DEFENDING MAURITIUS
AGAINST CYBER THREATS

The nation's G-SIRT fights the never-ending battle to build cyber defense capacity

By **Madan Kumar Moolhye**, Information Technology Security Unit, Mauritius Ministry of Information Technology, Communication and Innovation

The last three iterations of the Global Cybersecurity Index (GCI) published by the United Nations' International Telecommunication Union have ranked Mauritius as the country most committed to cyber security preparedness in Africa. How the Government Security Incident Response Team (G-SIRT) approaches capacity building — one of five pillars of criteria evaluated in the GCI — is evaluated here.

Importance of Capacity Building

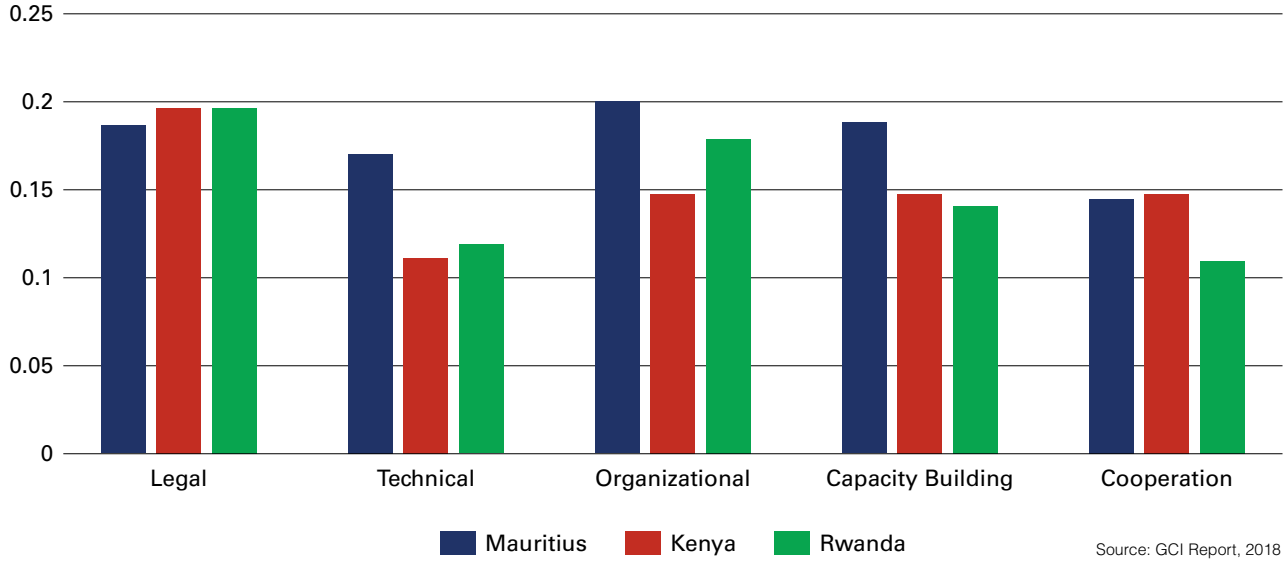
The G-SIRT operates under the Information Technology Security Unit (ITSU) of the Ministry of Information Technology, Communication and Innovation. The ITSU emphasizes the importance of constant development of its technical staff to achieve its objectives, which are:

- Implementing government policies regarding information technology (IT) security.
- Assisting ministries/departments in implementing security standards.
- Disseminating information on IT security.
- Carrying out security audits.
- Handling IT security incidents.

Cyber security awareness is accessible to a wide range of public officers through various deployment modes, such as:

- IT security awareness presentations conducted on-site.
- Circulation of fact sheets on security threats such as phishing, ransomware and identity theft.
- A cyber security module available via a 24/7 electronic learning system.

Top three scores in the Africa region according to the five pillars of GCI



Source: GCI Report, 2018

IDENTITY THEFT

'Know the Dangers'

What is Identity Theft?
Identity theft happens when an imposter uses someone's personal information such as name, address, identity number, credit card or bank account numbers for fraudulent purposes. This may also apply to an organization where a fake profile is created. Identity theft is considered as one of the most common cyber crimes in the world.

Fraudsters can get one's personal information by:
- Using the internet to search about someone or an organization.
- Stealing someone's wallet.
- Stealing postal mail.
- Going through your garbage bin (dumpster diving).
- Making use of malicious software/forged emails.
- Stealing digital information.

If you suspect you are a victim of identity theft, contact the relevant authorities, such as the police or your bank.

Signs of Identity Theft
- Your account statements show purchases that you are not aware of.
- You receive credit cards for which you did not apply.
- You are denied credit for no apparent reason.
- You get calls or letters from businesses about goods/services you did not buy.
- You discover an online profile corresponding to your name/organization which you cannot access.

Consequences of Identity Theft
Once your information is stolen, it may be used to:
- Buy things using your credit card/bank account.
- Commit fraud in your name.
- Create fake profiles in your name.
- Put your own/organization's reputation at stake.

Protecting Against Identity Theft
- Do not give out your personal information, especially via electronic means unless you know who you are dealing with.
- Do not share your sensitive information (such as password, PIN number) with anyone.
- Use strong passwords for all your accounts.
- Shop on secure and trusted websites ("https").
- Never store personal information on computers in public places such as cyber cafes.
- Install an up-to-date antivirus/spyware software.
- Do not use the same password for different accounts.
- Exercise caution on social networking sites.
- Practice safe internet surfing.

Source: Mauritius Ministry of Information Technology, Communication and Innovation

The G-SIRT collaborates regularly with the national Community Emergency Response Team of Mauritius (CERTMU), which addresses incident response at the national level. The G-SIRT acts as a sectoral incident response team within government. The CERTMU has organized several training events and cyber security drill exercises for the public and private sectors at regional and international levels.

The last cyber training drill involved local government teams such as G-SIRT, the data center and IT operators from ministries and law enforcement agencies. One of the main training objectives was to empower the G-SIRT to run cyber drills for government officials in the primary sectors, such as health, energy and utilities, which is a major goal for 2020-2021.

Information Security Management

Adopting the International Organization for Standardization's (ISO) international information security standard (ISO/IEC 27001) in the public and private sectors was a key project in the National Cyber Security Strategy (NCSS) of Mauritius. For the public sector, a novel approach was devised by the ITSU to develop a centralized information security management framework, based on a risk management approach and aligned to the standard. The framework is composed of template risk-treatment plans, addressing security threats to processes that are common to all ministries and that can easily be customized to cater to each sector.

Technical officers have been trained in developing the framework, empowering them to act as the main facilitators to ministries regarding training and implementation. In addition, customized capacity-building, cyber security professionals of the ministry have been trained on default ISO standards curriculum by international certifying bodies, such as India's Standardisation Testing and Quality Certification Directorate. G-SIRT staff also have been trained as security auditors for internal audits.

Government Security Incident Response

The G-SIRT responds effectively to information and communications technology (ICT) security incidents by providing proactive and reactive services to combat cyber threats. As part of its reactive services, the G-SIRT oversees incident management in the civil service through an automated incident handling system that includes a knowledge database available to cyber security professionals and ICT operational staff. This web-based system allows automatic incident escalation — as compared to the previous manual method — which facilitates speedier incident management with wider knowledge sharing. The G-SIRT team has also provided incident training to the operational IT teams posted in the ministries/departments.

Technical staff participation in workshops and cyber drills helps improve incident handling and enhances the provision of security recommendations to the public

sector. Interactions during regional/international workshops facilitate learning and information sharing, which is of high importance because cyber threats know no boundaries.

Security incidents suspected to be cyber crime are referred to the Police Cybercrime Unit for investigation, as per the Computer Misuse and Cybercrime Act. The G-SIRT also interacts with the national CERT for incidents having national impact.

On the proactive front, the team conducts security audits across the entire civil service. However, given the increasing complexity of cyber threats, additional tools and relevant training will be required to effectively protect the government. Furthermore, the G-SIRT is contemplating increasing its range of services to include malware analysis and forensics, capabilities that will require additional capacity building.

Training and Certification

The main challenges faced by G-SIRT are continuous workforce development and certification of its staff to counter the continuous emergence of new cyber security threats. Although technical officers benefit from workshops and seminars offered by donor countries, the skills gap is widening with the advent of technologies such as artificial intelligence and the internet of things.

The proportion of certified officers is low compared to threats in new domains. Certified cyber security training is needed so the team is better equipped to handle threats. Furthermore, to deliver the proposed additional services (e.g., malware analysis, cyber security audits), capacity building must be increased.

Another NCSS project is the incorporation of cyber security in the educational curriculum at primary, secondary and tertiary levels. There is no question that having a cyber security-conscious population would assist in building capacity while developing future professionals for a cyber security industry. The G-SIRT can work with academia and provide industry expertise to young professionals to complement their learning.

Conclusion

The G-SIRT will continue to emphasize professional development as it considers expanding its range of services to combat cyber threats, thereby increasing its contribution to Mauritius' strong GCI ranking. To manage increasing cyber risks, a capacity-building program is essential to counter existing threats, as well as being sufficiently adaptable to handle threats from new technologies. □

INFORMATION SECURITY MANAGEMENT SYSTEM (ISMS)

'Know the RISKS to SECURE better'

Information Security
Information is one of the most valuable assets of an organization and exists in many forms. Information security refers to the protection of information from a wide range of threats so as to preserve its confidentiality, integrity and availability.

Information Security Management System
An ISMS is a management framework, based on a risk management approach, to implement and improve information security. It allows an organization to:

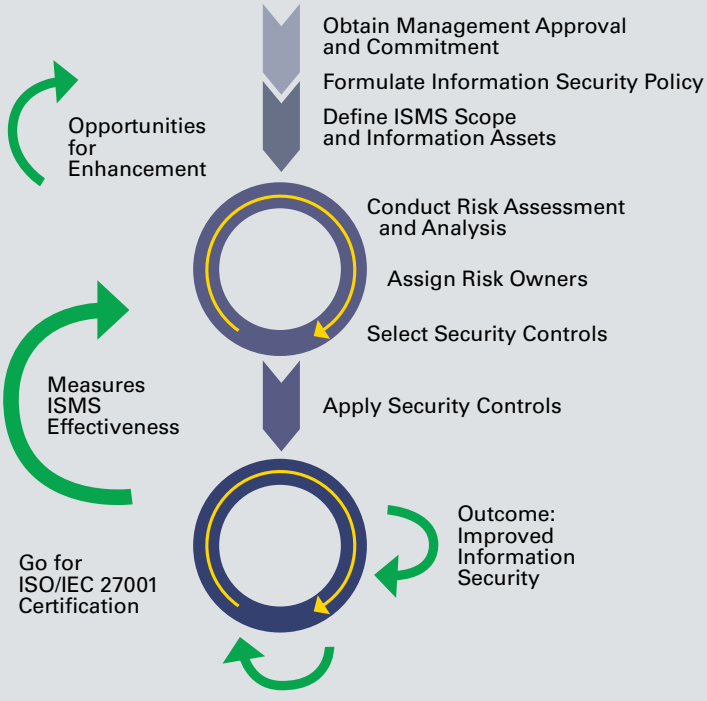
- Identify potential threats and their impacts on business processes.
- Evaluate the degree of risk in several areas.
- Apply adequate measures for eliminating or minimizing those risks.

The international standard ISO/IEC 27001 offers a comprehensive set of measures comprising best practices in information security, risk management and security controls.

Benefits of an ISMS

- Provision of user awareness on security threats and measures.
- Planning of effective business security objectives.
- Promotion of effective risk management.
- Better management of information security incidents.
- Increase in stakeholder confidence.

Steps to implement an ISMS based on ISO/IEC 27001



Source: Mauritius Ministry of Information Technology, Communication and Innovation