as a unit to perform a law enforcement role - though it will be able to support the Bermuda Police Service, should it be necessary. It

will perform functions such as dissemination of cybersecurity information and best practices, lead national recovery efforts in the event of a cyber-incident, and analyse cyber-vulnerabilities, incidents and attack methodologies.

Bermuda will also seek the assistance of the International Telecommunication Union (ITU) in conducting a CSIRT readiness assessment, the results of which will provide a comprehensive situational analysis of Bermuda's ability to respond to incidents. It will also submit guidelines on how to establish a CSIRT.

Actions:

3.1.3.1 Conduct a CSIRT readiness assessment.

3.1.3.2 Review existing regulations and legislation to determine current mandatory CSIRT functions, including information request capability.

3.1.3.3 Develop and enact legislation to establish a National CSIRT. The law should specify roles, responsibilities and ownership.

3.1.3.4 Establish and operationalise the Bermuda CSIRT.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.1.3.5 Bermuda has established a centralised institution for incident response and reporting. As a result, cyber-threat incidents across the island are regularly reported and accurately documented, enabling the effective management of cyber-incidents nationwide.

On-going Initiatives:

Objective 1.3.1 – conduct a CSIRT readiness assessment.

3.1.3.6 The ITU has been contacted to discuss requirements for entering into a partnership to potentially conduct a CSIRT readiness assessment in Bermuda.

Objective 1.3.2 - review existing regulations and legislation to determine current mandatory CSIRT functions, including information request capability.

3.1.3.7 The Bermuda Police Service (BPS) has the foundation that can respond to a basic incident. It includes basic training and equipment (computer forensics).

3.1.4 Specific Objective 1.4: Establish a framework to manage cyber-threats

Bermuda needs to identify and classify cyber-threats, enhance cyber-threat management, and provide support to organisations across all sectors on how to manage threats. This will involve, among other things, the gathering and dissemination of information about current and emerging cyber-threats nationwide. That function can be supported by the operationalisation of the Bermuda CSIRT.

Action

3.1.4.1 Develop and implement an incident reporting, incident response, and information-sharing framework.

3.1.4.2 Define, publish and continuously review the minimum incident register requirements to enable dependable incident analysis against a rapidly-evolving cyber-landscape.

3.1.4.3 Develop and continuously update cyber-incident scenarios and cyber-contingency plans that clearly define crisis management procedures. Such procedures would include the roles and responsibilities of all stakeholders during cyber-incidents and emergencies and can be used during cyber-exercises.

3.1.4.4 Conduct regular cyber-drills and exercises to test national crisis management measures and leverage lessons learned to improve crisis management measures and the national response to cyber-incidents.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.1.4.5 Bermuda has a detailed understanding of the cyber-threats facing it and as such has executed a joined-up, national approach to addressing cyber-threats and incidents.

On-going Initiatives:

Objective 1.4.1 – develop and implement a threat sharing framework.

3.1.4.6 Bermuda has enacted the Personal Information Protection Act (PIPA) 2016 which requires any organisation to notify the Privacy Commissioner of data loss involving personal details.

3.1.4.7 There are plans to align PIPA with GDPR.

3.1.5 Specific Objective 1.5: Establish and promote the adoption of appropriate technology, standards and good practices in cybersecurity

Bermuda will ensure that cybersecurity standards, guidelines, and technical and operational frameworks are developed, published and deployed nationwide.

These frameworks will be based on good cybersecurity practices and measures. They will ensure that both public and private organisations, including citizens, understand their responsibilities in securing their data, information systems and networks. They will also support and enhance ongoing work by the Government to deliver workshops which raise awareness on security and risk assessments. Bermuda will ensure that these standards, guidelines, technical and operational frameworks are tailored to national specifications that will enhance the cybersecurity posture of the country, especially with respect to the CIIs and ICT services.

Actions:

3.1.5.1 Develop and promote the adoption of appropriate standards and technology for cybersecurity.

3.1.5.2 Deploy Public Key Infrastructure (PKI) or related technologies Island-wide especially in e-government services to leverage the security features relating to confidentiality, authentication and data integrity.

3.2 Strategic Goal 2: Develop, enact and maintain appropriate legislation, regulation, policy and procedures to enhance cybersecurity and reduce cybercrime

A robust legal and regulatory framework is required to ensure that all organisations and citizens can enjoy the benefits of the digital environment in accordance with human rights, protecting the privacy of users and criminalising attacks in cyberspace. Bermuda needs to update and continuously review its legal and regulatory frameworks as they will provide all relevant stakeholders with the tools needed to effectively promote and strengthen cybersecurity and investigate and prosecute cyber-crimes.

It is important that Bermuda's established legal and regulatory cybersecurity framework is suitably-applicable and technology-neutral to enable Bermuda to tackle emerging cyber-threats effectively whilst still allowing innovation and growth in the ICT sector.

3.2.1 Specific Objective 2.1: Develop and maintain appropriate legislation, regulations, policies and procedures to meet current and future challenges

Bermuda will ensure it has a well-defined legal framework which establishes and maintains order and security for users of the electronic environment and which sanctions those who deliberately cause damage to computers, electronic networks and other critical information infrastructure. In reviewing and updating its legal framework, Bermuda will consider all relevant pieces of legislation to strengthen provisions addressing various cybersecurity issues. Instruments will be aligned to regional and international norms, thereby criminalising malicious cyber-activities in Bermuda and improving the investigation and prosecution of cybercrimes by ensuring that law enforcement and prosecutors have access to tools which enable them to do their jobs efficiently.

Bermuda will also undertake periodic reviews of existing laws, regulations, policies and procedures to ensure that the provisions adequately meet and adapt to the current and future cyber-landscape while ensuring harmonisation and compliance, where necessary, with other policies, laws and regulations that exist within the region or globally.

Actions:

3.2.1.1 Undertake a gap analysis of all existing and relevant legislation, regulations, policies and procedures related to cybersecurity.

3.2.1.2 Amend and create appropriate and relevant instruments identified by the gap analysis.

3.2.1.3 Create or amend legislation to adequately address cybercrime.

3.2.1.4 Review and enhance existing legal and regulatory frameworks to support innovation and the use of new technologies.

3.2.1.5 Conduct periodic reviews of legislation, regulations, policies and procedures.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.2.1.6 Bermuda has established a current and forward-looking legal and regulatory framework, which takes into account the continuously-evolving cyber-threat landscape and cybersecurity trends and strengthens Bermuda's capacity to protect its systems, networks and data.

3.2.1.7 Bermuda has the capacity to effectively implement the various comprehensive cybercrime provisions of its legal and regulatory framework, thereby enhancing Bermuda's ability to combat cybercrime.

3.3 Strategic Goal 3: Promote cybersecurity awareness and ensure capacity building

In order to effectively promote a safe and secure cyberspace, Bermuda is cognisant that there needs to be increased awareness at the national level. As such, the Government will assume a leadership role in promoting cyber-awareness and building capacity across all sectors. For this to be achieved, Bermuda will adopt a multi-disciplinary and multi-stakeholder approach which will seek to embed cybersecurity in education and in wider aspects of policy formulation.

A key aspect of this Strategy is also ensuring that Bermuda creates the skills and human technical capacity required for driving the digital and economic transformation of the country. This will be key not only to foster an innovative environment, but also to ensure that there is adequate human capacity to mitigate cyber-threats and to address cyber-incidents across the public and private sector.

Specific Objective 3.3.1: Raise national cybersecurity awareness

Bermuda has already taken significant steps to promote cybersecurity awareness among citizens and residents. The Cybertips programme provides practical tips, resources and contacts to help the community to use the Internet safely and to be on guard against online predators, cyberbullying, and inappropriate online content. The Cybertips team routinely visits schools to speak to students, teachers, and Parent-Teacher Associations about the importance of good digital citizenship and gives tips on how to develop a clean digital reputation.

Bermuda will ensure that this programme is enriched and expanded to ensure that cybersecurity awareness is enhanced across as wide an audience as possible and in the most effective and inclusive way feasible. Bermuda will also continue to recognise international days dedicated to cybersecurity and to host special events on those days.

Actions:

3.3.1.1 Build upon and expand the scope of existing Cybersafety programmes.

3.3.1.2 Establish a cybersecurity awareness and collaboration framework targeting private, public and civil society entities.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.3.1.3 All user groups in Bermuda understand the importance of cybersecurity, their responsibilities, and the various measures they need to take in order to protect their systems, networks and data.

On-going Initiatives:

Objective 3.1.1 – build and expand the scope of existing cyber safety programmes.

3.3.1.4 The Cybertips programme is ongoing at a number of schools and partner organisations. In addition to sharing cyber-safety information, it also promotes cybersecurity awareness and conducts threat-sharing activities in the professional community

3.3.1.5 Programmes on cyber-safety targeting senior citizens are ongoing

Specific Objective 3.3.2: Review and reform the education curriculum to include ICT, computer science and cybersecurity

Cybersecurity should be promoted at all levels of society. In today's digital age, there is a need to ensure that the education curriculum supports cybersecurity programmes not only to increase awareness across the board, but also to support persons who may be interested in such a career path. The Ministry of Education appreciates the importance of integrating computer science and cybersecurity instruction within the education system. What's more, the Department of ICT Policy and Innovation's ECAB Education Sub-Committee advises Ministers on developments in ICT and computer science and promotes the use of technology in this regard.

The IT Career Guide produced by the Department provides information on the various ICT-related careers in Bermuda, local IT courses, and scholarships available. It also contains interviews with Bermudians in the field and information for those who are thinking about exploring ICT as a career path.

Bermuda will ensure that cybersecurity is promoted through such initiatives and undertake to build the human and infrastructure capacity within its educational institutions to support these efforts.

Actions:

3.3.2.1 Encourage the provision and affordable access to secure ICT infrastructure to support technology education.

3.3.2.2 Develop the capacity of educators and other related entities.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.3.2.3 ICTs and cyberspace are fully leveraged by the education sector in Bermuda,

3.3.2.4 Cybersecurity instruction is a core component of Bermuda's education sector which enables the development of a sustainable pool of cybersecurity expertise locally.

On-going Initiatives:

Objective 3.2.2 – develop ICT capacity for educators and other related entities.

3.3.2.5 The Ministry of Education has finalised its Strategic Plan 2022 for education that recognizes the importance of ICT and computer science.

3.3.2.6 ECAB has an education sub-committee that advises Ministers on ICT and computer science.

3.3.2.7 There exists a Wifi-for-schools project which aims to make fast access available to all public schools within the current school year.

Specific Objective 3.3.3: Establish a cybersecurity excellence programme

Globally, countries are challenged by inadequate cybersecurity skills and expertise and Bermuda is no exception. Bermuda will promote the development of cybersecurity skills nationwide with a view to increasing the number and diversity of qualified cybersecurity professionals within the public and private sector.

Bermuda will also promote a culture of innovation and provide the facilities to support research and development by engaging with key stakeholders and forming partnerships. The establishment of a centre of excellence within the local tech hub will support the efforts and aid in creating a pool of qualified individuals in the field of cybersecurity.

Actions:

3.3.3.1 Promote partnerships with relevant organisations to facilitate capacity building, research and development.

3.3.3.2 Establish a cybersecurity centre of excellence in Bermuda.

3.3.3.3 Establish a framework to coordinate and promote collaboration and partnership on cybersecurity.

3.3.3.4 Develop a workforce development policy for local cybersecurity expertise.

Expected Outcomes: Upon the successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.3.3.5 Bermuda proactively supports R&D and innovation in cybersecurity by locally-based individuals and companies, which results in increased investment and growth of the cybersecurity sector of Bermuda.

Specific Objective 3.3.4: Foster a culture of innovation and leverage the adoption of good practice in cybersecurity

Innovation is at the forefront of Bermuda's agenda as it seeks economic diversification. The Government has commenced discussions on the development of the world's first Global Risk Management Digital Market in Bermuda which will support the Government's FinTech ambitions and the establishment of a smart Island innovation lab. This initiative will attract and support entrepreneurs, innovation, new business ventures, growth opportunities and job creation. Blockchain-based technologies are also being promoted. They have the potential to transform the way in which business in the world is conducted.

In keeping with Bermuda's international reputation for sound regulation, Bermuda will ensure that its legal and regulatory framework does not stifle innovation.

Actions:

3.3.4.1 Review existing and develop new, innovative programmes in cybersecurity.

3.3.4.2 Create a framework which supports R&D initiatives in educational institutions.

Expected Outcomes: Upon successful attainment of this specific objective, Bermuda expects to achieve the following outcome:

3.3.4.3 Increase investment in cybersecurity innovation and R&D on the Island which will contribute to overall economic prosperity while enhancing Bermuda's cybersecurity posture.

Specific Objective 3.3.5: Enhance the capacity of all Government ministries, departments and agencies (MDAs) (including the judiciary, law enforcement, prosecutors and other relevant agencies) to address cyber-threats and to combat cybercrime

In creating an aware and skilled society, Bermuda recognises the importance of also focusing on enhancing cybersecurity and cybercrime knowledge among law enforcement, prosecutors, judiciary and other similar entities. This is imperative as such officials need to possess the knowledge and skills required to effectively address cybercrime offences and contribute to a safe and secure society with respect for the rule of law.

Bermuda will undertake a training needs assessment to determine the type and level of training which is required by different stakeholders. Based on this, the Government will have a clearer picture of training needs and can prioritise their delivery. It is also critical for technical-level officials to continuously undergo training, thereby staying abreast of new developments.

When building capacity within the public service, it will be useful to conduct drills and simulation exercises which will bring together a wide cross-section of stakeholders, provide a learning platform to better understand each stakeholder's role and responsibilities, and encourage information sharing.

Actions:

3.3.5.1 Conduct a gap analysis to assess and identify cybersecurity and cybercrime training requirements of all government MDAs.

3.3.5.2 Train both MDA and external personnel on the new legal provisions of the legislation, regulation, policies and procedures related to cybersecurity.

3.3.5.3 Build capacity in MDAs to enforce/implement cybercrime related provisions of legislation and policies.

3.3.5.4 Promote awareness of minimum cybersecurity standards in all government MDAs.

3.3.5.5 Continuously roll out training programmes tailored to address cybersecurity and cybercrime training requirements of all government MDAs.

Expected Outcomes: Upon successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.3.5.6 All government MDAs possess the appropriate capacity to address cybersecurity and cybercrime effectively resulting in increased detection and management of cyber-threats, including cybercrime.

On-going Initiatives:

Objective 3.5.1 – conduct a gap analysis to assess and identify training requirements in cybersecurity and cybercrime.

3.3.5.7 The Bermuda Police Service has on-going multi-jurisdictional training.

3.4 Strategic Goal 4: Enhance local and international cybersecurity collaboration and cooperation

Bearing in mind the borderless nature of cyberspace, Bermuda appreciates the importance of collaborating with regional and international stakeholders to ensure a safe and secure cyberspace. Bermuda will build on existing cooperation and collaboration frameworks to take part in cybersecurity activities and debates taking place beyond the Island. These partnerships and opportunities will enable Bermuda to address cyber-issues and create a secure and open cyberspace to enhance the prosperity of all citizens and residents. This participation should result in information-sharing on global trends and good practices. It should also afford Bermuda increased capacity to address vulnerabilities and attacks.

Specific Objective 3.4.1: Promote Bermuda as a secure destination for conducting business

Bermuda will ensure that new regional and global partnerships are established while existing ones are strengthened. The promotion and publication of the Bermuda Cybersecurity Strategy will serve to raise global awareness of Bermuda's efforts to secure its cyberspace while attracting opportunities for collaboration in several areas beyond cybersecurity. The Government will encourage stakeholders involved in business and tourism to share the Strategy, be it on their respective websites or referring to the vision and objectives at international events.

Actions

3.4.1.1 Ensure Bermuda's progress and status in cybersecurity are publicized and widely disseminated.

3.4.1.2 Publish and publicise the Bermuda Cybersecurity Strategy.

Expected Outcomes: Upon successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.4.1.3 Bermuda's enhanced cybersecurity posture and joined-up approach to addressing cyber-threats and issues is widely recognised across the world thereby fostering trust and increasing interest in investing in Bermuda.

Specific Objective 3.4.2: Establish partnerships with relevant organisations at the local, regional and international levels to address cybersecurity issues

Cybersecurity requires partnerships at all levels, nationally and globally. Bermuda will embark on developing and strengthening partnerships with stakeholders around the world including nation-states on a bilateral basis, regional and international organisations, private sector organisations, academic institutions, and civil society.

Bermuda also appreciates that a key aspect of international cooperation is the promotion of discussions from the perspective of a small Island-state. This will necessitate greater participation in international debates at the regional, hemispheric and international levels.

Actions

3.4.2.1 Enhance local partnerships and collaboration across all sectors on cybersecurity and cybercrime.

3.4.2.2 Participate effectively in relevant cybersecurity-related regional and international fora.

3.4.2.3 Develop a strategy for international collaboration and engagements on cybersecurity and cybercrime.

3.4.2.4 Subscribe to relevant regional and international instruments relating to cybersecurity and cybercrime.

Expected Outcomes: Upon successful attainment of this specific objective, Bermuda expects to achieve the following outcomes:

3.4.2.5 Bermuda participates effectively in setting and addressing the international agenda on issues relating to cybersecurity and as a result, emerges as a leader in cybersecurity on the global scene.

3.4.2.6 Bermuda partners and collaborates effectively with relevant stakeholders locally and internationally to address cybersecurity-related issues

On-going Initiatives:

Objective 4.2.1 – enhance local partnerships and collaboration across all sectors on cybersecurity and cybercrime.

3.4.2.7 Bermuda is collaborating with international partners to develop and implement this Strategy.

3.4.2.8 There exists collaboration with other international crime-fighting organisations such as Interpol, the FBI, and the U.S. Drug Enforcement Administration.

3.4.2.9 The Bermuda Police Service has previously retained overseas agencies to conduct computer forensics.

Objective 4.2.2 – participate effectively in relevant cybersecurity related regional and international fora.

3.4.2.10 Bermuda currently participates in meetings of CARICOM, ICANN, the CTO etc.

4. Implementation and Management

4.1 Roles and Responsibilities

Although Bermuda is a small Island-nation, it is imperative that there be a collective understanding and recognition of the shared responsibility of all stakeholders in protecting the CIIs and ICT services in Bermuda. This understanding is essential to the management and implementation of this Strategy. The roles and responsibilities of key stakeholder groups in Bermuda are described as follows:

(i) The Government of Bermuda: Cybersecurity requires a Whole-Of-Government approach. The Government of Bermuda is responsible for ensuring the protection of the Island's cyberspace and of citizens. It is understood, however, that the lead authority within the government would be the department responsible for ICTs and cybersecurity.

Within the context of this Strategy, the Government will be responsible for managing the cyber-threats targeting the critical information infrastructure and national security of Bermuda. Bearing in mind that the Government holds national data and provides e-government services to citizens and organisations, it is crucial that the Government of Bermuda put in place robust and appropriate measures to protect the systems, networks and information it possesses and manages.

While some CII are owned and operated by the private sector, the Government of Bermuda is still responsible for ensuring that all CII is secure and resilient and able to support the continuous supply of essential services in Bermuda. This will require the Government to ensure all CII service providers comply with minimum security standards for CII.

Another key responsibility of the Government of Bermuda includes the promotion of awareness and the provision of information and advice to citizens, residents and users, thereby enabling them to adopt and implement the appropriate measures for protecting themselves. One crucial responsibility of the Government relates to fostering an enabling environment for cybersecurity, where Bermuda's education and training system produces a sustainable pool of cyber-expertise which will in turn drive an innovative and vibrant cyber-sector in Bermuda.

For all intents and purposes, the Government of Bermuda is responsible for ensuring the successful implementation of this Strategy and the attainment of the strategic goals and objected defined within it.

(ii) **Cybersecurity Governance Board:** This Strategy emphasises that Bermuda will establish a cybersecurity governance body under cybersecurity legislation to lead the implementation of the Strategy. While the membership of this body is yet to be defined, the current Cybersecurity Working Group will serve as the interim body until a formal governance structure is constituted to coordinate, plan and implement cybersecurity initiatives across Bermuda.

The body will also oversee the protection of CII in Bermuda and provide advice and support to organisations across the Island. One key role and responsibility of the governance body will be the adoption of nationally-established guidelines, standards, good practices, and security requirements necessary for the protection of ICT systems, networks, and data. In effect, the body will serve as the national source for cyber-security expertise and direction nationwide.

(iii) **Bermuda CSIRT:** The Strategy calls for the establishment of a national CSIRT for Bermuda. This Unit will be created to work alongside the governance board and will lead the cyber-incident response and management activities of Bermuda at the national level.

(iv) **Private Organisations:** private-sector entities based in Bermuda own and manage their own infrastructure in their day-to-day operations and in the provision of services. Consequently, they must deploy appropriate investments and measures and develop the right capacities to ensure the security and resilience of said systems, networks and information.

(v) **Owners and operators of Critical Information Infrastructure and Information Systems:** These entities in Bermuda, whether publicly- or privately-owned, are responsible for ensuring the protection and resilience of their systems, networks and data, and will be required to execute all appropriate measures to ensure their protection and resilience. They will also need to make investments and implement measures to ensure compliance with nationally-defined cybersecurity guidelines, security requirements, standards, processes, procedures, policies and frameworks.

(vi) **Bermuda Police Service:** In collaboration with other relevant stakeholders (national or international), the Bermuda Police Service will expand their efforts to disrupt, investigate and prosecute cyber-criminal activity conducted in, or targeting Bermuda. The Bermuda Police Service will work with the governance body and the CSIRT to support the national cyber-incident and cyber-emergency responses.

(vii) **Regulators:** There will be an increasing role for all regulators including the Bermuda Monetary Authority (BMA) and the Bermuda Regulatory Authority (RA).

The BMA regulates Bermuda's financial sector and develops risk-based financial regulations, which is especially relevant for Bermuda given the offshore economy. The BMA has a role in ensuring the sector complies with accepted standards and regulations, which also include anti-money laundering and anti-terrorist financing regulations.

The RA regulates the telecommunications and energy sectors. Telecommunications is the entry point for all data transiting in and out of the Island. It is critical that appropriate measures are employed by providers to protect Bermuda's cyberspace and its users. Additionally, as the main source of energy in the Island is from a single entity, it is a single point of failure. This requires that appropriate security measures are used to protect this vital service.

(viii) **Consumer Affairs:** Given the business focus of the Strategy, Consumer Affairs will have a role in ensuring that unfair business practices and unconscionable acts are not prevalent in everyday consumer business transactions.

(ix) **Civil Societies:** Those based in Bermuda will work with other relevant stakeholders to ensure the accountability and transparency of public and private sector organisations. They will also play a key role in building awareness of cybersecurity issues and trends nationwide and across all segment of Bermuda's society. Furthermore, they will facilitate, ensure and enhance engagement and dialogue among all stakeholders.

(x) **All Users:** Everyone Bermuda will be responsible for adopting and implementing all appropriate measures to protect themselves online and secure the systems, networks and data they own/or manage in their private and professional lives. It is critical that individuals do this as they are potentially weak links in the cybersecurity of the Island and could be an effective line of defence

against cyber-threats targeting Bermuda's collective data, networks and systems.

4.2 Approach for Monitoring and Evaluation

All monitoring and evaluation activities by Bermuda should enable the achievement of the national Vision and Strategic Goals of this Strategy by assuring the accurate reporting of progress, documentation of challenges faced, and the integration of lessons learned in on-going implementation activities.

Bermuda will establish a Monitoring and Evaluation Plan to monitor the progress and impact of the recommended objectives and milestones in the Strategy.

Bermuda is committed to monitor and evaluate this Strategy in a manner that supports informed and effective planning and decision-making. The Monitoring and Evaluation Plan for this Strategy will:

4.2.1.1 Be based on well-defined SMART Performance Targets for each stakeholder group involved in, and responsible for implementing specific elements of this strategy.

4.2.1.2 Be based on annual action plans which will establish a common understanding of the expected end results, outline the approach for achieving these end results and identify the resources required to achieve them. These annual action plans consider the Key Performance Indicators (KPIs), and Timelines provided in the Implementation Logical Framework.

4.2.1.3 Specify performance and progress-related indicators and establish who is responsible for collecting data on said indicators. The plan will also specify what methods and tools will be used to collect the data and how the data will be used. The plan will be built on the Key Performance Indicators (KPIs), SMART Performance Targets and Timelines.

4.2.1.4 Ensure that progress in achieving Expected Results and Expected Outcomes is regularly monitored and reported on. Promptly observe and report deviations.

4.2.1.5 Ensure the periodic assessment of performance against defined targets. These periodic reviews for determining progress in achieving Expected Outcomes and long-term impact of strategy will be undertaken as follows:

- Annual reviews,
- Mid-term review at the start of year 3 of this Strategy, and
- Long-term review by the end of year 4 of this Strategy.

4.2.1.6 Ensure that wherever necessary, remedial measures to keep implementation on track are adopted and implemented.

Glossary

Authentication: the process or action of verifying the identity of a user or process.

Bitcoin: a type of digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds. The Bitcoin operates independently of a central bank.

Blockchain: a digital database containing information (such as records of financial transactions) that can be simultaneously used and shared within a large decentralized, publicly accessible network.

Breach/Data Breach: the unauthorised movement or disclosure of information on a network to a party who is not authorised to have access to, or see, the information.

Cybercrime: criminal activity (such as fraud, theft, or distribution of child pornography) committed using a computer - especially to illegally access, transmit, or manipulate data.

Cyber-espionage: the use of computer networks to gain illicit access to confidential information, typically information that is held by a government or other organization.

Cyber-incident: a breach of a system's security policy in order to affect its integrity or availability and/or the unauthorised access or attempted unauthorised access to a system or systems.

Cyber threat: something capable of compromising the security of, or causing harm to, information systems and internet-connected devices, the data on them and the services they provide.

Cyber safety: the safe and responsible use of information and communication technologies.

Cybersecurity: measures taken to protect a computer or computer system (as on the Internet) against unauthorized access or attack.

Cyberspace: the online world of computer networks and especially the Internet.

Distributed Denial of Service (DDoS): the intentional paralyzing of a computer network by flooding it with data sent simultaneously from many individual computers.

Distributed Ledger Technologies: a database that exists across several locations or among multiple participants.

E-commerce: commercial transactions conducted electronically via the Internet.

Encrypted: when information is converted into a cipher or code especially to prevent unauthorized access.

FinTech: technology that seeks to improve and automate the delivery and use of financial services.

Internet of Things: the interconnection via the Internet of computing devices embedded in everyday objects, such as smart watches, enabling them to send and receive data.

Personal Data/Information: any information relating to an identified or identifiable natural person.

Phishing: the fraudulent practice of sending emails purporting to be from reputable companies in order to induce individuals to reveal personal information, such as passwords and credit card numbers.

R&D: Research & Development.

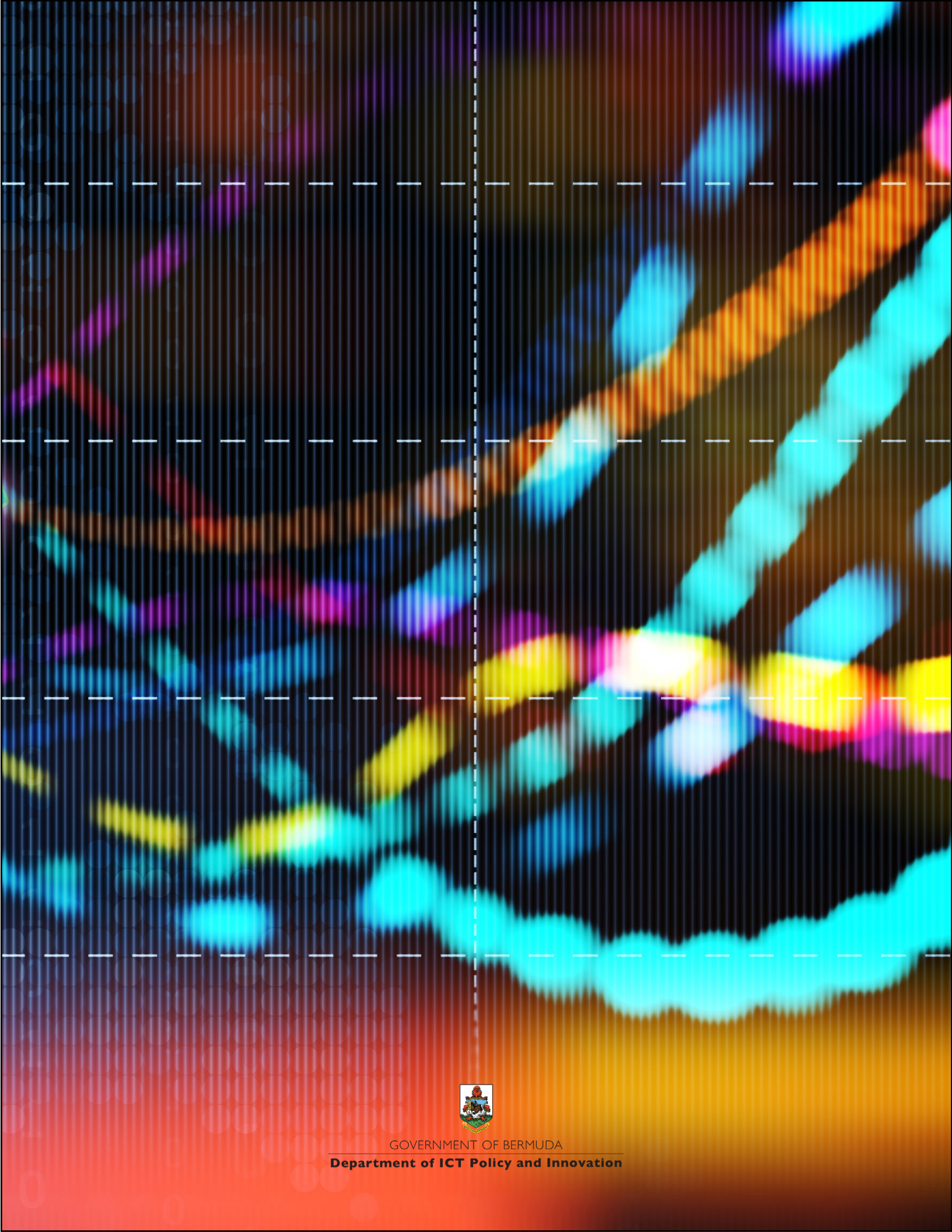
Ransomware: a type of malicious software designed to block access to a computer system until a sum of money is paid.

Risk: potential that a given cyber-threat will exploit the vulnerabilities of an information system to cause harm.

SMART: a method used for goal-setting to ensure that goals are: Specific, Measurable, Attainable, Relevant and Time-based.

Social Engineering: the use of deception to manipulate individuals into divulging confidential or personal information for fraudulent purposes.

Vulnerability: bugs in software programmes that have the potential to be exploited by attackers.



GOVERNMENT OF BERMUDA

Department of ICT Policy and Innovation