2017

Republic of Mauritius

CYBERCRIME STRATEGY

August 2017

Contact Us

Ministry of Technology, Communication and Innovation

Level 6, SICOM Tower

Wall Street Ebene

Republic of Mauritius

Table of Contents

LIST OF ABBREVIATIONS

AGO –Attorney General's Office
BOM – Bank of Mauritius
CERT-MU – Computer Emergency Response Team of Mauritius
CIB – Central Informatics Bureau
CC-Cybercrime Unit of Mauritius Police Force
DPO – Data Protection Office
FBI – Federal Bureau of Investigation
FSC – Financial Services Commission
FIU – Financial Intelligence Unit
ICAC – Independent Commission Against Corruption
ICTA – Information and Communications Technologies Authority
IJLS – Institute for Judicial and Legal Studies
ISP – Internet Service Providers
ITSU – IT Security Unit
MBA – Mauritius Bankers Association
MTCI – Ministry of Technology, Communication and Innovation
MPF- Mauritius Police Force
NCB – National Computer Board
ODPP – Office of the Director of Public Prosecutions

Part I

Introduction

Vision & Mission

Goals

1.0 INTRODUCTION

The Internet and digital technologies are revolutionising our society by driving economic growth and providing new ways to connect with one another. The use of technology is transforming the way business is being done by making it more effective and efficient. Consequently, there is an increased flow of innovation and productivity, thus driving the expansion of the cyberspace.

The ICT sector is a key sector in Mauritius and the Vision 2030 of the Government is to transform Mauritius into a SMART island, an evolution of the Cyber Island which was envisioned in 2001. The aim of the Government is to embed the use of technology in the day to day life of every Mauritian. This would imply that government services, businesses, lifestyle as well as the physical infrastructures would be centred around digital infrastructure.

The increasing reliance on the cyberspace brings new opportunities, but at the same time new threats. Cyber criminals are becoming more sophisticated, and continue to develop malicious software and devise improved methods for infecting computer systems and networks. Cyber criminals are adapting their tactics, as new defences are implemented. The cyberspace is being used as a platform to compromise critical infrastructures and commit crimes such as fraud, theft of sensitive data, amongst others. Cyber criminals can operate from anywhere in the world, targeting large numbers of people or businesses across international boundaries, and there are challenges posed by the scale and volume of the crimes, the technical complexity of identifying the perpetrators as well as the need to work internationally to bring them to justice. The Internet opens new opportunities to cyber criminals and enables aspiring criminals to enter the environment, based on a belief that law enforcement struggles to operate in the online world.

Cybercrime and Cybersecurity are words often considered interchangeable, however Mauritius has already a cybersecurity strategy that runs from 2014 to 2020. This new cybercrime strategy runs in parallel and deals with the issues pertaining to the investigation and prosecution of criminals, and the role of the criminal justice system, while the cybersecurity strategy focusses on prevention, mitigation and defence of critical national infrastructure assets. The two strategies may be merged in the future, however both documents are equally valuable and should be read in conjunction with one and other.

The Government recognises the serious threats posed by cybercriminals and the necessity to bring them to trial to answer for their criminal acts. In this perspective, a National Cyber Security Strategy was developed and approved by the Cabinet in 2014. The strategy provides an overview of what it takes to effectively protect information systems and networks and gives an insight into the Government's approach and strategy for protection of cyberspace in the country.

Nevertheless, as new crimes are developing at an exponential rate, there is a need to carry out proper investigation and prosecute offenders. In this context, a Cybercrime Strategy is required that will enable law enforcement agencies in Mauritius to detect, handle and prosecute cybercriminals and the judiciary to understand this highly technical and complex area whenever cases are brought before Courts. The Cybercrime Strategy will also support the existing National Cyber Security Strategy, hence forming part of the overall approach to provide rapid response to

cybercrime, thereby securing our Mauritian cyber-territory. The measures outlined in the Cybercrime Strategy will set out the Government's approach to fight cybercrime through improved law enforcement capability, effective criminal justice framework and active international engagement.

2.0 VISION

A safer and more secure digital environment for Mauritius

3.0 MISSION

To enhance the Government efforts to tackle cybercrime by providing a more effective law enforcement and criminal justice response

4.0 GOALS

- **To ensure that law enforcement agencies are able to detect, investigate cybercrime in a more efficient way**
- **To provide a more effective legal framework for investigating and prosecuting cybercrime**
- **To enhance the capacity of the judiciary to deal with cybercrime and digital evidence**
- **To develop an enhanced intelligence picture of the cybercrime threat facing Mauritius**
- **To work with international counterparts to improve cooperation on cybercrime**
- **To support the industry by responding to the shared problem of cybercrime**
- **To educate the community on the risks of cybercrime**

Part II

The National Response to Fight against Cyber Threats

Key Principles Supporting Our Approach

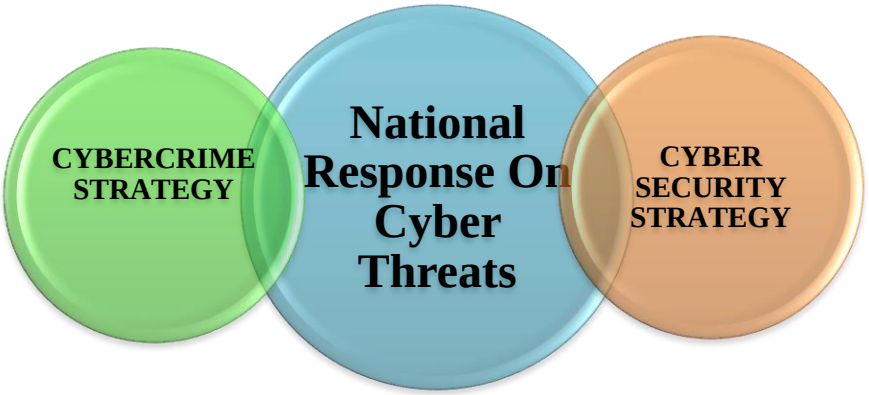
Key Priorities

5.0 THE NATIONAL RESPONSE TO FIGHT AGAINST CYBER THREATS

The Government recognises that the challenge presented by cyber-threats is one that requires a coordinated national response. Preparing for cyber-threats and cyber-defense involve immediate, transparent and better coordinated action from all parties in society, both individually and collectively. It is important to provide political guidance and strategic guidelines for cyber-security and take necessary decisions regarding the allocation of resources and prerequisites. The National Cyber Security Strategy sets out guidelines, measures and action plans that will enhance the cyber-threat preparedness of Mauritius and manage the disturbances caused by these threats.

However since the frequency and severity of cyber threat is accelerating, proper investigation of cybercrime and efficient prosecution of offenders is becoming a prerequisite to strengthen our resilience against these threats. It is, therefore, necessary to have a cybercrime strategy in place that will provide guidance to our law enforcement agencies and assist the judiciary with a better understanding of the area when it comes to judging these crimes.

The Cybercrime strategy represents a commitment from different stakeholders to work together to address the issues of cybercrime. While the strategy focuses on the steps that law enforcement agencies and the judiciary will undertake to respond to cybercrime, it also acknowledges the key roles played by industry and individuals and the importance of forging strong partnerships. The strategy sets out key principles and priority areas of focus over, outlining what we will achieve and how we will achieve it.



6.0 KEY PRINCIPLES SUPPORTING OUR APPROACH

Four key principles support our national approach to cybercrime. These principles form the underlying philosophy of our national response to cybercrime

1. **Knowing the dangers**

Having a better understanding of how cybercrime affects the country will help us address it. We need to know who it targets and why, how it targets them, who the perpetrators are and how

much harm it is causing. Equipped with this information, the Government and relevant stakeholders can better respond to cybercrime.

Victims of any type of crime should be able to report that crime to the authorities and expect an appropriate response. Reporting cybercrime is challenging in many countries and Mauritius is no exception. Often, the people to whom the crime is reported do not have the knowledge and background to respond effectively. While training will, in time improve the situation, the creation of a single on line reporting facility, due in September 2017, will provide a 'one stop shop" where victims may report cybercrime, be assured it will be directed to the correct investigative body and be able to check the progress of any investigation into their complaint. This online reporting portal is also key to gathering statistics to inform the government about the overall impact of cybercrime in Mauritius, and ensure the correct level of resources are applied to deal with the issue.

2. Public and Private Partnership

Tackling cybercrime is, and always will be, a shared responsibility between individuals, industry and Government. This means forging mutually beneficial partnerships to share information and combine efforts to combat cybercrime. Governments will also explore other partnership arrangements, including with overseas law enforcement agencies and with key industry sectors, such as Internet Service Providers (ISPs), online service providers and academia, amongst others.

3. Aiming on Prevention

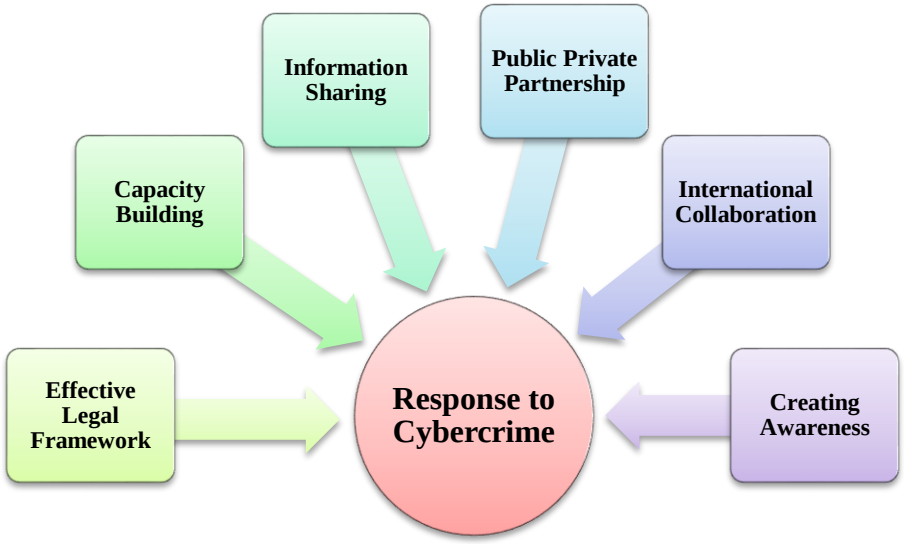
The Government recognises that it is better to prevent cybercrime from happening than to respond to it after it has occurred. In many cases, effective preventative measures are relatively low cost and easy to implement. Users need to take steps to avoid becoming victims of cybercrime. In the same way, Government and industry need to be proactive in anticipating where new threats might emerge.

4. Effective Criminal Justice Framework

To combat cybercrime, an effective legal framework is required. It is significant to understand that whilst technology is evolving rapidly, cyber-threats likewise develop and cyber-criminals become more creative. Thus, the rapid and continuous enactment of laws that address the development of cybercrime is important in order to maintain a safe and secure cyberspace.

7.0 KEY PRIORITIES

Six priority areas have been identified for strengthening the national response to cybercrime and they are as follows:



7.1 PRIORITY NO 1: DEVELOP A MORE EFFECTIVE LEGAL FRAMEWORK TO TACKLE AND PROSECUTE CYBERCRIME

In order to best tackle cybercrime, it is imperative to have an effective legal framework in place. The Computer Misuse and Cybercrime Act was enacted in 2003. It criminalises a number of acts perpetrated through computer systems and provides for the procedures to be followed for the purpose of investigation. In addition, Mauritius has, on 15 November 2013, become the first African country to accede to the Budapest Convention on Cybercrime. It came into force on 1 March 2014.

In order to ensure that our legal framework remains strong and resilient to cybercrime, it is important for us to ensure that it is constantly reviewed and revised, to align it with technological developments, international norms and standards, as well as legal and regulatory changes. Following accession to the Budapest Convention on Cybercrime, Mauritius will ensure that its existing laws are further strengthened and amended, as and when required, to promote compliance with the Convention.

Moreover, following the detection and investigation of cybercrimes, it is important that offences are effectively prosecuted. However, rapid advancements in the functionality of information and communication technologies (ICTs) and innate disparities between systems of law are challenges for first responders, investigating authorities, forensic interrogators, prosecuting agencies, and administrators of criminal justice. Consequently, many cybercrime offenders have evaded prosecution due to weaknesses in substantive criminal laws that do not address technological means of offending.

It is therefore significant that an effective criminal justice framework is developed that would facilitate the enforcement of evolving and new laws with regard to the different types of cybercrime and its prosecution. It would also provide legal practitioners and judicial officers with the capacity and expertise to deal with cybercrime and digital evidence.

7.1.1 Assisting prosecutors and the judiciary to deal with cybercrime and digital evidence

Prosecution of cybercrime offences is an important part of the enforcement framework to deal with cybercrime and assists in creating and maintaining public confidence in our criminal justice system. In order for cybercrime offences to be prosecuted effectively, prosecutors and judicial officers need to be able to understand and evaluate technical digital evidence. While Courts and the legal profession are becoming more accustomed to the use of new technology to commit crime, the admission of digital evidence can still be a challenge and a technical process. As the use of technology in crime grows, prosecutors and judges will increasingly be required to present and understand respectively highly technical details in order to effectively administer the law.

Government can assist prosecutors and the judiciary by providing the resources and the training required for them to respond to legal concepts associated with new technology and the facilities they need to analyse and consider digital evidence in a Court setting.

7.2 PRIORITY NO 2: BUILD CAPACITY TO BETTER ADDRESS CYBERCRIME

The rapid pace and cross border nature of cybercrime poses challenges for traditional regulatory and law enforcement approaches. The capacity and capability of investigators, prosecutors, legal professionals and the judiciary need to keep pace with evolving technologies. Training can also be provided to them to improve their understanding of digital evidence in court.

In order to generate the strongest possible response to cybercrime, there is a need to go beyond traditional law enforcement activities and explore options to predict, prevent and disrupt online criminal activity.

7.2.1 Cybercrime Investigation

The investigation of crimes involving technology requires that new knowledge and skills are acquired by those tasked with the investigation process, usually a law enforcement agency, such as the Mauritius Police Force (MPF). Currently the Cybercrime Unit (CCU) of the MPF is fully assisted by the IT Police Unit for forensics examination of digital evidence. To have a sustainable solution, the Cybercime Unit should acquire the required skills and knowledge. It is proposed to conduct a full analysis of the requirements and roles of the Cybercrime Unit and identify knowledge and skills acquisition requirements for each role within the Cybercrime Unit. This will improve the effectiveness of cybercrime investigations and give confidence to victims that their crimes are being treated seriously.

In addition, the Cybercrime Unit needs to be able to act rapidly to identify offenders and ensure that evidence of crimes is secured before it is deleted, often in the normal course of business.

The Cybercrime Unit also has a role in the crime prevention process and should engage, with others, in campaigns to protect the public from cybercrime.

Businesses are also affected, as victims, and also as holders of data that may be valuable evidence in investigations. Lawful access to such data is crucial in investigations, and the CCU will make it a priority to engage with the business community to share information about threats and also to ensure the smooth transmission of lawfully required data.

In addition to the specialist skills needed by the Cybercrime Unit and Police IT Unit, at the most basic level, all Police officers need to know how to take reports and gather and assess digital evidence, leaving specialist units to focus on more complex cybercrimes. Recruiting and retaining people with the appropriate skills is an essential component of ensuring our agencies are ready to deal with the cybercrime challenge. This may need a different approach, utilising the expertise of non-police officers to assist in the most technical cases.

7.2.2 Forensic Examination of Digital Evidence

Forensic examination of digital evidence is a scientific process as with all other forensic examinations such as those of blood, DNA and fingerprints. As such, it is a process that stands independently of criminal investigations. The function is provided by the Police IT unit, for the Mauritius Police Force. The current practice, whereby the Police IT Unit, is also on many occasions involved in the criminal investigation process, will cease, once the Cybercrime Unit has acquired the skills identified in the previous paragraph. The MPF will consider applying for accreditation under ISO 17025, which will give the assurance of independence and quality control of its procedures. It is important that all agencies conducting digital forensics examinations in Mauritius are compliant with international standards.

When dealing with digital evidence, general forensic and procedural principles should be applied. Actions taken to secure and collect digital evidence should not affect the integrity of that evidence. Persons conducting an examination of digital evidence should be trained for that purpose. Activity relating to the seizure, examination, storage, or transfer of digital evidence should be documented, preserved and be made available for review. The examiner should be aware of the need to conduct an accurate and impartial examination of the digital evidence. Digital evidence is fragile and can be altered, damaged, or destroyed by improper handling or examination. Examination is best conducted on a copy of the original evidence. The original evidence should be acquired in a manner that protects and preserves the integrity of the evidence. The purpose of the examination process is to extract and analyse digital evidence. Extraction refers to the recovery of data from its media. Analysis refers to the interpretation of the recovered data and putting it in a logical and useful format. Actions and observations should be documented throughout the forensic processing of evidence. Agencies likely to handle digital evidence should identify appropriate external resources for the processing of digital evidence before they are needed. These resources should be readily available for situations that are beyond the technical expertise or resources of the department. Agencies should also develop policies and procedures to ensure compliance with local laws. The basic steps to conduct a computer forensic

examination are policy and procedure development, evidence assessment, evidence acquisition, evidence examination, and documenting and reporting.

7.3 PRIORITY NO 3: PROMOTING AN INTELLIGENCE-LED APPROACH AND SHARING INFORMATION

Criminals are quick to find ways to exploit new technologies to further their unlawful activities. Agencies must stay up-to-date with these methods so that they can recognise emerging trends, patterns and problem areas. Sharing quality, timely and comprehensive information and intelligence between law enforcement agencies, intelligence agencies and the private sector will lead to a better understanding of cybercrime and more effective responses. This will occur in a privacy-protective way, in accordance with legislative frameworks and with effective oversight.

We aim to develop an enhanced intelligence picture of the cybercrime threat facing Mauritius. To achieve this, we will focus our efforts on gathering intelligence from the public, business and government agencies and undertaking mutually beneficial information exchanges with the private sector. In addition, an industry liaison officer within the Cybercrime Unit can also help to achieve this goal as he/she will develop the trust network that is needed and also promote the partnership to combat cybercrime.

7.3.1 Cybercrime intelligence and cyber-defence

The value of collecting intelligence information about threat sources and possible cyber-attacks cannot be underestimated. A well-deployed cyber-attack can yield important information that can compromise communication and the economy at large. The changing phase of cyber-attacks as well as ever increasing sophistication of attack methods have complicated the efforts of collecting valuable intelligence information for effective proactive, preventive and protective measures.

Cyber-defence relates to defensive actions against activities primarily originating from hostile actors that have political or economic motivation that have an impact on national security, public safety or economic well-being of the society. The cyber-defence environment requires the deployment of technologies and capabilities for real time protection and incident response. Generally, cyber-defence is driven by intelligence on the threat to achieve the kind of defence that directs, collects, analyses and disseminates the relevant actionable intelligence information to the stakeholders concerned for necessary proactive, preventive and protective measures.

7.3.2 Security threat early warning and response

Rapid identification, information exchange and remediation can often mitigate the damage caused by malicious cyber space activity. For these activities to take place, it requires the setting up of a cyber-threat monitoring system that will enable to better respond, monitor and coordinate cyber-threats at the national level. The system will have the capability for early detection of potentially devastating cyber-attacks and the ability to respond to cyber security incidents in real

time. Through this establishment, cyber-threats can be monitored round-the-clock for critical installations.

The functions of the system will be to:

- Reduce the risk of cyber security threats and attacks on government websites and portals, as well as critical information infrastructures.
- Carry out round-the-clock security operations for early detection and prevention of potential cyber-threats.
- Gather cyber-threat intelligence, which it will analyse and assess for drawing up defensive measures at the national level.
- Promote awareness of cyber threats and coordinate security responses in both public and private sectors.

To improve our collective understanding of the cybercrime threat environment, the government will explore options to enhance the two-way flow of information between government agencies and the private sector where appropriate.

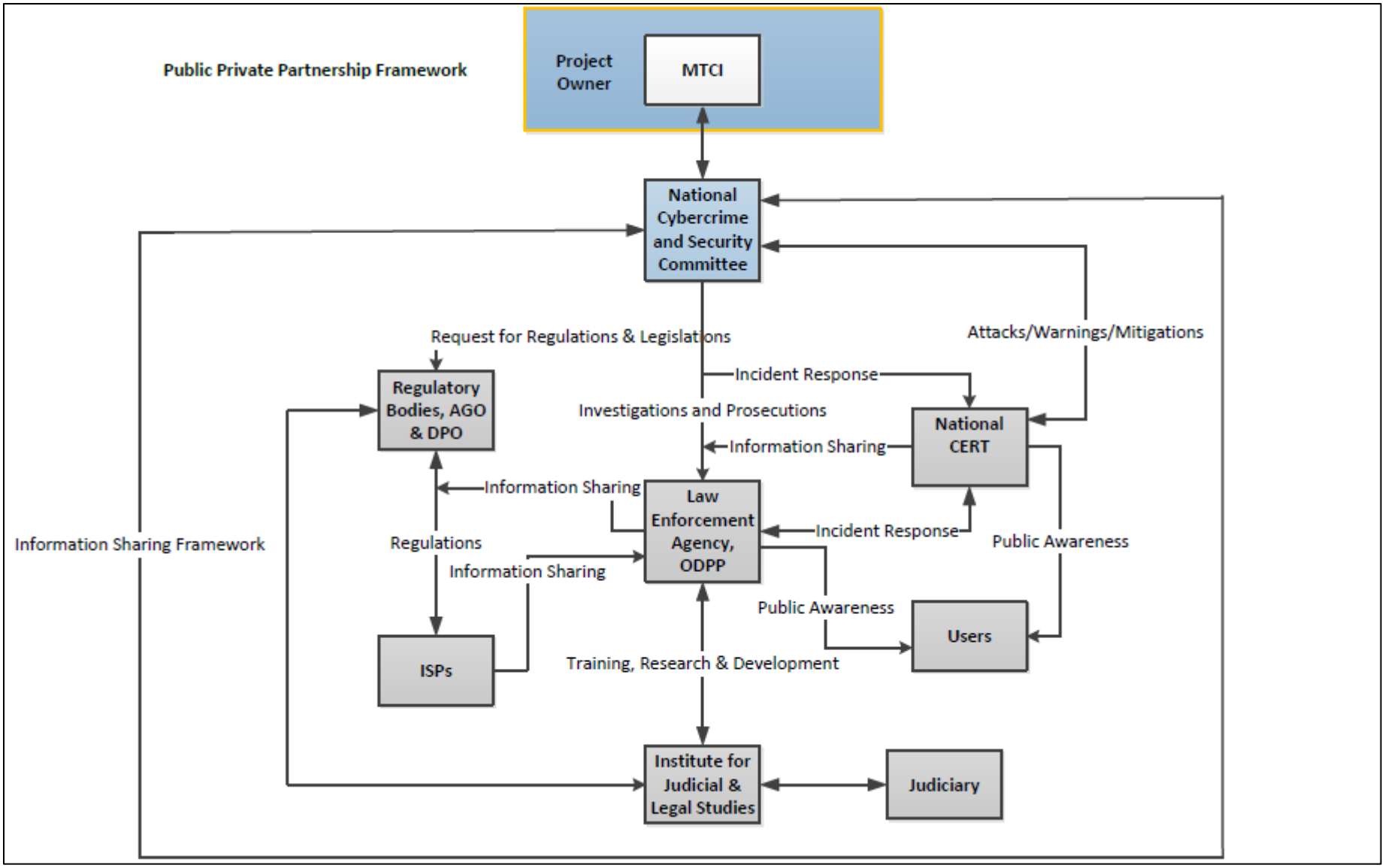
7.4 PRIORITY NO 4: FOSTERING A PUBLIC AND PRIVATE PARTNERSHIP

To fight against cybercrime and safeguard the country's critical information infrastructure, a collaborative working of all key players in Public and Private sector is required. In this strategy, the Public sector refers to government institutions.

The private sectors shall include members from the Banking & Financial, ICT/BPO & Broadcasting, Health, Transport & Logistics, Tourism, Energy, Manufacturing, Sugar sectors and Academia.

An effective public-private partnership for cybercrime will provide the ability to identify threats, anomalous behaviours, and effective response. The partnership will also set the stage to carry out Research and Development in the areas of cybercrime and find ways to mitigate new threats. Finally, this will also help to empower stakeholders to address cybercrime in a more effective way.

To further elaborate on the partnership, the framework below is proposed.


Public Private Partnership Framework
Project Owner
MTCI
National Cybercrime and Security Committee
Request for Regulations & Legislations
Attacks/Warnings/Mitigations
Incident Response
Regulatory Bodies, AGO & DPO
Investigations and Prosecutions
National CERT
Information Sharing
Information Sharing
Law Enforcement Agency, ODPP
Information Sharing Framework
Regulations
Incident Response
Public Awareness
Information Sharing
Public Awareness
Users
ISPs
Training, Research & Development
Institute for Judicial & Legal Studies
Judiciary

The Main Stakeholders of the PPP are:

- Regulatory bodies (ICTA, BoM, FSC)
- Attorney-General's Office (AGO)
- Mauritius Police Force
- Office of the Director of Public Prosecutions (ODPP)
- Data Protection Office (DPO)
- National CERT (CERT-MU)
- IT Security Unit
- Financial Intelligence Unit (FIU)
- Institute for Judicial and Legal Studies (IJLS)
- Internet Service Providers and Private Sectors
- Academia

7.4.1 Roles and Responsibilities

Stakeholders	Roles
Ministry of TCI (Government)	Acts as the Project owner and is responsible for setting-up of the necessary legal framework for strategy implementation.
National Cybercrime and Security Committee	The National Cybercrime and Security Committee will act as the decision-making body and will include representatives from the MTCI, National CERT (CERT-MU), Police, ICTA, BoM, FSC, FIU, ICAC, DPO, AGO, ODPP, IJLS, ISPs & Private sectors to oversee and monitor the implementation of the strategy.
National CERT	The National CERT (CERT-MU), a division of the National Computer Board is the advisory body for information security issues in the country. The responsibility of the national CERT is to provide technical assistance to law enforcement with regard to cybercrime.
Mauritius Police Force	The Mauritius Police Force will be represented by members of the Cybercrime Unit and the Police IT Unit. Their roles are described below: ***Cybercrime Unit:*** • To enable effective prevention, investigation, and prosecution of various aspects of cybercrime • To gather data on cybercrime for analysis purposes • To provide capacity building programmes for the Police • To conduct sensitisation campaigns on cybercrime in schools and organisations as well as for the general

	public ***Police IT Unit:*** • To carry out forensic examination of electronic evidence and provide reports to the Cybercrime Unit/local Police for prosecution
Data Protection Office (DPO)	The Data Protection Office will act as the advisory body on data protection and privacy issues.
Office of the Director of Public Prosecutions (ODPP)	The role of the ODPP are listed below: • Prosecuting cases involving cybercrime. • Tendering legal advice during cybercrime investigation and assist with the procedural tools such as expedited preservation order, disclosure order, production order, search and seizure and real time collection of data. • Providing capacity building programmes for officers of the ODPP and investigators. • Assisting in the training and awareness programmes for law enforcement agencies.
Attorney General's Office (AGO)	The AGO will be responsible for: • Advising and assisting on legal frameworks and legislative amendments required to respond to cybercrime more effectively; • Drafting of appropriate legislation to be introduced and presented before the National Assembly; • Making and receiving formal mutual legal assistance requests to and from foreign countries to seek or provide evidence to support cybercrime investigations or prosecutions.
Regulatory Bodies	The Regulatory bodies shall include the ICTA, FSC and the Bank of Mauritius (the financial sector regulator). The roles of the regulatory bodies will be to: • Establish, control, inspect and enforce regulations regarding cybercrime • Encourage organisations to adopt security best practices and guidelines
Institute for Judicial and Legal Studies (IJLS)	The responsibilities of the IJLS are as follows: • Conduct courses, seminars or workshops for the training of judicial and legal officers in the area of cybercrime and electronic evidence. • Identify areas of need and interest where specialised knowledge is required, and promote and co-ordinate research and development in the area of cybercrime and electronic evidence.

	• Establish areas of co-operation and linkages with local, regional and international organisations in training in cybercrime and electronic evidence.
Financial Intelligence Unit	The role of the FIU will be to: • Analysing and disseminating to investigatory and supervisory authorities' information pertaining to suspected proceeds of crime and alleged money laundering offences, including the financing of any activities or transactions related to terrorism, occurring in the digital environment. • Undertake, and assist in, research projects in order to identify the causes of money laundering and terrorist financing committed in the digital environment and its consequences**.**
IT Security Unit	The IT Security Unit will establish IT Security best practices and promote implementation of information security standards within the Civil Service to improve the level of preparedness and dealing with cybercrime.
ISPs and Private Sector	ISPs and the Private Sector will be represented through respective Associations. Their responsibilities will be to: • Provide strategic insights on security architecture, operations and risk management approaches to users • Provide mitigation strategies in the face of attacks • Co-operate with law enforcement agencies in combating cybercrime.
Academia	The role of academia will be to: • Conduct research and development in the field of cybercrime. • Regular reiew of school curricullum to integrate cybercrime contents.

<u>The successful implementation of the PPP will allow the following:</u>

- ***Information sharing with the private sector***

Businesses are often the first to become aware of emerging cybercrime threats and are also best placed to protect themselves against them. Information sharing arrangements between businesses and governments must be robust and effective. While there are sound policy reasons for certain barriers to information sharing including privacy, commercial and national security concerns,

these must be balanced with the importance of sharing information to support our collective efforts to address the cybercrime challenge.

- ***Enhanced collaboration and co-operation among stakeholders***

The PPP framework will facilitate collaboration and co-operation amongst stakeholders, including the private sector in the area of cyber security in general and protection of critical information infrastructure, particularly actions related to cyber threats, vulnerabilities, breaches, protective measures and adoption of best practices.

7.5 PRIORITY NO 5: IMPROVING INTERNATIONAL COLLABORATION ON CYBERCRIME

Cybercrime is an international problem which requires a coordinated and co-operative international response. While Governments can regulate within their own borders, they cannot regulate externally. There is a need to ensure that countries are able to support the fight against cybercrime and that there are international standards for operational work. International co-operation is most easily facilitated where different legislative systems have common offences which allow for the investigation and prosecution of an offence regardless of the jurisdiction it may have been committed in or wherever the evidence of an offence may be located. Common offences also allow for the possibility of extradition by providing for dual criminality requirements.

One commonly experienced difficulty is in making requests for data to other law enforcement agencies or data owners outside the country. This process varies in its success, speed and complexity dependent on the country, or more frequently the company concerned. Many exchanges are facilitated by personal contacts or the reputation of the organisation or individual requesting the data. The success of a request is not always dependent on whether a country has signed an international convention or agreement which indicates it will provide the co-operation sought.

Criminals are increasingly making use of a variety of technical communication methods for the facilitation of offences and also for the purpose of criminal communications. Tracing the source of communications is essential to trace the offender identity and as intelligence. These communications may be made via ISPs in any part of the world. If any jurisdiction makes it more difficult for law enforcement to obtain details of information, such as subscriber information, then investigations and possible prosecutions will potentially falter.

Our purpose is to identify and reduce barriers to swift and effective international co-operation in response to cybercrime. This can be done through mutual legal assistance, which consists of cooperation between different countries for the purpose of gathering and exchanging information, and requesting and providing assistance in obtaining electronic evidence.

Other channels such as the 24/7 Point of Contact established under Article 35 of the Budapest Convention on Cybercrime must be used for sending requests for mutual assistance for the investigation and prosecution of cybercrime. The 24/7 points of contact are provided for investigations involving electronic evidence that require assistance from foreign law enforcement. In investigations involving computer networks, it is often important for investigators to move at unprecedented speeds to preserve electronic data and locate suspects, often by asking Internet Service Providers to assist by preserving data. Therefore, to enhance and supplement traditional methods of obtaining assistance, this mechanism can be used to expedite contacts between two jurisdictions.

The 24/7 Network of Contact Points is provided to countries acceding to the Budapest Convention on Cybercrime, the Group of 8 countries (G8) and Interpol.

Since Mauritius acts as a hub for knowledge exchange within Africa, it is imperative for law enforcement agencies to make maximum use of these communication channels in the fight against cybercrime and sharing of information between other countries.

7.5.1 Harmonised legal frameworks

Differences in national laws and the capacity of local agencies to enforce those laws can create a barrier to effective international co-operation on cybercrime. Savvy cyber-criminals can exploit these inconsistencies by operating in countries with weak laws or enforcement regimes.

Mauritius acceded to the Budapest Convention on Cybercrime in November 2013. The principles enshrined in the Budapest Convention are being implemented through the Global Action on Cybercrime (GLACY) Project. GLACY is a joint project of the European Union and the Council of Europe aimed at supporting countries worldwide in the implementation of the Budapest Convention. The Convention provides a comprehensive model framework of offences and law enforcement powers and facilitates close co-operation between member countries. It has become the cornerstone of a harmonised approach to cybercrime for a growing global community of nations. Following the successful implementation of the GLACY project, there is a GLACY + project running up to 2020.

The specific objective of GLACY is to enable criminal justice authorities to engage in international co-operation on cybercrime and electronic evidence on the basis of the Budapest Convention on Cybercrime.

Results are expected in the following areas:

- Engagement of decision-makers
- Harmonisation of legislation
- Judicial training
- Law enforcement capacities

- International cooperation
- Information sharing
- Assessment of progress

The national Computer Emergency Response Team (CERT-MU) has also developed relationships with international CERTs and working groups in response to global cyber-threats.

CERT-MU is also affiliated with Forum of Incident Response and Security Teams (FIRST) since May 2012. FIRST is the premier organisation and recognised global leader in incident response. Membership in FIRST enables incident response teams to be more effective in responding to security incidents as well as to be more proactive.

7.6 PRIORITY NO 6: CREATING AWARENESS BY EDUCATING CITIZENS TO PROTECT THEMSELVES

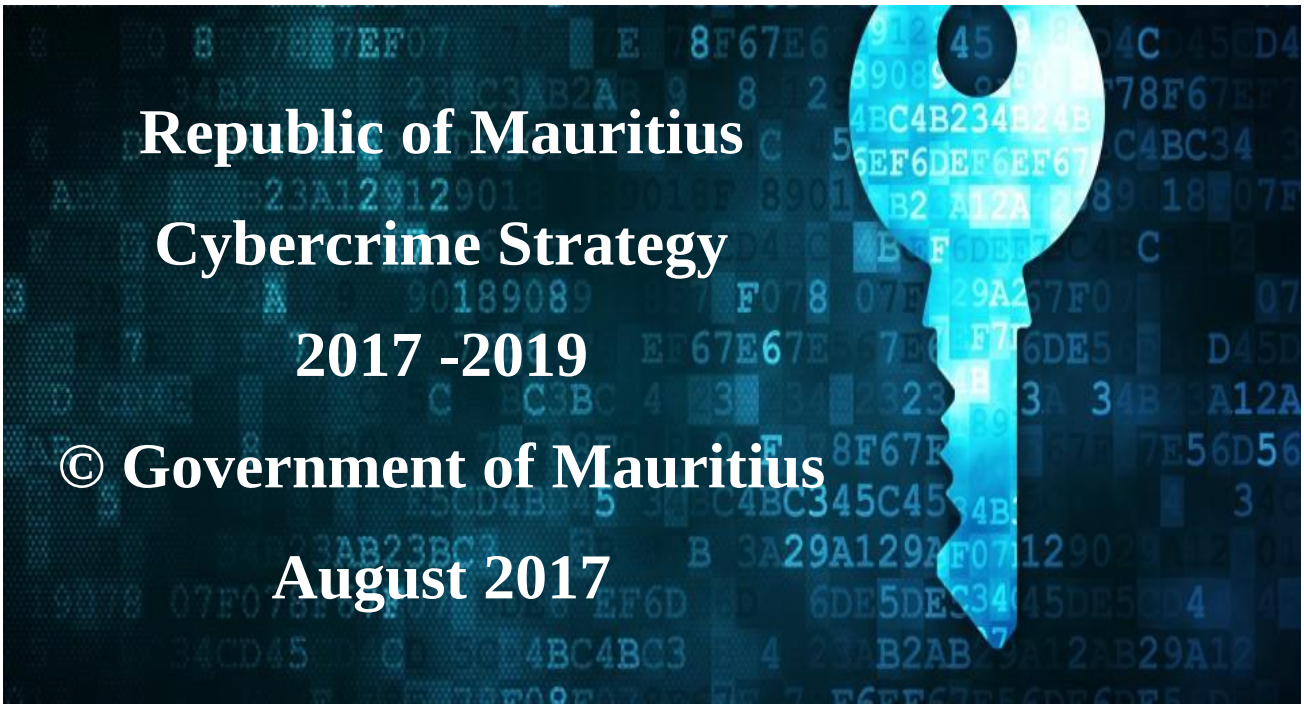
The main purpose of cybercrime prevention is to ensure that information and education is made available to the public and businesses which will enable them to stay safe online. The best way to stop cybercrime is to prevent it from happening in the first place and as part of that the public and business needs to be provided with accurate, relevant information on how to keep themselves safe online and to secure their devices and data.

Cybercrimes are easily carried out due to a lack of cybercrime awareness on the part of computer users, system/network administrators, technology developers, auditors, CIOs, CEOs and corporates.

Apart from end users in organisations, common people or laymen must also be aware of the types of cybercrimes and how they can protect themselves. In this context, public education and awareness is significant. This can be achieved through the collaborative efforts of both the public and private sectors.

The following initiatives are, therefore, proposed for user awareness, education and training:

- A comprehensive national awareness programme on cybercrime
- Training and education programmes on cybercrime in secondary schools and universities
- Incorporating cybercrime contents in school curriculum
- Regular broadcasting of cybercrime related programmes on national television to educate citizens


Republic of Mauritius
Cybercrime Strategy
2017 -2019
© Government of Mauritius
August 2017