PROJECT ON THE NATIONAL CIRT ESTABLISHMENT IN BARBADOS

August 2013 – September 2016

POST IMPLEMENTATION ASSESSMENT REPORT

PROJECT ON THE NATIONAL CIRT ESTABLISHMENT IN BARBADOS

Project Number..... 9BAR13002

Project Manager ..... Marco Obiso

Prepared by..... Onder Cetinkaya

Date..... 21 October 2016

The main goal of the project was to assist Barbados in the establishment of a national Computer Incident Response Team (CIRT), which will serve as a trusted, central cybersecurity coordination point of contact, aimed at identifying, defending, responding and managing cyber threats.

ITU assisted Barbados with the necessary cybersecurity capacity building and technical training to establish its national CIRT. These efforts are expected to also enhance regional and international collaboration.

PARTNERS

International
Telecommunication Union

1 BACKGROUND

Many countries and governments are using the dynamic and inter-connected environment of today's networked information systems to improve communications, protect information, and encourage competitiveness. Computers have become such an integral part of our daily activities that internet-related risks have become part of business risks and this is also valid for government services where online government services have taken up. Valuable country assets and critical national infrastructures are now at risk over the Internet. In this dynamic, and interconnected environment cyber-attacks occur rapidly and can spread across the globe in minutes without regard to borders, geography, or national jurisdiction. Enhancing cybersecurity and protecting critical information infrastructures is essential to each nation's security and economic well-being.

There is a growing need to be able to communicate, coordinate, analyze, and respond to cyber-attacks across different public and private sectors, as well as within national borders. It is important for governments to create and identify a national organization that will serve as a focal point to secure cyberspace and protect critical information infrastructure, through surveillance, warning, response and recovery efforts, as well as facilitate collaboration between government entities, the private sector, academia, and the international community when dealing with cybersecurity issues.

Collaboration at the national and international level is crucial to effectively align capabilities and expertise that will help manage incidents, raise awareness related to cyber security issues and take steps towards remediation.

The establishment of the Barbados national Computer Incident Response Team (CIRT) was needed to help ensure the protection of the nation's critical information infrastructures, assist in drafting a national roadmap on the country's approach to cybersecurity related issues, and serve as a focal point to further build and implement a national cybersecurity culture.

PROPOSED SOLUTION IN THIS PROJECT – CIRT (COMPUTER INCIDENT RESPONSE TEAM)

A CIRT is a key component of a national cybersecurity strategy and is a solid building block onto which other cybersecurity related activities could be linked. The creation of a national CIRT and its related processes, may also serve as the basis for the development of the following activities:

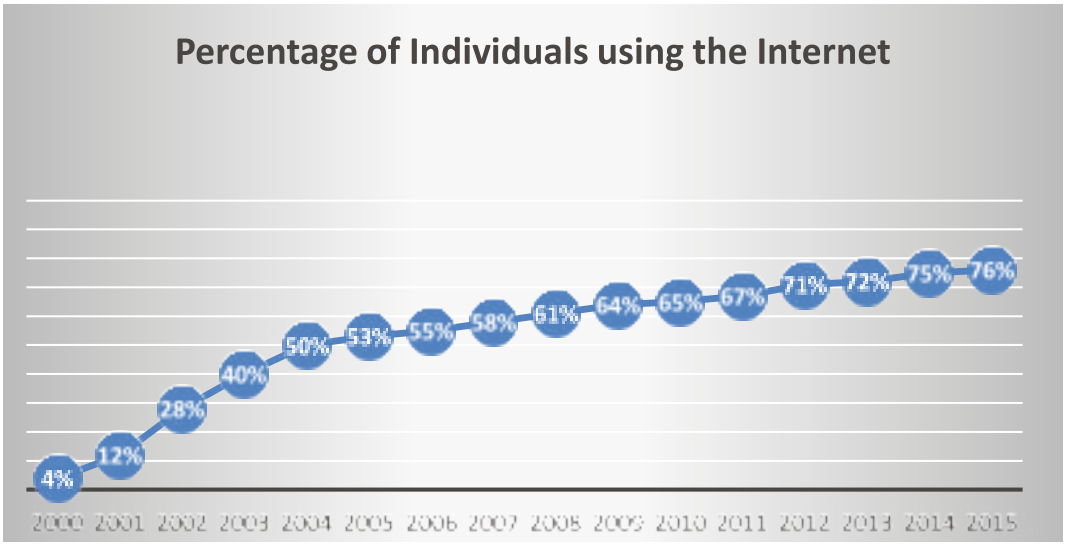
- build a knowledge based platform that supports the country's development and implementation of a national cybersecurity strategy, as well as a national focus on the protection of critical information infrastructures;
- the creation of a national cybersecurity culture and related awareness raising initiatives;
- develop other related national cybersecurity platforms, such as a national Public Key Infrastructure (PKI), an e-Government framework, a national identity and access management framework, combating SPAM, botnets, etc.;
- assist in the planning and implementation of a national strategy on child online protection;
- enable, develop and further enhance the country's national incident response and management capabilities.

2 SCOPE OF REVIEW

Barbados is an island state in the Caribbean with a vibrant community and increasing ICT needs. Over the last decade, Barbados has had sustained real GDP growth and moderate price stability. However, this small open economy also remains vulnerable to a number of external shocks, such as the current recession with started in 2007.

Against the backdrop of economic ups and downs, the ICT sector has shown a steady evolvement, whereby the increasing number of internet subscriptions both in mobile and fixed broadband internet, resulted in higher penetration rates and greater use of telecom services all over the island.

Indicator	**2010**	**2011**	**2012**	**2013**	**2014**	**2015**
Fixed-telephone subscriptions	137,486	140,668	143,358	148,735	151,394	156,857
Mobile-cellular telephone subscriptions	350,061	347,917	349,296	307,708	305,456	334,792
Active mobile-broadband subscriptions	0	0	100,000	118,000	125,000	157,713
Fixed-broadband subscriptions	56,190	62,634	66,884	67,798	77,730	78,269
Percentage of households with Internet	47	49	56	57	62	63



Source: ITU statistics

The increased use of internet on the other hand has also brought potential cyber threats that could adversely affect the provision of services of the ICT infrastructure. To this end, the Barbados Administration decided to invest in the establishment of a national CIRT and collaborated with ITU to implement a CIRT project.

The main goal of the project was to assist Barbados in the establishment of a national CIRT that will serve as a trusted, central cybersecurity coordination point of contact, aimed at identifying, defending, responding and managing cyber threats. ITU assisted Barbados with the necessary cybersecurity capacity building and technical training to establish its national CIRT.

The project was implemented between 2014 and 2016 with a budget of CHF 138,163. Following the completion of the project activities in August 2016, an evaluation mission was undertaken between 5 and 7 September 2016, to conduct a post implementation review of the project. The purpose of the post implementation review was to assess the level of achievement of the expected results and the project objectives, based on the KPIs and targets defined in the project document, as well as draw lessons learned, point out challenges encountered and any other issues.

The post implementation review was conducted through a series of meetings, starting with the beneficiary administration, as well as other stakeholders that either were involved in the project or may have potential influence on the success of the established national CIRT. The below pictures capture instances from those different meetings, which took place during the post implementation review.

3 RESULTS

A functioning national CIRT able to provide Barbados' stakeholders with a basic set of services.

Key Performance Indicator

Availability of the CIRT

Initial Target

By the end of the project

Achieved

Yes

Remarks

Following the installation work in August 2016, it is observed that the equipment was in place and in working condition. The equipment is securely accommodated at the premise of Division of Energy and Telecoms.

Utilization and operation of the CIRT by building an effective/efficient capable CIRT that is ready to respond to cyber-attacks targeting the national critical information infrastructure.

Key Performance Indicator

- Adequate staffing of the CIRT
- Availability of documented processes and guidelines
- Number of incidents handled by the established CIRT

Initial Target

By the end of the project

Achieved

Yes

Remarks

- It was noted the center was staffed by the Telecommunications Unit. The administration confirmed that staffing needs can be re-visited when the center evolves and operates in full capacity.
- Staff in charge of the CIRT has been trained by the subcontractor and provided with the manuals and other guidance documents on the use of the system.
- The system is capable of sending incident reports as the Barbados NCIRT portal is online and accessible.
- At the time of the mission, there has been no incident reporting since the system was quite recently installed.

Enhanced national expertise on cyber security and reduction of the human capacity gap in cybersecurity

Key Performance Indicator

Number of people trained

Initial Target

At least 3 persons trained

Achieved

Yes

Remarks

During the project, training sessions were organized in the field of cyber security related matters.

National awareness training programmes are developed to result in improvements in cybersecurity procedures, to defend and protect infrastructures and government agencies.

Key Performance Indicator

Drafting of a roadmap on the building of a national cybersecurity culture, as a part of national cybersecurity strategy, within the framework of national CIRT enhancements.

Initial Target

By the end of the projects

Achieved

Yes (Partially)

Remarks

- Cybersecurity assessment exercise before the start of the project and the trainings conducted during the mission has already raised some level of awareness among the different stakeholders. Telecom Unit officials indicated their intention to conduct further awareness raising activities to involve other government entities during the operationalization of the CIRT.
- In the interviews it was expressed by Barbados officials that the cybersecurity strategy will be part of the overall ICT strategy, which is currently under preparation. Since ICT related matters fall into jurisdiction of different government entities, there is need for an overall coordination.

4 FINANCIAL STATUS

Project cash contributions ensured as planned?		
(Y/N/Not applicable)	Percentage (%)	Explanations
Yes	100%	Barbados had provided CHF 139,168 in cash to the project.

Is the level of expenditure at the expected level?	
(Y/N/Not applicable)	Percentage (%)
Yes	88.4%

Any funds remaining unused?		
(Y/N/Not applicable)	Percentage (%)	Explanations
Yes	11.6%	CHF 16,128

5 FINDINGS

The established center is intended to assume the following functions:

a) coordinate and assist Government Ministries and Agencies in implementing proactive services to reduce the risks of cybersecurity incidents as well as respond to such incidents when they occur,

b) conduct awareness to educate the local population about the adverse effects of cyber threats and cybercrime,

c) provide timely alerts to all its stakeholders.

The national CIRT is utilizing the available resources as a start, while there is potential to evolve as more resources are allocated to the team. This is also the best approach

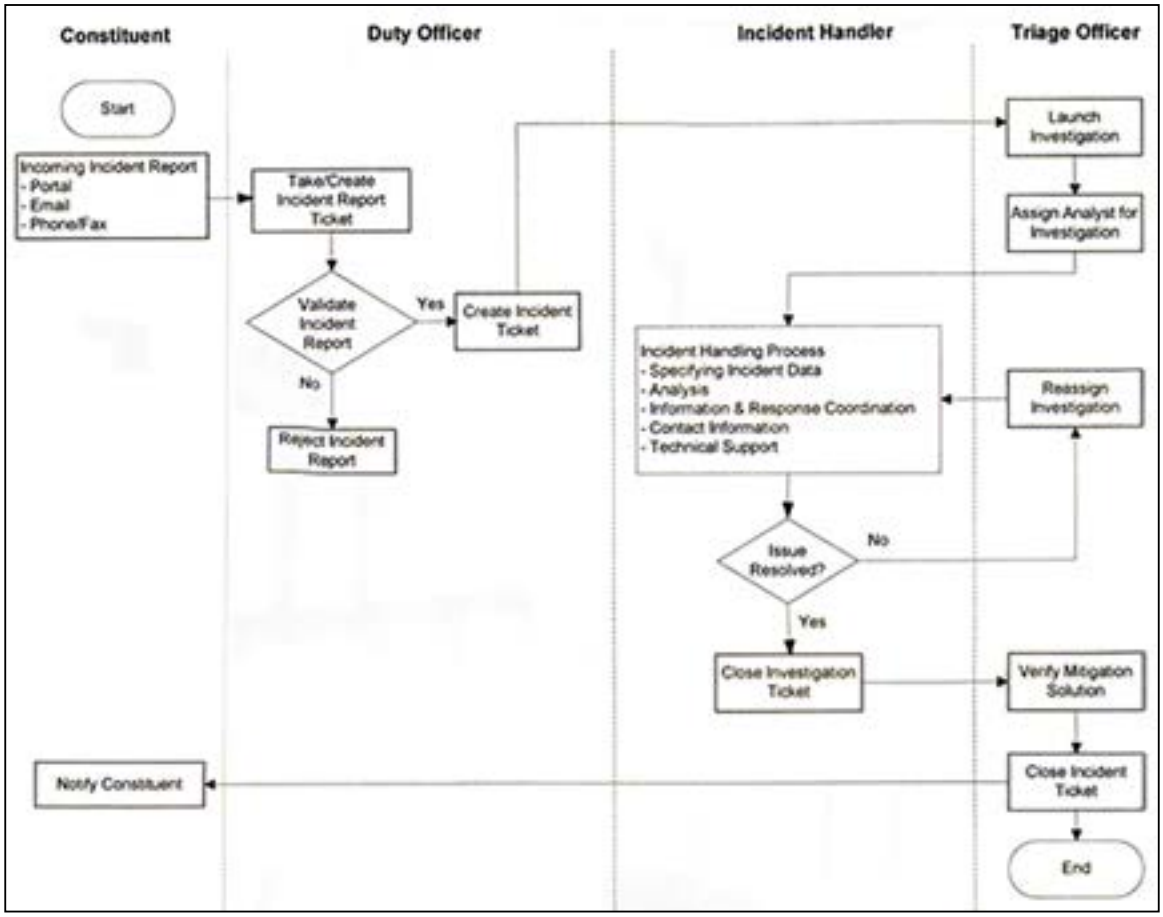
because it enables the Barbados national CIRT to get the necessary buy-in from the government. Below are the services to be provided by the established center:

INCIDENT HANDLING, RESPONSE AND COORDINATION

Incident response will be performed by the Barbados CIRT. In the first instance, it will be implemented as a basic coordination service. The staff will receive incidents from the portal and email from its stakeholders and facilitate communications between the requestor and the appropriate destination about incidents involving third parties.

For example, if a stakeholder/ constituent requires assistance from an ISP, they can contact the CIRT who will in turn contact the correct provider on the stakeholder's behalf if the incident is valid. CIRT will act as a trusted intermediary between its stakeholders who need to contact external network providers, CIRTs, governments or other entities with security related information.

The following flowchart describes the incident handling process:



SECURITY ADVISORIES

Analysts will produce security advisories that cater to specific and targeted audiences. The types of security advisories will include:

a) Security advisories for the general users of the public agencies and government. These advisories contain short information that is clear to the average computer user, so that they may protect themselves online.

b) Security advisories for government stakeholders. These will provide timely information for a current activity that represents a threat to either business interests or to critical infrastructure.

AWARENESS

Awareness campaigns are very important for the sustainability of a CIRT, as they are a valuable tool for stakeholders to become aware of the existence and importance of a national CIRT. Campaigns may take place in the form of advertising on television, website or print; media liaison and press releases; workshops, seminars and training sessions.

The creation of a stakeholder email list is vital as it allows trusted communication between BNCSIRC stakeholders and the CIRT team. This email list would only be open to staff of organizations that meet the criteria of a CIRT stakeholder. Subscriptions to this list will be controlled by CIRT staff who will vet people wishing to join to ensure they meet the criteria. Ongoing monitoring and participation by BNCSIRC staff will also be required. This service is relatively easy to implement and provides a visible and useful initial engagement with the stakeholders.

Meeting with Mr Clifford Bostic, Deputy Chief Telecommunications Officer, Division of Energy and Telecommunications Prime Minister's Office

Servers of the established CIRT which are located at the premises of the Telecom Division

6 LESSONS LEARNED

- For the establishment of national CIRTs, the beneficiary country needs to be prepared to procure the necessary hardware in a timely manner, related to the duration of a project. The procurement rules and procedures take time to apply in governments, which might result in delays of the overall implementation of the project. Therefore, the project duration needs to be carefully planned and beneficiary countries require to be well informed on these procurement related matters.
- To organize trainings before the deployment of the system, helped raise awareness and provided good insight on the overall importance and need on cybersecurity. However, additional hands-on trainings following the installation of the system would be beneficial. Such additional assistance would be very useful to quickly operationalize the established CIRT.

Meeting with Mr Charles Cyrus,
Director of the National Council for Science and Technology

7 CONCLUSIONS

Based on the interview sessions with key persons from the Barbados Administration and the different stakeholders, it can be concluded that :

- the project was implemented efficiently and effectively, the activities were completed, and the results were achieved as planned.
- the project addressed a genuine need for the country in the area of cybersecurity. To this end, all stakeholders underlined the importance of having a national platform to handle cyber-attacks, communicate alerts and coordinate activities on the safety of critical infrastructure.
- assistance provided to the Barbados Administration was very timely and appropriate, considering the fact that it is most often the government entities that are prone to cyber threats. This issue is becoming much more imminent, especially with the recent plans of the government to provide governmental services over the internet.
- the project also contributed to raise awareness on cybersecurity and created a sense of urgency on this subject. The training on cybersecurity which was organized within the project, was also attended by the different project stakeholders. Involvement of the stakeholders will also benefit the future operations of the CIRT, as the system requires all related and interested parties to be connected.

Meeting with Ms. Ashell Forde,
Telecommunications Officer in charge of the CIRT

8 RECOMMENDATIONS

Computers have become such an integral part of our daily activities that computer-related risks cannot be separated from business, health, and privacy risks. Valuable country assets and critical national infrastructures are now over the Internet at risk.

It is important for governments to create and identify a national organization that will serve as a focal point to secure cyberspace and protect critical information infrastructure, through surveillance, warning, response and recovery efforts, as well as facilitate collaboration between government entities, the private sector, academia, and the international community, when dealing with cybersecurity issues. The establishment of Barbados NCIRT will help ensure the protection of the nation's critical information infrastructures, assist in drafting a national roadmap on the country's approach to cybersecurity related issues, and serve as a focal point for further build and implement a national cybersecurity culture.
The following recommendations are made concerning the establishment of a national CIRT in Barbados:

- Further awareness raising activities are needed to highlight the importance of coordination among government entities in cybersecurity related matters.
- Review of the current national ICT strategy and consider including cybersecurity related matters in the next ICT strategy.
- Encourage different stakeholders to take part in CIRT related activities and trainings.
- The established national CIRT needs to start providing service to other government entities and stakeholders to get subscribed.
- Additional guidance from ITU could be provided to the Barbados Administration, based on their future cybersecurity needs.

The 9BAR13002 project will be formally closed. A closure report will be prepared by the ITU Project Manager.

9 ANNEX

LIST OF PERSONS MET

- Mr. Clifford Bostic, Deputy Chief Telecommunications Officer, Division of Energy and Telecommunications Prime Minister's Office
- Ms. Ashell Forde, Telecommunications Officer in charge of the CIRT, Division of Energy and Telecommunications Prime Minister's Office
- Mr Charles Cyrus, Director, National Council for Science and Technology
- Mr. Andy Parris, President & CEO, Trustworthy Systems inc. (TSi)
- Mr. Anthony Greenidge and Mr. Ian Wood, Senior Managers for IT Advisory, KPMG
- Mr. Andrew Linton and Mr. Matt Gibson, Program Directors at Ozone Wireles

ITU Projects

ITU Headquarters, Geneva, Switzerland

Email: Bdtprjhq@itu.int

Tel: +41 22 730 6090

www.itu.int/en/ITU-D/Projects/