CYBERSECURITY

READINESS ASSESSMENT

FOR ESTABLISHING A NATIONAL CIRT

(AFGHANISTAN, BANGLADESH, BHUTAN, MALDIVES AND NEPAL)

Report

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

ITU

JANUARY 2012
Telecommunication Development Sector

Readiness assessment for establishing a national CIRT (Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal)

January 2012

IMPACT
INTERNATIONAL MULTILATERAL PARTNERSHIP AGAINST CYBER THREATS

ITU

The International Telecommunication Union commissioned the CIRT assessment of Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal in cooperation with national consultants of those countries, International Multilateral Partnership Against Cyber Threats (IMPACT) experts, and supported by the Department of Broadband, Communications and the Digital Economy (DBCDE) of the Government of Australia.

This report was compiled from reports carried out by Mr Anju Singh and Mr Jagdish Singh, Mr Sivanathan Subramaniam under the supervision and direction of the International Telecommunication Union (ITU) Regional Office for Asia and the Pacific, Bangkok.

ITU) would like to express sincere gratitude to Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal for their support and cooperation by providing valuable inputs for the preparation of this report. In particular, we would like to convey our appreciation to Mohammad Yousaf (Afghanistan), Shamsuzzoha (Bangladesh), Sonam Dudka, (Bhutan), Mohamed Nasih (Maldives), and Swoyambhu Man Amatya (Nepal) for their support for data/information collection and coordination as well as local arrangements necessary for making the study achieve its objectives. We would like to express our special gratitude to the DBCDE of the Government of Australia for their support.

FOREWORD

The International Telecommunication Union (ITU) in partnership with the International Multilateral Partnership Against Cyber Threats (IMPACT) advocates the establishment of national CIRT (Computer Incident Response Team) to identify, defend, respond and manage cyber threats and enhance cyberspace security in the sovereign country. This needs to be coupled with the gathering of its own intelligence instead of relying on secondary reporting of security incidents from CIRT constituencies or other sources.

This framework of a fully organized and operational CIRT model is beginning to be adopted by many national governments in their national information security master plan or equivalent.

A fundamental role of ITU, following the World Summit on the Information Society (WSIS) and the 2010 ITU Plenipotentiary Conference (specifically Resolution 130[1]), is to build confidence and security in the use of information and communication technologies (ICTs). Heads of state and government and other global leaders participating in WSIS, as well as ITU Member States, entrusted ITU to take concrete steps towards curbing the threats and insecurities related to the Information Society.

The ITU Global Cybersecurity Agenda (GCA) provides a framework within which the international response to the growing challenges to cybersecurity can be coordinated and addressed in response to its role as Facilitator for WSIS Action Line C.5.

The World Telecommunication Development Conference (WTDC) held in Hyderabad, India in 2010, adopted Programme 2 on Cybersecurity, ICT applications and IP-based network-related issues, as well as Resolution 69[2], clearly underlining the importance to ITU Members of the issue of Cybersecurity for the next four year developmental cycle.

As Director of the Telecommunication Development Bureau, I am committed to implementing the decisions of Member States related to achieving global cybersecurity, and I am convinced that the development and deployment of core capabilities such as CIRTs will contribute to the overall objective.

I will therefore work with all other stakeholders to ensure that countries are properly equipped to fight cyberattacks and cybercrime, in order to create a safe, peaceful, and secure cyber environment for all.

Brahima Sanou
Director, Telecommunication Development Bureau

---

[1] Strengthening the role of ITU in building confidence and Security in the use of information and communication technologies.

[2] Creation of national computer incident response teams, particularly for developing countries, and cooperation between them.

TABLE OF CONTENTS

Page

Page

CHAPTER 1
INTRODUCTION

1.1 Background

The International Telecommunication Union and a team of experts from IMPACT, carried out readiness assessment of cybersecurity situation in five least developed countries in the South Asia to review the institutional and regulatory framework, existing critical information infrastructure, and identify areas of improvement and recommend suggestion for establishing a Computer Incidence Response Team (CIRT). This assessment was carried out as an input to the ITU Ministerial Forum held from 3-5 August 2010 in Maldives which resulted in a ministerial declaration resolving priority areas *inter alia* for cybersecurity in Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal (ABBMN).

1.2 Objectives

The objectives of the CIRT assessment study were to assess the capability and readiness to build a sustainable national CIRT, based on an analysis of stakeholder attributes with relevance to security incident response needs of ABBMN countries. The national CIRT will identify, respond and manage cyber threats and at the same time enhance cybersecurity.

The other objectives and deliverables of the assessment study were to:

i. conduct cybersecurity readiness assessment of the country;

ii. propose institutional and organizational requirements and arrangements for the establishment of the national CIRT;

iii. make the necessary recommendations that will improve cybersecurity readiness of the ABBMN countries;

iv. provide a phased implementation approach to establish a national CIRT with the relevant solutions and documentation;

v. recommend a manpower plan for the national CIRT; and

vi. provide any other recommendations or plans pertaining to the national CIRT establishment.

1.3 What is a national CIRT?

A national CIRT responds to computer security or cybersecurity incidents by providing necessary services to a defined constituency to effectively identify threats, coordinate actions at national and regional levels, disseminate information, and act as a focal point for the constituency in matters related to cybersecurity. CIRTs primarily focus on the response to ICT related security incidents on behalf of one or more stakeholders. In order to provide an overarching cybersecurity service to a constituency, most CIRTs offer services such as reactive services, proactive services and security quality management services. There are several acronyms used to describe teams providing similar types of services such as CSIRC, CSRC, CIRC, CSIRT, IHT, IRC, IRT, SERT and SIRT[4].

[4] The definitions are derived from Incident Prevention, Warning, and Response (IPWAR) Manual, USDOE, 205.1-1, September 2004 and also Handbook for Computer Security Incident Response Teams (CSIRT), 2nd Edition, April 2003.

1.4 The need for a national CIRT

The trends and statistics speak for themselves, and the rapidly increasing number of cyber attacks is now a global trend. Cyber attacks which were previously launched only for nuisance purposes or by "script-kiddies" have now escalated into more catastrophic attacks motivated by money, political agendas and in some cases as weapons of cyberterrorism.

From among all cyber threats, targeted attacks have the most impact. The motivations for such attacks can range from theft, such as phishing, to critical information gathering leading to a larger impact attack, such as a major disruption to telecommunications infrastructure. Targeted attacks have also grown in sophistication by striking from distributed bases.

The fundamental role of government in the fight against cyber threats is to:

- ensure the continuity of society in times of crisis;
- protect essential services and critical national infrastructure;
- improve resistance to disruption;
- contain contagion;
- restore control of information dissemination;
- recover a state of normality quickly;
- identify trends and vectors of cyber attacks; and
- train personnel as responders.

This role will be ensured by the national CIRT.

1.5 Benefits of having a national CIRT

Having highlighted what a national CIRT is and the need to establish one, the benefits of establishing a national CIRT are to:

- serve as a trusted focal point within and beyond national borders;
- identify and manage cyber threats that may have adverse affect on the country;
- respond systematically to cybersecurity incidents and take appropriate actions;
- help the constituency to recover quickly and efficiently from security incidents and minimise loss or theft of information and disruption of services;
- utilise information gained during an incident handling to better prepare for handling of future incidents and to provide for protection of systems and data;
- deal properly with legal issues that may arise during incidents;
- endeavour to exchange knowledge within the constituency;
- make general security best practices and guidance available through publications, websites, and other modes of communications;
- promote or undertake the development of education, awareness and training materials appropriate for a variety of different audiences;
- identify and maintain a list of CIRT capabilities and points of contact.

The establishment of a national CIRT is as essential as having emergency services such as a fire department and a police force and the benefits cannot be trivialised. Figure 2.1 shows how ITU-IMPACT illustrates the roles and responsibilities that a national CIRT can play in protecting against cyber threats and potentially drive and promote initiatives such as national cybersecurity strategies, policies, cyber

forensics services, national Public Key Infrastructure (PKI), digital signatures, governance, legislation, Critical Information Infrastructure Protection (CIIP), cybersecurity awareness, training and education, research, international cooperation, and security assurance.

Figure 1: The roles and responsibilities of national CIRTs as IMPACT sees them

1.6 Assessment methodology

The on-site assessment and off-site documentation were carried out ITU-IMPACT experts. The on-site assessment methods include meetings, training, interview sessions and site visits. The meetings and face-to-face interview sessions are conducted using a questionnaire and responses gathered were used to assess the need for and existing capability of national cybersecurity mechanisms. The information gathered was also used to form the recommendations for a plan of action which is outlined in this report.

1.7 Assessment justification

The readiness assessment is divided into focal areas that point out the issues, details the findings and analysis conducted, as well as recommends solutions to the issues. The focal areas include the ICT readiness of the country, cyber threats affecting the country, cybersecurity/ICT legislation, common standards/regulatory framework, constituency/stakeholder participation, cybersecurity training and education, physical infrastructure and operational aspects, and the financial model to be adopted.

CHAPTER 2
READINESS ASSESSMENT

This chapter describes the readiness assessment methodology adopted for carrying our CIRT Assessment for Afghanistan, Bangladesh, Bhutan, Maldives and Nepal, including background, key objectives, deliverables, and the benefits of having a national CIRT.

2.1 Readiness assessment: Afghanistan

This section contains all the key findings from the assessment including, key issues, analysis and recommendations for the enhancement of the cybersecurity situation in Afghanistan. These findings are based on the information gathered during the on-site assessment and general research conducted by the expert.

2.1.1 ICT readiness of Afghanistan

Key Issues

The main areas that were observed and found to be key issues of ICT readiness for Afghanistan were:

i. No robust or reliable ICT Infrastructure.

ii. Current levels of Internet penetration are still low and thus the cybersecurity awareness and knowledge among the Afghan people are still growing.

iii. Low usage of ICTs in both public and private sectors although the public sector is showing signs of improvement.

iv. The general public lacks knowledge of ICTs and people have to travel outside Afghanistan to obtain this knowledge and skill-sets.

v. Power outages are quite common in the country due to unreliable power supply.

Key Findings and Analysis

From the on-site meetings and interviews conducted, the following information was gathered:

i. The overall reliability and robustness of ICT infrastructure and services is the main reason for the low ICT penetration rate among the private and public sectors. Currently, the majority of the country still depends on microwave and wireless communications which do not provide good bandwidth for data connections.

   According to ITU statistics (annual country data by region on Internet indicators[5]), there are only about two Internet users per 100 inhabitants in Afghanistan.

ii. It is expected that by March 2010, the Afghanistan Optical Fibre Cable Ring Project, the biggest fibre optic project in the country, will be completed. The optical fibre will connect the entire country and the adjacent countries, such as Turkmenistan, Uzbekistan, Tajikistan and China, which exposes the country to more cybersecurity risks and threats. The faster Internet connection, which will result from this project, may provide a safe haven for cybercriminals.

[5] www.itu.int/ITU-D/icteye/Indicators/Indicators.aspx#

Table 1 – Internet indicators: subscribers and users 2008

Internet Usage – Afghanistan 2008			
Subscribers (000s)	**Subscribers per 100 inhabitants**	**Users (000s)**	**Users per 100 inhabitants**
1.2	-	500	1.84

iii. The E-Government Interoperability Framework (e-GIF) has been drafted and it is expected to be rolled-out by April 2010. This project will enable all governmental systems to interoperate (virtually operate as a single large system). The interconnection will definitely introduce new risks and cyber threats to the systems.

iv. A new state-of-the-art National Data Centre (NDC) was launched in October 2009 and will host all government websites, applications and emails. In other words, most of the government sensitive and confidential data will be hosted at the NDC.

v. Some of the banks are already providing online banking services but the current services are limited to static services, whereby customers can only login to view their account balance or statement but no transactions can be performed.

vi. The Government is also planning to introduce a smart card system for the general public to replace the current paper-based identity card which can be easily duplicated. The smart card will contain personal information, driving licence and possibly international passport details.

vii. Other government initiatives in ICT such as National Internet Exchange Point (NIXA)[6] and National Internet Registry (NIRA) will bring the ISP communities within the country onto a single platform which will require proper regulations and policies to manage them and avoid disputes. There are currently 24 ISPs licensed by the Afghanistan Telecom Regulatory Authority (ATRA).

viii. Other ICT based services are also slowly creeping into the market such as M-PAISA – a mobile phone based money transfer service.

ix. The Afghanistan Network Information Centre (AFGNIC) is responsible for the administration of IP address assignments and registrations. To date they have registered more than 2,000 domains and they are also planning to provide online registration.

x. The universities or colleges in Afghanistan have recently started offering degree courses in computer science but the academic sector does not have suitable courses in cybersecurity.

Recommendation

i. Improve the overall readiness, availability and reliability of ICT infrastructure by including mirror sites and backup. It is necessary to provide a reliable infrastructure for IT operations, in order to minimize any chance of disruption to critical applications initiated. The current state-of-the-art National Data Centre (NDC) needs to have reliable backups including physical backup in order to maintain availability of critical applications. Basic antivirus protection software should be provided to client PCs in all government agencies to contain the spread of viruses and malware.

ii. Training, specifically in the area of Cybersecurity, needs to be improved in order to raise the level of ICT readiness.

iii. Awareness on the current government ICT initiatives needs to be enhanced to increase the usability of these applications.

[6] ITU Provided assistance to MCIT for establishment of Afghanistan Internet Exchange under Special Concentrated Assistance in 2009.

iv. The implementation and continuous improvement of a cybercrime legislation would need to complement ICT readiness.

v. Suitable regulatory framework for development of telecommunication infrastructure as well as services provided by the Internet Service Providers need to be developed to cater for constant technological innovations.

2.1.2 Cyber threats affecting Afghanistan

Key Issues

i. There seems to be an absence of suitable mechanisms to identify, detect or deter cyber threats within government sectors. The private sector may have such mechanisms but the information is often not shared with government sectors. Some government agency PCs are not equipped with appropriate and reliable protection software, i.e. antivirus, to block malware and viruses.

ii. Some government agencies claim that they have never experienced any sort of cyber attack. There are two possible reasons for this, either they are not keen to share the attack information, or they do not know that they are being or have been attacked. The network of the country is much dispersed and thus the detection of cyber incidents is very difficult.

Key Findings and Analysis

Even though there were no reported cases of severe cyber attacks, some patterns of attacks were detected by government agencies involving the internet directly or indirectly. The following information from on-site meetings and interviews was gathered:

i. The lack of incidents reported by government departments may mean that either the incidents go undetected or there is no central point to monitor and keep track of incidents.

ii. The Afghanistan Telecom Regulatory Authority (ATRA) received the most reports of attacks. However, the attacks are mostly GSM-based attacks because of the high penetration rate (more than 10 million subscribers as of 2009). ATRA has also received many complaints from customers on illegal activities and threatening e-mails.

iii. One of the leading banks also received death threats and slanderous e-mails but when they were reported to ATRA nothing could be done because there were no mechanisms to take appropriate action. The bank also experienced lots of virus and malware attacks.

iv. ATRA also suspects that their radio database is being attacked and infiltrated and sensitive information is being accessed.

v. One of the ISPs claims that they experience attempted Denial of Service (DoS) or Distributed DoS attacks to their servers every now and then but they have never experienced any serious downtimes.

vi. MCIT also claims that there was an incident of “ping to death” back in 2004 or 2005 on government networks.

vii. There was also an incident where NATO’s network was hacked from a dial-up connection and the relevant ISP’s servers were confiscated to conduct further investigation to track the perpetrator.

viii. An ISP also experienced losses of approximately AFN 2 million on a mobile phone prepaid top-up card fraud.

ix. In another isolated case in 2007, it was reported that a victim lost USD 40,000 to a phishing scam.

x. In 2008, there was a widespread scam in the form of a web-based pyramid scheme. Plenty of Afghanis fell victim to this scam.

xi. There are also many reported attacks on using SIM cards to make long distance calls without being charged. Various police reports were made but an effective solution to this problem is not in place.

xii. Owning a credit card is fast becoming a fashion statement in Afghanistan and there have already been reported credit card frauds.

xiii. With any Internet connected system, the threat from external sources is high and, similarly, internal threats cannot be ignored either. Some of the Government's top secret and secret data are kept on servers which are not connected to the Internet but the risks from the inside must be taken into consideration as well.

xiv. Without appropriate security controls and mechanisms and the ability to monitor and detect attacks, it would not be possible to manage the risks however they manifest themselves.

xv. Some university domains were badly infected by virus attacks from disks and CDs used by students on the network due to the absence of antivirus software. Administration of user accounts was affected with the outburst of virus attacks that blocked users from logging in.

Recommendation

i. It is clear from the above findings that the setting up of a National CIRT to manage incidents from a central point is crucial. Awareness of the need to report all incidents to this central point is vital. The CIRT will also provide knowledge of available best practises that can be shared and implemented on their respective networks.

ii. It is also recommended that in the future, large organizations that are responsible for the country's critical national infrastructure should establish their own CIRTs in collaboration with AfCIRT.

2.1.3 Cybersecurity / ICT legislation

Key Issues

There are two main areas of concern for cybersecurity or ICT legislation:

i. Lack of cybercrime legislation hindering law enforcement investigations.

ii. Some of the telecommunication regulations such as Afghanistan Telecommunication Law and Radio Regulation needs to be reviewed and updated to address the constantly changing technological and regulatory scenario due to convergence.

Key Findings and Analysis

i. The new draft ICT Law is expected to enable and facilitate electronic communications and transactions in the public interest. It covers almost every aspect of ICT; including security, electronic signatures, Public Key Infrastructure (PKI), admissibility and evidential weight of electronic evidence, Digital Rights Management (DRM), and Cybercrime.

ii. ATRA has a set of laws and regulations, but they also have a set of special procedures for the telecommunication industry developed by the ATRA board.

iii. Other than the above, no government agency or department seems to have any relevant information on security or cybersecurity related policies or procedures that are in place.

Recommendation

i. While there is a definite need for a CIRT capability, the need for cybercrime legislation is a more immediate requirement, or at least should be developed in parallel with CIRT capabilities.

ii. The creation of ICT related legislation, policies and frameworks needs to be technology neutral to cater for the dynamic nature of ICT technologies.

2.1.4 Common standards / regulatory frameworks

Key Issue

No awareness on common cybersecurity standards or regulatory frameworks.

Key Findings and Analysis

Government agencies and departments are not fully aware of the many cybersecurity standards that can be adopted to increase security, such as ISO/IEC 27001, COBIT, FISMA and ITIL.

Recommendation

i. With the establishment of a CIRT, knowledge of available best practices with regards to cybersecurity standards could be implemented.

ii. Training in the area of cybersecurity standards and regulatory frameworks needs to be provided to key personnel in government agencies.

2.1.5 Constituency / stakeholder participation

Key Issues

i. Constituencies are not willing to share information regarding cyber security incidents because of trust issues.

ii. Constituencies fear that by reporting incidents, their reputation may be tarnished by a failure to secure the network.

Key Findings and Analysis

i. The AfCIRT initiative has been welcomed by all stakeholders and constituencies, who also recognise the need to improve the level of awareness and security skills of ICT personnel within the country.

ii. Most stakeholders are eager to work together to establish the AfCIRT and to contribute with whatever means possible. However, any resistance from the constituencies to share information may be overcome by AfCIRT by earning their trust and nurturing it for the continued success and sustainability of the CIRT.

iii. Being the main stakeholder, MCIT agreed to allocate the necessary budget for the establishment and maintenance of AfCIRT.

iv. The stakeholders also recognised that AfCIRT should not become a white elephant project and become less effective once established.

v. Constituencies are afraid that their reputation will be tarnished if they admit to having been compromised or affected by cyber threats and will be singled out for not safeguarding their networks or information assets.

vi. Constituencies have also expressed their fear that by reporting vulnerabilities they are open to more attacks if the vulnerabilities are disclosed – again a trust issue.

Recommendation

i. Stakeholders and constituencies need to understand that the establishment of AfCIRT is imperative and will benefit them in dealing with cybersecurity incidents. The active participation

of the stakeholders and constituencies can be gained by ensuring and demonstrating the privacy and confidentiality of the information provided by them.

ii. The recommended type of service AfCIRT will be providing to its constituents in this case is hybrid services. Basically, there are three services provided by a CIRT to its constituents which are Bounded, Unbounded and Hybrid:

   a) **Bounded** – The service is bounded by some constraints such as just for the government or just for the funding source:

   b) **Unbounded** – The service is provided to anyone requesting it: and

   c) **Hybrid** – The combination of both services.

2.1.6 Local cybersecurity expertise

Key Issues

i. Currently there is very little cybersecurity expertise within the country.

ii. Hiring cybersecurity experts from outside the country is not encouraged due to the sensitive nature of Afghanistan-government-specific information that will be handled by AfCIRT.

iii. Due to the delicate security nature of the country, foreign experts may leave whenever security threats reach a critical level.

iv. Universities and colleges are not producing local cybersecurity expertise because of a lack of cybersecurity-specific courses available.

Key Findings and Analysis

i. From the interviews conducted with all the existing AfCIRT staff, it is concluded that the need to provide them with the right training and knowledge is paramount. Almost all of them are inexperienced and have never received any sort of cybersecurity related training.

ii. The interviewees are also unaware of any sources of cyber threat information on the Internet.

iii. None of the other stakeholders and constituencies have the human resources capacity to handle cybersecurity incidents. Most of them do not even have a basic knowledge of cybersecurity.

Recommendation

i. To improve the level of awareness and security skill-sets of the local ICT expertise by sending them for identified training. Prior to that, an assessment of training needs should be conducted to identify the right people to be sent for the right training.

ii. The ministries such as the Ministry of Higher Education together with MCIT and AfCIRT can develop a cybersecurity-specific syllabus to be made available in local colleges and universities.

iii. Occasionally, conduct awareness programmes in public places and government offices to improve levels of awareness.

2.1.7 Cybersecurity training and education in Afghanistan

Key Issues

i. No available training and education in cybersecurity in the country.

ii. There is also no local expertise to drive the development of local cybersecurity courses.

Key Findings and Analysis

Based on the information gathered, there is no single available cybersecurity-related training or education within the country because there is no demand from the local industry.

Recommendation

It is envisaged that IMPACT may conduct external training with the main intention of training the trainers. It is expected that Afghanistan will create cybersecurity experts through this initiative.

2.1.8 Current AfCIRT Physical Infrastructure

Key Issues

i. Office security only relies on human capabilities such as security guards and army personnel.

ii. Basic facilities and infrastructure such as proper lighting and elevator services are not in place.

iii. No operational policies and procedures are in place.

Key Findings and Analysis

i. The visit to the current AfCIRT premises provided a good view of its physical aspect, however it is not fit to host the AfCIRT due to its lack of security controls.

ii. The current location of AfCIRT servers was found to be without the standard requirements of security.

iii. The current AfCIRT office was also found to be inappropriate and too cramped for the AfCIRT staff to carry out the daily CIRT activities.

Recommendation

i. The security to the AfCIRT office needs to be installed with security fittings such as access control and CCTV surveillance systems.

ii. The office should have a working area large enough to fit the current staff of five people and a meeting room. Discussions and meetings pertaining to cybersecurity incidents should not be conducted outside of these premises.

iii. It is also recommended that all servers are transferred to the National Data Center which is equipped with the necessary security controls.

2.1.9 Financial Model

Key Issues

Justifying budget requests for initiatives such as AfCIRT can be a daunting task in a country such as Afghanistan which still lacks ICT penetration and no clear evidence of cyber attacks.

Key Findings and Analysis

i. It is clear that there is strong support from MCIT and the Government in general to fund the establishment of AfCIRT.

ii. A budget proposal for the establishment of AfCIRT was understood to have been submitted to the Ministry of Finance of Afghanistan.

Recommendation

It is envisaged that for a public private partnership, a financial model needs to be created.

2.2 Readiness assessment: Bangladesh

This section contains all the key findings from the assessment including, key issues, analysis and recommendations for the enhancement of the cybersecurity situation in Bangladesh. These findings are based on the information gathered during the on-site assessment and general research conducted by the expert.

2.2.1 ICT infrastructure

This section presents the findings on the standard of ICT infrastructure in Bangladesh, the extent of use of ICT facilities such as network infrastructure and access devices, and the level of dependency on ICT for communication of key components within the country's administration, governmental institutions, organizations as well as private entities.

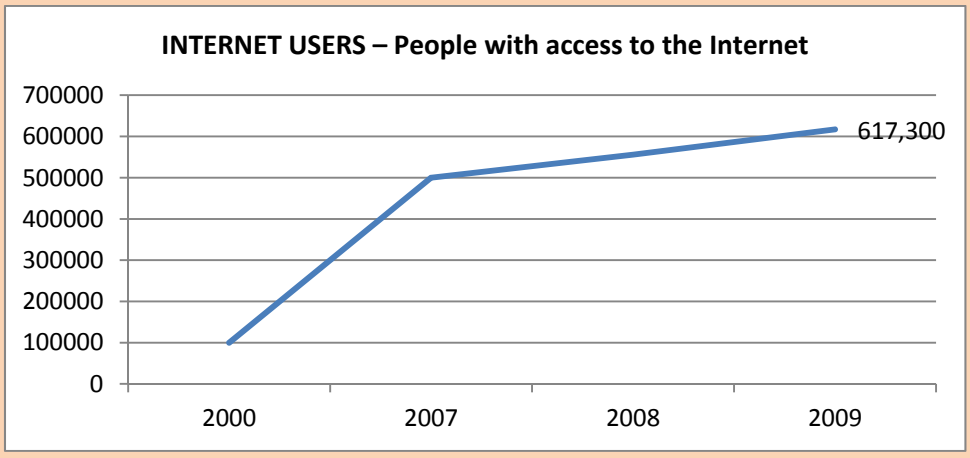
Key Findings, Issues and Analysis

From the on-site meetings and interviews conducted, the following information was gathered:

i. The telecommunication sector underwent a series of reforms starting from the mid-nineties that resulted in the expansion of ICTs in the country, nevertheless most projects are still in their early implementation phases and mostly limited to the capital city Dhaka and the major cities around Bangladesh. IT activities started in Bangladesh in 1993 with the introduction of e-mail service using dial-up connections offered by three Internet Service Providers (ISPs). In 1996, Bangladesh tested the Internet (VSAT-based) for the first time. Its high cost, however, limited access to the Internet to business users. The Bangladesh government decision to deregulate VSAT reduced this cost and opened the door for general users to access the Internet at a cheaper rate.

ii. As of March 2010, the Internet penetration rate reached 4.2 per cent[7] out of a total population of 162 million[8]. Nearly 6 million users access the Internet via GPRS/EDGE technology, and 1.2 million are corporate and home users, out of which around 1 million are broadband users (128 kbps).

Figure 2: Bangladesh number of Internet users[9]



[7] Latest Internet Penetration data provided by BTRC

[8] United Nation Estimate

[9] Data Source – International Telecommunication Union (ITU)

iii. There has been a sharp increase of mobile Internet users from 2009 to 2010 due to the increase of GPRS/EDGE services offered by mobile network operators.

iv. In 2008, Broadband Wireless Access (BWA) (WiMAX) licenses were awarded through open auction and the WiMAX network roll-out is being carried out by two companies; BanglaLion Communication and Augere Wireless Broadband Bangladesh Ltd.

v. Bangladesh joined the 14 nation SEA-ME-WE4 submarine cable consortium[10] to install submarine optical fibre cable to provide national broadband connectivity with information super highway access, thus enabling all ISPs, both public and private, to have direct access globally.

Figure 3: SEA-ME-WE4 submarine cable consortium

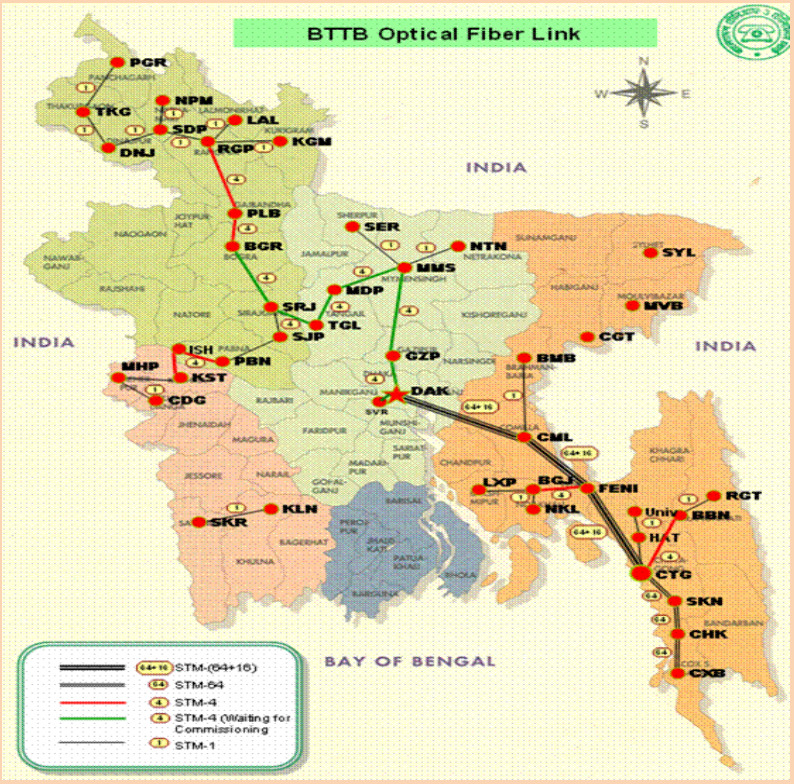
vi. Establishment of fibre optic links in Bangladesh began in 1986, along with the installation of new digital switches. Starting with the optical fibre link between Dhaka's Maghbazar and Gulshan telephone exchanges, all intra-city inter-exchange connections are now established through short distance fibre optic links. The inter-city portions between the major cities started with the completion of the STM-16 fibre link between Dhaka to Chittagong in 2001.

vii. The government published its "Vision 2021" which targets the establishment of a resourceful and modern country by 2021 through effective use of information and communication technology called "Digital Bangladesh". The philosophy behind "Digital Bangladesh" comprises ensuring people's democracy and rights, transparency, accountability, establishing justice and ensuring delivery of government services to all through maximum use of technology and with the ultimate goal of improving standards of living for all. Four elements of "Digital Bangladesh" have been emphasized: human resource development, people involvement, civil services, and use of information technology in business.

viii. There are 51 banks in Bangladesh; 41 local and 10 international banks. Bangladesh Bank (BB), being the monetary authority of the country, is at the forefront of the government's positive commitment to "Vision 2021" towards Digital Bangladesh. BB is introducing in stages services like e-banking, e-commerce, e-recruitment, e-tendering, mobile banking and automated clearing house services, and it is expected that all banks will comply to this requirement of offering these services by the end of 2010. All these are highly likely to increase the volume of phishing scams, credit card fraud, identity theft and other money related cybercrimes.

[10] www.buzz247.com/i/article/51/200/SEA-ME-WE-4-Submarine-Communication-Cable-System.html

Figure 4: BTTB optical fibre link[11]



ix. The use of pirated copies of software is widespread. The ITU/IMPACT expert also observed that the sale of pirated copies of software is common on Dhaka streets and markets. This is a major obstacle to ensuring security of systems, as they cannot receive the appropriate patches.

x. It was also noted that there is an e-Government framework at the ministerial level. All ministries, divisions, directorates, departments and autonomous organizations have web sites where all policy documents, forms, circular, orders, notifications, and information relevant to the public etc. are posted and regularly updated. There is a Bangladesh Government[12] web portal that provides information on the most popular citizen services by the Government of Bangladesh, the basic information of the structure of Bangladesh Government, current news, upcoming events and other important information and links.

xi. Bangladesh encourages local companies to produce its own software. The ICT policy states that the government will support start-up financial support to local software industries to boost the development of local software[13]. Whereas, on hardware, the government encourages local institutions and R&D organizations to research, design and manufacture specialised informatics equipment.

xii. There are in total about 300 legally registered ISPs in Bangladesh. MANGO Teleservices Ltd and Bangladesh Telecommunications Company Limited (BTCL) act as the International Internet Gateway (IIG). Following the introduction of the Bangladesh International Long Distance

11 www.btcl.gov.bd/home/main/map_optical.php

12 www.bangladesh.gov.bd/index.php?option=com_frontpage&Itemid=1

13 www.comminit.com/pdf/itpolicyNEW.pdf

Telecommunications Services (ILDTS) Policy[14], all international data traffic pass through a legitimate IIG. All the ISPs are connected to these IIGs to get the international Internet bandwidth (IP bandwidth). The IIGs are connected to the Point of Presence (PoP) of the submarine cable company to get to the International Private Leased Circuit (IPLC). BTCL (the former government owned incumbent Bangladesh Telegraph and Telephone Board ('BTTB')) has been awarded one IIG license through open auction, while privately owned Mango Teleservices was awarded a license[14]. Along with the submarine cable bandwidth, both IIGs have redundant international connectivity through the satellite IP bandwidth of BTCL. Following a recent policy amendment, the Government of Bangladesh has decided to award more IIG licenses.

xiii. There are steps being taken to increase telecommunications and Internet coverage in Bangladesh. These include the reduction of Internet tariffs and offering lower fees and charges for ISPs (as a result of VSAT deregulation).

The above findings show that the Government of Bangladesh is very positive in bringing in technology. It is, therefore, of the utmost importance to implement the right tools and methods to protect the infrastructure.

Recommendations

i. The decision makers at governmental and ministerial levels need to take into account and accord due priority to security, reliability and availability of systems in all ongoing ICT infrastructure projects. The principle of defence in depth should also be adopted by government in all projects related to ICT. Bangladesh is at the stage of incorporating new ICT technologies to its Critical National Information Infrastructure (CNII) and this transition needs systems to be designed with adequate security.

ii. Suitable regulatory framework for development of telecommunication infrastructure and Internet Service Providers need to be developed to cater for constant technological innovations.

iii. Officials should take steps to discourage the use of pirated software. Awareness on security and basic computer safety should be raised.

iv. Training, specifically in the area of cybersecurity is needed in order to raise the level of ICT readiness.

v. Preparation and investment in back-up solutions to frequent power outages and Internet connection discontinuity is needed.

vi. Drafting of a disaster recovery plan should be initiated as soon as possible.

vii. An acceptable set of standards for equipment, applications and security policies should be established to ease ICT management and efficiency.

viii. Government should formulate a coordinated ICT investment strategy for all parts of the country.

ix. The implementation of and continued improvement of cybercrime legislation is needed to complement ICT readiness.

2.2.2 Cyber threats affecting Bangladesh

The need for CIRT services in a country has already been highlighted in chapter 1 of this report. Mitigating and eradicating cyber threats affecting a country is definitely one of the critical factors when establishing a national CIRT. This section discusses the key findings, issues, analysis and recommendations concerning cyber threats affecting Bangladesh. The findings in this section are based on stakeholder accounts and information provided by some key personnel. The stakeholders provided the information regarding the

[14] www.btrc.gov.bd/licensing/guidelines/iig_guidelines.pdf

threat landscape in Bangladesh. Often there were few or no supporting documents to substantiate their facts.

Key Findings, Issues and Analysis

i. Overall, there is no proper organization or mechanism dealing with detection, tracking and mitigation of cyber attacks and cybercrime at the governmental level. Isolated cases are treated on an ad-hoc basis either by the Police Cybercrime Unit in the Criminal Investigation Department (CID) or the unofficial private CIRT that was started by a few motivated individuals or by the victims themselves.

ii. On 20 March, 2010, hackers attacked 20 district websites operated by the Prime Minister's Office. The hackers threatened Bangladesh with a cyber war. The Minister for Science and ICT told newspapers that the hackers broke into the system apparently to get "secret information". It is obvious here that cyber security was not implemented and to mitigate the problem, an expert meeting, to help strengthen cyber security and prevent cyber attacks was held at the Prime Minister's Office on 29th March 2010. The Access to Information (A2I) programme coordinated the effort and two committees were formed in that meeting, one for formulating a policy regarding cyber security and the other for taking necessary steps if a cyber attack takes place.

iii. Suspected vandalism on BTCL physical infrastructure disrupted telephone and Internet services for several days. On Friday, 11 June 2010, 4100 pairs of underground cable were damaged by City Corporation workers while working at Tejgaon-Aarong Link Bridge. Consequently, 3500 phone lines under Gulshan Exchange in Tejgaon, Niketan, East-Nakhalpara and surroundings were out of order[15]. This indicates possible vulnerability to acts of sabotage and the physical security vulnerability of the country's infrastructure.

iv. ICT infrastructure, computer systems and users in Bangladesh are exposed to and suffer from most types of cyber threats and attacks affecting the rest of the world, including malicious software, electronic fraud, web defacement, and email account hacking.

v. Online scams by means of social engineering e-mails such as the Nigerian 419 scams and phishing websites go hand in hand with identity theft. This has created concerns in the Bangladesh cyberspace, and on the international scene. The people of Bangladesh have also fallen victim to swindlers in the past and lost large sums of money.

vi. In 2008, a Bangladeshi petty hacker named Shahi Mirza occupied the Rapid Action Battalion (RAB) web site. In his confession to the police, Mirza claimed that he hacked not only the RAB web site, but he had also been hacking domestic and international web sites for a long time. He invaded at least 21 domestic web sites including the web site of the Bangladesh Army.

vii. An analyst of Premium Bank Brokerage House, Mahbub Saroar[16], was reported to have robbed nearly 5 million Taka from investors of the Dhaka Stock Exchange, by disseminating misleading share-tips to his Face Book friends manipulating prices of certain shares in the Dhaka Stock Exchange. While in police custody Mahbub allegedly provided startling information about Internet fraud.

Based on the gathered information, there is no clear defence strategy in place in case of a major cyber attack on government infrastructure. Most of the interviewees have no clue of what to do in the event of a cyber crisis in Bangladesh. The findings above are incidents that have been reported. There might be many others that have not been reported. This is the main concern.

---

15 www.btcl.gov.bd/

16 http://rezwanul.blogspot.com/2010/03/bangladesh-police-arrest-facebook-stock.html

Recommendations

i. It is clear from the above findings that the setting up of a national CIRT as a focal point to manage incidents and as a coordination centre to manage information sharing and information flow for cybersecurity is crucial. Awareness of the need to report all incidents to this central point is vital. The CIRT will also provide knowledge of available best practises that can be shared and implemented on their respective networks.

ii. It is also recommended that in the future, large organizations that are responsible for critical national infrastructure should establish their own CIRTs in collaboration with the national CIRT. These would be known as sector CIRTs and they would be constituents of the national CIRT.

iii. Stakeholders should adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organizations to connect to the Internet.

iv. Outreach programmes should be developed to increase public awareness of the dangers associated with cyber threats. Training and education should be conducted to teach users basic steps for dealing with IT security issues.

v. Create a database to record complaints, which will be examined together with other agencies like national CIRT, Interpol, Cybercrime Unit in the Criminal Investigation Department (CID), Rapid Action Battalion (RAB) and other institutions like banks, ISPs and so forth that will help in tracking cyber criminals.

vi. Develop and/or update the legal framework to make Bangladesh less favourable as a cyber crime haven for criminals. The government together with its agencies should draft and pass cyber crime laws which should be used to criminalise all forms of electronic fraud.

vii. The government agencies should start using security features such as encryption, PGP, SSL, SSH to secure their communications.

2.2.3 Cybersecurity legal framework

Mitigating and eradicating cyber threats affecting a country cannot be done by just using technologies and services. It has to be coupled with a robust and up to date legal framework to cater for the dynamic nature of ICT environments and cybercrime tactics. This section discusses the key findings, issues, analysis and recommendations for the cybersecurity legal framework in Bangladesh.

Key Findings, Issues and Analysis

i. There is no comprehensive cybersecurity law enacted or adopted yet. ICT related crimes are usually treated under the existing penal code.

ii. However, an expert meeting to help strengthen cyber security and prevent cyber attacks was held at the Prime Minister's Office (PMO), on 29 March, 2010. Two separate committees were formed to formulate two policies -- one for ensuring cyber security and the other for taking necessary steps if a cyber attack takes place.

iii. The Government of Bangladesh in its active fight against cyber threats has approved in principle to amend previous legislation calling for jail terms and heavy financial penalties to tackle new forms of crime[17]. The proposed law has suggested provisions for a maximum 10 years in jail and Taka 10 million (USD 150, 000) in fines for hacking into computer networks and putting false and libellous information or indecent material online.

[17] www.futuregov.net/articles/2009/apr/22/bangladesh-plans-strict-cyber-crime-laws/

Recommendations

i. Stakeholders should expedite the process of amending or passing of cyber laws because delays give cyber criminals the chance to exploit legal loopholes. The legal framework should be able to address not only national issues, but facilitate and foster international cooperation. ITU-IMPACT would support and assist[18] Bangladesh to ensure that national cyber laws would be developed within international cooperation principles.

ii. The rapid changes in technology and attack vectors require amendment and review of cyber laws in order to combat cybercrime and it is highly recommended that the Bangladesh Government expedites the process of passing the necessary laws.

iii. It is important to develop and implement awareness campaigns to educate users, law enforcement and policy makers about cyber laws, the impact of cybercrime and measures of combating it. The national CIRT can take on the leading role of creating cybersecurity awareness campaigns.

iv. Due to rapid changes in technology, there is a need to create laws which are technology neutral in order to cater for the dynamic nature of ICT technologies.

v. While there is a definite need for a CIRT capability, the need for cybercrime legislation is currently a more immediate requirement. A national CIRT capability should at least be developed in parallel with drafting and passing of cyber laws. Without cyber laws, a national CIRT cannot perform its duties effectively.

2.2.4 ICT regulatory framework

This section discusses the key findings, issues, analysis and recommendations for the ICT regulatory framework in Bangladesh.

Key Findings, Issues and Analysis

i. The Bangladesh Telecommunication Regulatory Commission (BTRC) regulates the establishment, operation and maintenance of telecommunication services in Bangladesh as per Bangladesh Telecommunication Act 2001 and advises the government on information and telecommunication policy.

ii. In 2009, the Bangladesh Government, spearheaded by MoSICT adopted a national ICT policy which includes action items for realizing the goals of national development. The National ICT Policy 2009 is a revision of the National ICT Policy 2002.

iii. All Bangladesh ISPs are regulated by BTRC.

Recommendations

i. The regulators such as BTRC and implementers such as MoSICT should have adequate personnel with cybersecurity technical skills and relevant knowhow to handle matters related to national cybersecurity. These people can drive the national agenda for protection and regulation of CNII by forming working groups or forums for cybersecurity where they can actually collaborate with various stakeholders within the government.

ii. Rural communications development programmes should be continued to ensure equitable distribution of technology services throughout the country.

iii. BTRC and MoSICT should encourage the use of relevant standards and best practices.

[18] www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

iv. It is recommended that training in the area of cybersecurity standards and regulatory frameworks is provided to key personnel in government agencies.

2.2.5 Critical National Information Infrastructure (CNII)

CNII is a term used to describe information assets that are essential for the functioning of a society and economy. The alarming rise of premeditated attacks with potentially catastrophic effects on interdependent networks and information systems across the globe, has demanded that significant attention should be paid to critical information infrastructure protection initiatives of a sovereign country. This section discusses some key findings, issues, analysis and recommendations for the Bangladesh CNII.

Key Findings, Issues and Analysis

Listed below are the critical sectors in Bangladesh identified during the interview sessions with the stakeholders:

i. banking and finance,
ii. information and communications,
iii. power and energy,
iv. health services,
v. water and food services,
vi. national defence and security,
vii. transport,
viii. government, and
ix. emergency services.

There is no defined cybersecurity strategy in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber attack on the critical national infrastructure.

Recommendations

i. Since the CNII sectors are well defined, it is recommended that Bangladesh start formulating national strategies such as a National Cybersecurity Policy (NCP) to safeguard its CNII sectors. References can be made to frameworks such as National Cybersecurity Framework[19] that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

ii. The NCP should recognise the critical and highly interdependent nature of the CNII and aim to develop and establish a comprehensive programme and a series of frameworks to ensure the effectiveness of cybersecurity controls over vital assets. The policy should be developed to ensure that the CNII are protected to a level that is commensurate with the risks faced[20].

iii. Terms of reference for the NCP should include, but not be limited to:

- standard cybersecurity systems across all elements of the CNII,
- strong monitoring and enforcement of standards, and

[19] A generic national framework for CIIP: www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

[20] International CIIP Handbook: An Inventory and Analysis of National Protection Policies: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

- development of a standard cybersecurity risk assessment framework for the country.

2.2.6 Constituency / stakeholder participation

A constituency is the specific community that the national CIRT is established to serve. Stakeholders are the people who will be involved in the planning, strategy and decision making of the national CIRT. Stakeholder organizations can also be a part of the constituency. This section discusses the key findings, issues, analysis and recommendations for constituency and stakeholder participation in forming the BdCIRT.

Key Findings, Issues and Analysis

The major stakeholders that expressed their enthusiasm to cooperate and contribute to the national CIRT study are the BTRC (hosting the BdCIRT), banks, national defence, ISPs and telecommunication operators. All the parties present agreed that CIRT services should be offered to government and other public institutions at the initial stage. However, their concern is that the private sector and the general public are also in dire need of an organization that responds to their incidents. It was, therefore, emphasized that the BdCIRT grows rapidly in order to accommodate the general public, or acquires the capacity to set up other CIRTs in a decentralized fashion to cater for the expanding number of future constituencies.

i. It was agreed that the BdCIRT should also give priority to Critical National Information Infrastructure.

ii. A national CIRT will be needed for the general public in order to give consumers confidence in online transactions. The Bangladesh population needs a reliable organization that guarantees some level of safety and tracking of offenders / cybercriminals with the rapid growth of Internet services in the past few years and years to come.

Recommendations

i. One of the critical success factors of a national CIRT is the active participation from stakeholders and constituencies in information sharing and coordination work. The involvement from these parties should start from the very beginning, as early as the planning stage of the BdCIRT establishment. Once established, the BdCIRT is responsible for earning and nurturing the trust of the stakeholders and the constituencies.

ii. Constituents need to understand that the establishment of BdCIRT is imperative and will benefit them in dealing with cybersecurity incidents at the national level. The active participation of the stakeholders and constituents can be gained by ensuring and demonstrating that the privacy and confidentiality of their information will never be compromised and will be protected to the best of its ability.

iii. The recommended and targeted type of service BdCIRT will be providing to its constituents is Hybrid Services. However, at its initial stage the services will be more bounded to government agencies and ministries. Once it has reached a certain maturity, it shall start rendering its services to anyone requesting them which will give it the hybrid status. Basically, there are three kinds of services provided by a CIRT to its constituents:

   - **Bounded** – The service is bounded by some constraints such as just for the government or just for the funding source:
   - **Unbounded** – The service is provided to anyone requesting it, and
   - **Hybrid** – The combination of both services.

2.2.7 Local cybersecurity expertise

One of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise. Many CIRTs have failed because of this specific reason. This section discusses the key findings, issues, analysis and recommendations for local cybersecurity experts in Bangladesh.

Key Findings, Issues and Analysis

i. From the information gathered and research conducted by the ITU/IMPACT expert, it can be concluded that there are very few locally produced cybersecurity experts in Bangladesh. This is mainly attributed to the fact that universities, colleges and other local training institutions do not have adequate cybersecurity-specific courses.

ii. The idea of hiring foreign cybersecurity experts is not fully favoured due to the lack of trust when it comes to sensitive governmental information.

iii. All stakeholders and constituent organizations recognized that there is a strong need for training of individuals in cybersecurity. However, those with IT and networking backgrounds in stakeholders' organizations could be eligible to undertake cybersecurity courses.

Recommendations

i. One of the most pressing issues at the moment is the establishment of the national CIRT and getting the correct technical expertise to operate and maintain it. This can be achieved by sending the identified candidates for appropriate training and seminars be it locally (if available) or abroad. This does not have to wait until the right set of education programmes or training are made available within the country (which is discussed in the next section).

ii. To establish the national CIRT, stakeholders should conduct a talent search to identify the right people with the right attitude and qualifications to man the CIRT. Training needs assessments should also be conducted to identify the right set of courses that the identified personnel should sign up to.

iii. The ministries such as Ministry of Higher Education together with MoSICT and the proposed national CIRT can develop a cybersecurity-specific syllabus that can be made available in local colleges and universities.

iv. Occasionally the proposed national CIRT can conduct awareness programmes in public places and in government offices to increase levels of awareness.

v. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programmes relevant to cybersecurity areas with college and university students. The research programmes can be coupled with rewards such as scholarships or employment to encourage more participation.

vi. ITU in collaboration with IMPACT could assist in developing local expertise by leveraging scholarship programmes that are available for countries through its partnership with various world-renowned training providers.

2.2.8 Cybersecurity education and training

As discussed, one of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise due to the limited availability of cybersecurity education and training programmes in Bangladesh. This section discusses the key findings, issues, analysis and recommendations for cybersecurity education and training in the country.

Key Findings, Issues and Analysis

i. Cybersecurity education in Bangladesh is limited to occasional seminars, workshops and regional conferences that some of the participants have attended in the past. Apart from that, proper cybersecurity courses or subject are not available at national universities.

ii. More often than not, the local institutions depend on foreign expertise in developing courses.

iii. Some of the local students and IT experts, especially in the ISP industry, are aware of cybersecurity certification courses overseas, but they don't know how to have access them, or lack the financial means to take the courses without a sponsor as the cost is often too high for them.

Recommendations

i. One of the most important elements in establishing and sustaining a national CIRT is the competency of the personnel. Training and human capacity development programmes must be in place to have locally produced experts.

ii. Through partnerships and MoUs, the government can bring in various cybersecurity training providers into the country and make the courses more easily accessible to the people. Scholarship programmes can also be offered to encourage the Bangladeshi people to venture into cybersecurity areas.

iii. It is imperative for Bangladesh to start including cybersecurity in the syllabus of higher education institutions. This has to be done before it is too late due to the rapid development and outreach of latest technologies within the country. Stakeholders such as Ministry of Higher Education, MoSICT and BTRC etc. need to collaborate to make this happen.

iv. ITU in collaboration with IMPACT can assist in helping Bangladesh and the stakeholders to design courses and promote research programmes through its various divisions.

2.3 Readiness assessment: Bhutan

This section contains all the key findings from the assessment including, key issues, analysis and recommendations for the enhancement of the cybersecurity situation in Bhutan. These findings are based on the information gathered during the on-site assessment and general research conducted by the expert.

2.3.1 ICT infrastructure

This section presents the findings on the standard of ICT infrastructure in Bhutan, the extent of use of ICT facilities such as network infrastructure and access devices, and the level of dependency on ICT for communication of key components within the country's administration, governmental institutions, organizations as well as private entities.

Key Findings, Issues and Analysis

From the on-site meetings and interviews conducted, the following information was gathered:

i. Telephone links in Bhutan were first introduced in the mid 1980s, on a microwave system, and the first satellite earth station was commissioned in 1990. A telecom network, constructed between 1992 and 1999, was the most critical foundation for the development of ICT. A decade after the introduction of ICT infrastructure, Internet access was introduced to Bhutan on 2 June 1999.

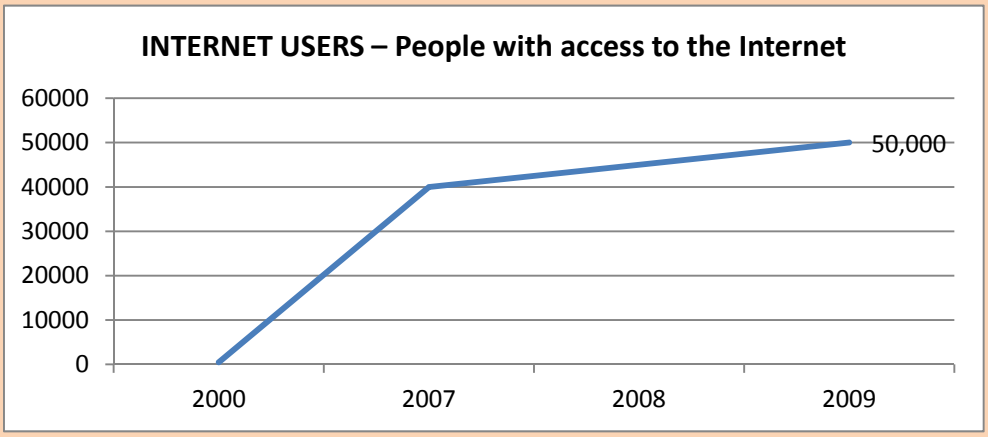
ii. Due to landlocked nature of the location, Bhutan faces geo-demographic constraints for the roll-out of ICT infrastructure, including harsh terrain and small scattered populations. The expensive infrastructure cost against the small population does not give a strategic business edge to most

providers. As such, Bhutan has capitalised on mature technologies including using power lines for connection.

iii. Bhutan Telecom Limited (BTL), in 2004, installed an Optical Ground Wire (OPGW) transmission system with Synchronous Transport Module (STM)-1 capacity connecting Thimphu, Paro and Phuentsholing over the Bhutan Power Corporation's (BPC) 66kV transmission lines. International connectivity is also provided via satellite earth station in Thimphu, which connects voice traffic to London, Tokyo and Singapore. All district headquarters are connected, either via the microwave backbone or 8Mbps radio links[21]. With the expansion of international bandwidth, BTL launched DSL-based broadband services on 1 March 2008 and, as of August 2008, it covers 15 dzongkhags (districts).

iv. Internet penetration rate in 2010 reached 7.1 per cent[22] of a population of 699,8416. The number of Internet users rose from 2009 to 2010 by only 5,000 users. The increase is concentrated at Thimpu, Bhutan's capital. Aside from government offices, there are very few personal computers (26 personal computers per 1,000 people)[23] and the use of computers is limited to urban areas only.

Figure 5: Bhutan number of Internet users[24]



v. Banks in Bhutan have launched Internet banking services, including account inquiries, cheque book requests, internal fund transfers, and loan repayments. This is highly likely to increase the volume of phishing scams, identity theft and other money related cybercrime.

vi. The use of pirated copies of software is widespread. The ITU/IMPACT expert also observed that the sale of pirated copies of software is common on Bhutan markets. This is a major obstacle to ensuring security of systems, as they cannot receive the appropriate patches.

vii. It was also noted that there is an e-government framework at the ministerial level implemented by DIT. Establishment of ICT units in all government ministries is considered to be an important step. There is a web portal of Bhutan Government[25] that provides information on the most popular citizen services by the Government of Bhutan, basic information on the structure of Bhutan Government, current news, upcoming events, and other important information and links.

---

21 BIPS Update July, 2009 www.doim.gov.bt/doc/policy/bips_update.pdf

22 www.internetworldstats.com/asia/bt.htm

23 www.estandardsforum.org/system/briefs/235/original/brief-Bhutan.pdf?1274217068

24 Data Source – International Telecommunication Union (ITU)

25 www.bhutan.gov.bt/government/index_new.php

The portal received a boost with the completion of the Thimphu WAN connecting 42 of 72 listed organizations. The Thimphu WAN allows these organizations to access each other's websites and other online resources at very high speed. However, the Thimphu WAN is at present available only in the capital. There are plans for the laying of fibre optic connections in all dzongkhag and geog (districts and sub-districts). DIT is currently piloting an electronic signature system with UNDP and ITU support which will be a key part of a fully-fledged e-government systems infrastructure[26].

viii. The Government of Bhutan encourages local companies to produce their own software although most of the off-the-shelf software is currently imported. ICT equipment is already exempted from import duty and ICT companies have been accorded a tax holiday.

ix. Two ISPs, DrukCom Private Enterprise and Samden Tech Pvt Ltd, were licensed in 2004 to provide VSAT-based Internet and value added services (VAS). These new ISPs have done away with the monopoly enjoyed by DrukNet of BTL and created a competitive market. Due to their presence in the market, the cost of Internet services such as leased lines and web hosting has been reduced, connectivity has been enhanced, and new services such as broadband have been introduced.

x. Since 2003, the Royal Government of Bhutan, in cooperation with ITU and other partners, has been revamping post offices in remote and rural locations into ICT centres, allowing rural inhabitants to join the information society[27].

The observations above show that the Government of Bhutan is very proactive and amenable to bringing new technological solutions into the country[28]. As the ICT infrastructure is in its infancy, it is of utmost importance to implement the right tools and methods to protect the critical information infrastructure of the country.

Recommendations

i. The decision makers at governmental and ministerial levels need to take into account and allocate sufficient priority to security, reliability and availability of systems in all ongoing ICT infrastructure projects. The principle of defence in depth should also be adopted by the government in all the projects related to ICT. Bhutan is at the stage of incorporating new ICT technologies to its Critical National Information Infrastructure (CNII) and this transition needs systems to be designed with adequate security.

ii. Regulations for telecommunications and ISPs in the area of cybersecurity need to be developed to cater for constant technological improvements.

iii. Officials should take steps to discourage the use of pirated software at least at the government level. Awareness on security and basic computer safety should be raised.

iv. Training, specifically in the area of cybersecurity is needed in order to raise the level of ICT readiness.

v. Preparing and investing in back-up solutions for power outages and Internet connection discontinuity.

vi. Drafting a disaster recovery plan should be initiated as soon as possible.

vii. An acceptable set of standards for equipment, applications and security policies should be established to ease ICT management and efficiency.

---

26 www.idrc.ca/en/ev-140931-201-1-DO_TOPIC.html

27 www.itu.int/net/itunews/issues/2010/05/22.aspx

28 www.kuenselonline.com/modules.php?name=News&file=article&sid=10277

viii. Government should formulate a coordinated ICT investment strategy in areas to secure the critical information infrastructure for all parts of the country.

ix. The implementation of and continued improvemet of cybercrime legislation[29] is needed to complement ICT readiness.

2.3.2 Cyber threats affecting Bhutan

The need for CIRT services has already been highlighted in chapter 1 of this report. Mitigating and eradicating cyber threats affecting a country is definitely one of the critical factors when establishing a national CIRT. This section discusses the key findings, issues, analysis and recommendations concerning cyber threats affecting Bhutan. The findings in this section are based on stakeholder accounts and information provided by some key personnel. The findings in this section are based on stakeholder accounts. The stakeholders provided the information regarding the threat landscape in Bhutan. Often there were few or no supporting documents to substantiate their facts.

Key Findings, Issues and Analysis

i. Overall, there is no proper organization or mechanism dealing with detection, tracking and mitigation of cyber attacks and cybercrime at the governmental level. Isolated cases are treated on an ad-hoc basis either by the ISPs or computer related government departments.

ii. On 16 July 2010, the Paro district court sentenced an employee of the National Housing Development Corporation (NHDC) to one year in prison, in the first ever online defamation case in Bhutan. The defendant was ordered to pay compensatory damages of Nu. 36,000 (USD 772) each to a couple, both forest rangers, within one month of the judgment[30].

iii. On 19 June 2010, local ISP Druknet had around 50 of its websites hacked. Users trying to access certain websites hosted by the ISP were greeted with a blank home page and a message that said the website had been hacked[31].

In 2007, a tour operator in Thimpu lodged a complaint against his former partner for hacking into his email account and deleting tourist enquiries. The case is said to be still being investigated because the accused has fled the country[32].

i. GhostNet is a large-scale cyber spying operation discovered in March 2009. A computer can be controlled or inspected by attackers, and even has the ability to turn on camera and audio-recording functions of infected computers, enabling monitors to perform surveillance. Compromised systems were also discovered in Bhutan.

ii. ICT infrastructure, computer systems and users in Bhutan are exposed to and suffer from most of the cyber threats and attacks affecting the rest of the world. These include malicious software, electronic fraud, web defacement, and email account hacking.

iii. Online scams by means of social engineering e-mails such as the Nigerian 419 scams and phishing websites go hand in hand with identity theft. This has created concerns on the international scene and if not addressed, would also create concerns in the Bhutan cyberspace.

Based on the information gathered, there is no clear defence strategy in place in case of a major cyber attack on government infrastructure. Most of the interviewees have no clue of what to do in the event of

[29] www.judiciary.gov.bt/html/act/PENAL%20CODE.pdf – chapter 31

[30] http://kuenselonline.com/modules.php?name=News&file=article&sid=8762

[31] www.kuenselonline.com/modules.php?name=News&file=print&sid=15822

[32] www.kuenselonline.com/modules.php?name=News&file=article&sid=8628

cyber crisis in Bhutan. The Royal Bhutan Police has recently taken the step to create a sub-division that will deal with Cybersecurity.

The findings above are incidents that have been reported. There might be many others that have not been reported. This is the main concern.

Recommendations

i. It is clear from the above findings that the setting up of a national CIRT as a focal point to manage incidents and as a coordination centre to manage all information sharing and information flow for cybersecurity is crucial. Awareness of the need to report all incidents to this central point is vital. The CIRT will also provide knowledge of available best practises that can be shared and implemented on their respective networks.

ii. It is also recommended that in the future, large organizations that are responsible for critical national information infrastructure should establish their own CIRTs in collaboration with the national CIRT. These would be known as sector CIRTs and they would be constituents of the national CIRT.

iii. Stakeholders should adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organizations to connect to the Internet. ISPs, for example, need to deploy and maintain proper monitoring systems at the international gateways to track and block malicious traffic from infecting the information infrastructure. This, to a certain extent, ensures the availability of services, systems and data for the subscribers.

iv. Outreach programmes should be developed to increase public awareness about the dangers associated with cyber threats. Training and education should be conducted to teach users basic steps for dealing with IT security issues.

v. Create a database to record complaints which will be examined together with other agencies like national CIRT, Interpol, Cybercrime Unit of the Royal Bhutan Police and other institutions like banks, ISPs and so forth that will help in tracking cyber criminals.

vi. Develop and/or update the legal framework to make Bhutan less favourable as a place for cyber crime criminals. The government together with its agencies should draft and pass cyber crime laws which should be used to criminalise all forms of electronic fraud.

vii. The government agencies should start using security features such as encryption, PGP, SSL, SSH to secure their communications.

2.3.3 Cybersecurity legal framework

Mitigating and eradicating cyber threats affecting a country cannot be done by just using technologies and services. It has to be coupled with a robust and up to date legal framework to cater for the dynamic nature of ICT environments and cybercrime tactics. This section discusses the key findings, issues, analysis and recommendations for the cybersecurity legal framework in Bhutan.

Key Findings, Issues and Analysis

i. There is no comprehensive cybersecurity law enacted or adopted yet. ICT related crimes are usually treated under the existing penal code[33] of Bhutan under Chapter 31.

ii. All provisions relating to cybersecurity issues and offences are based on Bhutan Information, Communication and Media Act 2006 (BICMA)[34] under chapter 7 – PROVISIONS RELATING TO CYBER ISSUES.

[33] www.judiciary.gov.bt/html/act/PENAL%20CODE.pdf

Recommendations

i. Stakeholders should expedite the process of amending or passing of cyber laws because delays give cyber criminals the chance to exploit legal loopholes. The legal framework should address not only national issues, but facilitate as well international cooperation. ITU-IMPACT would support and assist[35] Bhutan to ensure that national cyber laws would be developed within international cooperation principles.

ii. The rapid changes in technology and attack vectors require amendment of outdated cyber laws in order to combat cybercrime and it is highly recommended that the Bhutan Government expedites the process of passing the necessary laws.

iii. It is important to develop and implement awareness campaigns to educate users, law enforcement and policy makers about cyber laws, the impact of cybercrime and measures of combating it. The national CIRT can take on the leading role of creating cybersecurity awareness campaigns.

iv. Due to rapid changes in technology, there is a need to create laws which are technology neutral in order to cater for the dynamic nature of ICT technologies. This is one of the best ways to combat cybercrime effectively.

v. While there is a definite need for a CIRT capability, the need for cybercrime legislation is currently a more immediate requirement. A national CIRT capability should at least be developed in parallel with drafting and passing of cyber laws. Without cyber laws a national CIRT cannot perform its duties effectively.

2.3.4 ICT regulatory framework

This section discusses the key findings, issues, analysis and recommendations pertaining to the ICT regulatory framework in Bhutan.

Key Findings, Issues and Analysis

A Telecommunications Act was passed in 1999, a Copyright Act in 2000, and the Bhutan Information, Communications and Media Act was passed in 2006. Bhutan is building its institutional capacity to regulate and support ICT activity through the Department of Information and Media (DoIM), Department of Information Technology (DIT) and Bhutan InfoComm and Media Authority (BICMA), and the establishment of ICT units in ministries to assist them harness the potential of ICT.

All ISPs in Bhutan are regulated by BICMA.

Recommendations

i. The regulators such as BICMA and implementers such as DIT need to have adequate personnel with cybersecurity technical knowhow to handle matters related to national cybersecurity. These people can drive the national agenda for protection and regulation of CNII by forming working groups or forums for cybersecurity where they can actually collaborate with various stakeholders within government.

ii. Rural communications development programmes should be continued to ensure equitable distribution of technology services throughout the country.

iii. DIT and BICMA should encourage the use of relevant standards and best practices.

---

[34] www.dit.gov.bt/legislations/bicmact.pdf

[35] www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

iv. It is recommended that training in the area of cybersecurity standards and regulatory frameworks is provided to key personnel in government agencies.

2.3.5 Critical National Information Infrastructure (CNII)

CNII is a term used by governments to describe information assets that are essential for the functioning of a society and economy. The alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe has demanded that significant attention is paid to critical information infrastructure protection initiatives. This section discusses the key findings, issues, analysis and recommendations for the Bhutan CNII.

Key Findings, Issues and Analysis

Listed below are the critical sectors in Bhutan identified by the stakeholders during the interview sessions:

- banking and finance,
- information and communications,
- power and energy,
- health services,
- sater and food services,
- national defense and security,
- transport,
- government, and
- emergency services.

There is no defined cybersecurity strategy in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber attack on critical national infrastructure.

Recommendations

i. Since the CNII sectors are well defined, Bhutan should start formulating national strategies such as a National Cybersecurity Policy (NCP) to safeguard its CNII sectors. Generic frameworks[36] that comprise legal, regulatory, technology, public-private cooperation, institutional, and international aspects are available.

ii. The NCP should recognise the critical and highly interdependent nature of the CNII and aim to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. Policy should be developed to ensure that CNII is protected to a level that is commensurate with the risks faced[37].

iii. Terms of reference for the NCP should include, but not be limited to:
    - standard cybersecurity systems across all elements of the CNII,
    - strong monitoring and enforcement of standards, and
    - the development of a standard cybersecurity risk assessment framework for the country.

---

[36] A generic National Framework for CIIP.
URL: www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

[37] International CIIP Handbook: An Inventory and Analysis of National Protection Policies.
URL: www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

2.3.6 Constituency / stakeholder participation

A constituency is the specific community that the national CIRT is established to serve. Stakeholders are the people who will be involved in the planning, strategising and decision making of the national CIRT. Stakeholder organizations can also be a part of the constituency. This section discusses the key findings, issues, analysis and recommendations for constituency and stakeholder participation in forming the BtCIRT.

Key Findings, Issues and Analysis

i. The major stakeholders that expressed their enthusiasm to cooperate and contribute to the national CIRT project are: the DIT (hosting the BtCIRT), BICMA, banks, national defence, ISPs and telecommunication operators.

ii. The stakeholders recognized the imminent need to establish a national CIRT, BtCIRT, and are willing to give their full support. All the parties present agreed that CIRT services should be offered to government and other public institutions at the initial stage. However, their concern is that the private sector and the general public are also in dire need of an organization that responds to their incidents. It was therefore emphasized that BtCIRT grows rapidly in order to accommodate the general public, or acquires the capacity to set up other CIRTs in a decentralized fashion to cater to the expanding constituency in the future.

iii. It was agreed that the CIRT should also give priority to Critical National Information Infrastructure.

iv. A national CIRT will be needed for the general public in order to give consumers confidence in transacting online. Bhutan population needs a reliable organization that guarantees some level of safety and tracking of offenders/cybercriminals with the rapid growth of Internet services in the past few years and years to come.

Recommendations

i. One of the critical success factors of a national CIRT is the active participations from the stakeholders and the constituencies in information sharing and coordination work. Involvement of these parties should start from the very beginning, as early as the planning stage of the CIRT establishment. Once established, the CIRT has a burden of earning and nurturing the trust of the stakeholders and the constituencies.

ii. Constituents need to understand that the establishment of BtCIRT is imperative and will benefit them in dealing with cybersecurity incidents at the national level. The active participation of the stakeholders and constituents can be gained by ensuring and demonstrating that the privacy and confidentiality of their information will never be compromised and will be protected to the best of its ability.

iii. The recommended and targeted type of service BtCIRT will be providing to its constituents is **Hybrid Services**. However, at its initial stage the services will be more bounded to government agencies and ministries. Once it has reached a certain maturity, it shall start rendering its services to anyone requesting them which will give it the hybrid status. Basically, there are three kinds of services provided by a CIRT to its constituents:

- **Bounded** – The service is bounded by some constraints such as just for the government or just for the funding source:
- **Unbounded** – The service is provided to anyone requesting it: and
- **Hybrid** – The combination of both services.

2.3.7 Local cybersecurity expertise

One of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise. Many CIRTs have failed because of this. This section discusses the key findings, issues, analysis and recommendations for the local cybersecurity experts in Bhutan.

Key Findings, Issues and Analysis

i. From the information gathered and research conducted by the ITU/IMPACT expert, it can be concluded that there is a small pool of highly skilled ICT personnel in Bhutan. The private sector in general lacks sufficient technical and managerial skills to initiate innovative growth in ICT businesses. This is mainly attributed to the fact that the local universities, colleges and other local training institutions lack cybersecurity-specific courses. Bhutan produces only about 100 or less IT graduates per year.

ii. The idea of hiring foreign cybersecurity experts is not favoured due to the lack of trust when it comes to sensitive governmental information.

iii. All stakeholders and constituent organizations recognized that there is a high need for training of individuals in cybersecurity. However, those with IT and networking backgrounds in stakeholder organizations could be eligible to undertake cybersecurity courses.

Recommendations

i. The most pressing thing at the moment is the establishment of the national CIRT and getting the correct technical expertise to operate it. This can be achieved by sending the identified candidates for appropriate training and seminars be it locally (if available) or abroad. This does not have to wait until the right set of education programmes or trainings are made available within the country (which is discussed in the next section).

ii. To establish the national CIRT, stakeholders should conduct a talent search to identify the right people with the right attitude and qualifications to man the CIRT. Training needs assessments should also be conducted to identify the right set of courses that the identified personnel should sign up to.

iii. The ministries such as Ministry of Education together with MoIC and the proposed national CIRT can develop a cybersecurity-specific syllabus that can be made available in local colleges and universities.

iv. Occasionally the proposed national CIRT should conduct awareness programmes in public places and also in government offices to increase levels of awareness.

v. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programmes relevant to cybersecurity areas with college and university students. The research programmes can be coupled with rewards such as scholarships or employment to encourage more participation.

vi. ITU in collaboration with IMPACT could assist in developing local expertise by leveraging scholarship programmes[38] that are available for countries through its partnership with various world-renowned training providers.

2.3.8 Cybersecurity education and training

As discussed, one of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise due to the limited availability of cybersecurity education and training

[38] www.impact-alliance.org/services_centre_training_partner.html

programmes in Bhutan. This section discusses the key findings, issues, analysis and recommendations for cybersecurity education and training in the country.

Key Findings, Issues and Analysis

i. Cybersecurity education in Bhutan is limited to seminars, workshops and regional conferences that some of the participants have attended in the past. Apart from that, proper cybersecurity courses or subject are not available at national universities.

ii. More often than not, the local institutions will have to depend on foreign expertise in developing courses.

iii. Some of the local students and IT experts especially in the ISP industry are aware of cybersecurity certification courses overseas, but they don't know how to have access to them, or lack the financial means to take the courses without a sponsor as the cost is often too high for them.

Recommendations

i. One of the most important elements in establishing and sustaining a national CIRT is the competency of the personnel. Training and human capacity development programmes must be in place to have locally produced experts.

ii. Through partnerships and MoUs, the government can bring in various cybersecurity training providers into the country and make the courses more easily accessible to the people. Scholarship programmes can also be offered to encourage the Bhutanese people to venture into cybersecurity areas.

iii. It is imperative for Bhutan to start including cybersecurity in the syllabus of higher education institutions. This has to be done before it is too late due to the rapid development and outreach of latest technologies within the country. Stakeholders such as Ministry of Education and MoIC should collaborate to make this happen.

iv. ITU in collaboration with IMPACT can assist Bhutan and the stakeholders to design courses and promote research programmes through its various divisions.

2.4 Readiness assessment: Maldives

This section contains all the key findings from the assessment including, key issues, analysis and recommendations for the enhancement of the cybersecurity situation in Maldives. These findings, issues, analysis and recommendations are based on the information gathered during the on-site assessment and general research conducted by the expert.

2.4.1 ICT infrastructure

This section presents the findings on the standard of ICT infrastructure in Maldives, the extent of use of ICT facilities such as network infrastructure and access devices, and the level of dependency on ICT for communication of key components within the country's administration, governmental institutions, organizations as well as private entities.

Key Findings, Issues and Analysis

From the on-site meetings and interviews conducted, we gathered the following information:

i. In August 2001, the Government of Maldives drafted a policy to reform the telecommunication sector. In the Maldives telecommunication policy 2001-2005, in order to reduce the digital divide within the country, the following was proposed:

- conduct ICT awareness and training programmes to promote the use of ICTs,

- establish community tele-centres throughout the country to provide affordable and easy Internet access,
- plan to establish a wideband data network connecting the entire country using the most appropriate technology, and
- develop human resources required for ICT needs of the country and retain them within the country.

ii. In general, this 2001 telecommunication policy achieved its targets. In 2006, the Maldives telecommunication policy 2006-2010 was introduced. It aims to expand the national telecom infrastructure to provide broadband services to all parts of the country without any discriminatory charges. Progress has been made but several projects still face delays because of lack of qualified personnel and government structure changes. However, the national ICT Policy, brainstormed in 2003, is still not completed.

iii. Dhiraagu introduced Internet to Maldives in October 2006 with dial-up connections for about 575 users. The Internet community in Maldives has grown rapidly over the past decade to reach 87,862 users in 2009[39]. This represents a penetration rate of 22.2 per cent of a total population of 396,334 (2009 census). As of 2009, Maldives counted 17,880 broadband Internet users.

iv. For Internet connections, Maldives had been relying solely on satellite technologies (VSAT) until 2005 for cost effectiveness reasons. Satellite is adequate for low traffic generated by a small country like the Maldives. The cost of access to existing cable consortiums for wide fibre bandwidth is high, so it seemed unnecessary nor could the cost be justified.

v. In 2005, the government revisited the feasibility and approved the decision to connect the Maldives to international submarine optical fibre cable. Watania, Focus Infocom and Reliance Infocom India formed the coalition WARF Telecom International and connected the Maldives in October 2006 to India, and later on with a second international gateway to Colombo, Sri Lanka.

vi. Maldives has a very high cellular communication penetration rate with 147.9 mobile subscribers per 100 inhabitants. All inhabited highlands have access to fixed line telephones with a teledensity of 15.89 per cent[40]. There are three licensed telecom operators, namely Dhiraagu that has been operating since 1988; Focus Infocom Raajjé (ROL) established in 2003, the country's second ISP and, Wataniya starting its operation in 2005.

vii. ADSL broadband Internet services are available over the fixed-line telephone network in Malé and 13 other islands. It reaches out to 40percent of the population with 11,530 ADSL lines and 1,076 ISDN lines[41].

viii. Broadband Internet is also available through cable TV networks (CATV) in the capital city Malé and a few other islands.

ix. Traditional Internet service providers are facing increasing competition from internet services offered by mobile operators. The introduction of GPRS and EDGE services has enabled many in Maldives to access the Internet through mobile devices.

x. Wataniya Telecom introduced 3G services and 3.5G HSDPA in 2008.

xi. The concern with such rapid changes in the ICT landscape is the lack of adequate provisions for cybersecurity to match this transformation.

---

39 ITU latest statistics on ABBMN countries dated 5 July 2010

40 See www.idrc.ca/en/ev-140978-201-1-DO_TOPIC.html accessed on: July 6 2010.

41 See Telecom & Statistics www.cam.gov.mv accessed on: July 6 2010

Table 2: Number of Internet users[42]

Year	2007	2008	2009
Internet Users	49,700	71,738	87,862

xii. Dhiraagu introduced mobile WiMAX in February 2010. Their mobile WiMAX currently covers 50 islands near to Malé Atoll and they are officially running the service in 27 islands within range to extend their broadband coverage. The tariff rates are fixed in a prepaid system currently consisted of three prepaid plans; two plans for home users, one at Rf 250 for 2GB and the other at Rf 449 for 4GB and one plan targeted for business users priced at Rf 1,900 for unlimited use. This is still considered costly and to some extend limits the expansion of Internet usage in Maldives.

xiii. There is another government project of establishing an independent network for emergency communications and distribution of early warnings in disaster situations.

xiv. In 2005, the Government of Maldives kick-started the implementation of the Government Network of Maldives (GNM). This project is lead by NCIT and consists of the physical and logical infrastructure enabling data exchange between government and government related organizations and the e-government Service Platform in a secure and reliable way. Certain services were launched by the end of 2009, for instance the Department of National Registration (DNR) can now enable some other organizations to access their database and share services electronically.

xv. E-government portals infrastructure is currently based on Microsoft SharePoint. This has been raising some concerns in terms of privacy and security since the back end of the software is only known by Microsoft Corp.

xvi. The physical infrastructure connects all the government organizations and related agencies in Malé and the 20 Atoll capitals by optical fibre, ADSL, and satellite network technologies. Fibre will be the main distribution network technology used and will be laid in Malé and the 20 Atoll capitals. In addition, ADSL technology will be used in Malé to connect some of the agencies housed in temporary locations. A nationwide VSAT network will be established to connect all the islands to Malé[43].

xvii. The Government of Maldives has established a computer network that connects the atoll capitals and government agencies. The network is based on optical fibre cable infrastructure in Malé and VSAT for the connection to atoll capitals.

xviii. The Information Technology Development Plan also allocates for the development of several intranet networks. The main intranets that will be created include an intranet for government agencies, an intranet for schools, an intranet for faculties of the Maldives College of Higher Education, an intranet for the Courts of Justice and an intranet for the police[44].

xix. Maldivians have been enjoying e-government services (at https://citizen.egov.mv/ and https://business.egov.mv/) including:

- national ID applications/ renewal,
- registration of births,
- scholarship applications,

---

42 ITU latest statistics on ABBMN countries dated 5 July 2010

43 See www.ncit.gov.mv/page.php/87/Government_Network_of_Maldives.htm accessed on: July 6 2010.

44 See www.ncit.gov.mv/page.php/87/Government_Network_of_Maldives.htm accessed on: July 6 2010.

- attestation of certificates,
- driving license renewals,
- police reports,
- government job applications,
- housing registrations,
- senior citizen allowances
- ambulance services,
- appeal for court cases,
- fishing vessel registrations,
- import /export declaration processes,
- Inward clearance of vessels, and
- registration of tourist resorts.

xx. However, citizen information on births contained in the national registration department database and the health database do not match.

xxi. Several online services are available to the public:

- online booking in the tourism industry has grown since 2002,
- web based SMS by Dhiraagu is popular, with a directory where customers can search for information by name or numbers (reverse directory), and
- the health department provides basic online information about disease, nutrition, and e-books.

xxii. The Ministry of Construction and Public Infrastructure has an online database called Harbour Permit and Mooring Database, which can be used to obtain information about the types of permits given to vessels using the inner harbour of Malé and Villingili.

xxiii. The e-payment platform for remittance and business transactions is available in Maldives, but the adoption is slow due to lack of awareness and the fact that the public still hold some fears about using such a system. However, withdrawing cash at ATMs for transactions can be a very tedious process as one needs to take a 1.5 hour boat trip to Malé for banking transactions. Bank of Maldives offers Internet banking, debit and credit cards facilities. Emergence of e-commerce services is also evident and has started to play an important role in everyday business.

xxiv. Other e-commerce solutions include eCommerce Maldives, Badhige an online food delivery service with a real-time online ordering system, and Raa atoll and Alifushi payment solutions.

xxv. In August 2007, the Bank of Maldives launched the Maldives Internet Banking (MIB) service, which allows customers to pay utility bills and do other bank transactions online.

xxvi. Maldives Monetary Authority (MMA), the central bank of Maldives, started the promotion of mobile phone banking in 2008. The system is designed with two components:

- an Electronic Funds Transfer Exchange, which would be both a software platform and a physical business unit to provide a clearing system for payments (similar to a cheque clearing system), answer customer queries, maintain the software, and sign up and maintain banking agents; and
- a network of banking agents comprised of shops and similar entities around the country to operate as cash handling points

xxvii. From 2006, NCIT has been supporting the implementation of an IT incubator project to boost the IT industry by hosting ICT manufacturing and software development companies among others. The pillars of the project are as follows:

- ICT Precinct (ICT infrastructure) to help provide key infrastructure necessary to enter into joint ventures with offshore firms;
- Applications Development Centre (ICT infrastructure) to provide application development expertise;
- Technology Incubator (ICT infrastructure) to provide a vibrant environment for young people to establish IT ventures and learn valuable business and technical skills;
- Project Loan Support (ICT usage) to provide ready access to development funds and financing;
- Mobile Commerce and Payments Trial (ICT usage) to provide a new baseline of activity and demonstrate the broader benefits and efficiency of electronic commerce;
- Strategic Alliance Program (ICT facilitation) to create the right environment for skill, knowledge and technology transfer and promote partnerships between local enterprises and offshore companies;
- ICT Cadets (ICT facilitation) to enable young people to explore career and entrepreneurial opportunities in the IT sector; and
- Skills Certification (ICT facilitation) to raise the ICT capability, level of professionalism and commercial orientation of the local industry.

xxviii. The use of pirated copies of software is still widespread. The representative reported that the sale of pirated copies of software is common in Maldives's streets and markets. The piracy rate stands at 95 percent. This is a major obstacle to ensuring security of systems, as they cannot receive the appropriate patches.

xxix. There are two licensed ISPs in Maldives. Dhiraagu and Focus Infocom's Raajje Online (ROL).

xxx. In terms of cybersecurity initiatives, the Department of defence and the Maldives Police Service initiated a Cyber-Crime Project in 2008 with the assistance of the Federal Bureau of Investigation (FBI).

Recommendations

i. The decision makers at governmental and ministerial levels need to take into account and allocate sufficient priority to security, reliability and availability of systems in all ongoing ICT infrastructure projects. Principle of defence in depth should also be adopted by government in all projects related to ICT. Maldives is at a stage of incorporating new ICT technologies to its Critical National Information Infrastructure (CNII) and this transition needs systems to be designed with adequate security.

ii. Regulations for telecommunication and Internet Service Providers need to be developed to cater for constant technological improvements.

iii. Officials should take steps to discourage the use of pirated software. Awareness on security and basic computer safety needs to be raised.

iv. Preparing and investing in back-up solutions to frequent power outages and Internet connection discontinuity.

v. Drafting a disaster recovery plan must be initiated as soon as possible.

vi. An acceptable set of standards for equipment, applications and security policies should be established to ease ICT management and efficiency.

vii. Government should formulate a coordinated ICT investment strategy for all parts of the country.

viii. The implementation of and continued improvement of cybercrime legislation is needed to complement ICT readiness.

2.4.2 Cyber threats affecting Maldives

The need for CIRT services has already been highlighted in chapter 1 of this report. Mitigating and eradicating cyber threats affecting a country is definitely one of the critical factors when establishing a national CIRT. This section discusses the key findings, issues, analysis and recommendations concerning cyber threats affecting Maldives. The findings in this section are based on stakeholder accounts and information provided by some key personnel. Often there were no supporting documents to substantiate their facts.

Key Findings, Issues and Analysis

The findings in this section are based on stakeholder accounts. The stakeholders provided the information regarding the threat landscape in Maldives. Representatives from CAM (Telecommunication Authority) took the time to discuss with the ITU/IMPACT expert and describe the threats and actual cybercrime cases they have encountered over the past few years.

i. Overall, there isn't any mechanism for reporting cybercrimes in Maldives. Facilities and skilled individuals to detect computer crime incidents are not widely available.

ii. Cybercrime in the Maldives ranges from credit card fraud and phishing to various forms of unauthorised access, hacking and defacement, child abuse (via chat) and social networking websites. For Instance, in April 2008, three Maldivians and one Malaysian were arrested by the Maldivian Police on charges of using fake credit cards to purchase Rf3.5 million worth of goods from shops[45].

iii. Fake SMS, SMS phishing and spam is also widespread in the Maldives.

iv. Maldives Police has revealed cases of fraud where people have been lured by the promise of employment by undertaking various courses. This is usually done by phone or email. The money is collected from the victim for course fees or rent.

v. Impersonation, mailbox theft, fake lottery prize, and credit card fraud are also means used by Maldives cybercriminals to steal money from foreigners.

vi. Several findings point to the vulnerability of systems in Maldives: e-banking systems only use basic authentication, no security standards are utilised, and government websites are frequently hacked into because of the poor security consideration in web development.

vii. A grey hat group "Jadecrew" has exposed vulnerabilities or hacked several key government portals[46]:

- In April 2010, http://egov.mv showed vulnerabilities that can lead to identity theft.
- The President's Office website www.presidencymaldives.gov.mv was hacked in April 2010, defaced, and usernames and passwords were displayed on the home page.
- The Maldives Stock exchange was hacked, www.mse.com.mv
- TAM/CAM, the Telecommunication Authority of Maldives website www.tam.gov.mv/index.php was reported to have been hacked in February 2010.

[45] See Maldives Live http://maldiveslive.blogspot.com/2008/04/three-maldivians-one-malaysian-arrested.html accessed on: July 7 2010

[46] See http://jadecrew.org/blog/ accessed on: 7 July 2010

viii. Similar cases of web defacement have been reported on government portals including, the immigration portal (www.immigration.gov.mv), the High Court (www.highcourt.gov.mv) and the elections Commission portal (www.elections.gov.mv) which were all hacked on the same day, 19 October 2009[47].

ix. Government servers are frequently under attack, but such incidents are usually not reported. The agencies concerned seek IT support from third party vendors.

x. Based on the gathered information, there is no clear defence strategy in place in case of a major cyber attack on government infrastructure.

Spam campaigns and e-mail chains containing viruses, and Trojan horse malwares easily infect PCs on government premises, universities and private sector organizations in general. Lack of knowledge on best practices is the main reason behind this problem. Most organizations do not take ICT security matters seriously, limiting protection to physical measures like firewalls.

Recommendations

i. It is clear from the above findings that the setting up of a national CIRT as a focal point to manage incidents, and as a coordination centre to manage information sharing and information flow on cybersecurity is crucial. Awareness of the need to report all incidents to this central point is vital. The CIRT will also provide knowledge of available best practises that can be shared and implemented on their respective networks.

ii. In the future, large organizations that are responsible for the country's critical national infrastructure should establish their own CIRTs in collaboration with the national CIRT. These would be known as sector CIRTs and they would be constituents of the national CIRT.

iii. Apart from certain mechanisms to track scammers, Maldives does not have any means or mechanism to recognise the kinds of malicious traffic that are flowing into or targeting the country. This can be tackled with the implementation of sensor networks (honeypots) at ISPs and international gateways to capture malicious traffic that target the country's systems. These sensors are decoy systems that will trick attackers into thinking that they are attacking real systems and will enable the operators of the sensors to capture information like malware, originating sources of attacks and network traffic information for further detailed study and trend analysis

iv. Stakeholders should adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organizations to connect to the Internet. It is recommended that network operators and service providers take technical measures to secure their network access.

v. Outreach programmes should be developed to sensitise the public about the dangers associated with cyber threats. Training and education should be conducted to teach users basic steps for dealing with IT security issue.

vi. Record complaints and create a database, which will be examined together with other agencies like national CIRT, INTERPOL, immigration, forensic bureau, prisons, police and other institutions like banks and so forth that will help in tracking cyber criminals.

vii. Once the CIRT has been setup it is highly encouraged that it gains membership with International organizations such as FIRST (Forum of Incident Response and Security Teams), IMPACT and regional CIRT establishments. These organizations are very experienced in coordinating and collaborating in cybersecurity matters and will provide the national CIRT with a good platform to share information.

[47] See www.zone-h.org/archive/domain=MV accessed on: 7 July 2010

viii. Develop and/or update the legal framework to make Maldives less favourable as a cybercrime haven for criminals. The government together with its agencies should draft and pass cybercrime laws which should be used to criminalise all forms of electronic fraud.

ix. Private businesses, especially the banks, should work together with the police to fight cyber crime. This can be made easier by the banks sharing information regarding internal bank fraud with the police. The police should also keep this information confidential in order to build trust between the two parties.

x. The government agencies and ministries should deploy secure communication infrastructure by employing tools such as encryption and GRC (Governance, Risk and Compliance). Encryption can be chosen from a vast variety of algorithms and technologies such as PGP, TrueCrypt, RSA, SSL and SSH to secure their communications[48].

2.4.3 Cybersecurity legal framework

Mitigating and eradicating cyber threats affecting a country cannot be done by just using technologies and services. It has to be coupled with a robust and up to date legal framework to cater for the dynamic nature of ICT environments and cybercrime tactics. This section discusses the key findings, issues, analysis and recommendations for a cybersecurity legal framework in Maldives.

Key Findings, Issues and Analysis

i. Presently, in Maldives there are no specific or comprehensive cyber laws enacted. The criminals can technically always get away with their offenses because there aren't specific laws to counter their illicit activities. However, there are laws though not directly related to cybercrimes but in a way can, to a limited extent, be used to deal with this issue. The applicable laws in some cases are part of the ordinary national penal code.

ii. The draft Telecommunications Act was completed in 2007 and is now awaiting approval by the Citizen's Majlis. The bill will be taken up during the 1st or 2nd session of the Citizen's Majlis in 2009. In the meantime, the Maldives Telecommunications Regulation 2003 is being implemented[49].

iii. Although there are no cyber laws, the issue of cybercrime has been taken into account in other laws being drafted. The current telecom policy cites the need for cyber laws[50].

iv. Some of the telecommunication regulations are somewhat outdated and thus insufficient to cater for current needs and technology.

v. The two legal bodies currently reviewing all laws and working on drafts for eighty new laws are the Attorney General's office and the Prosecutor General's Office.

vi. In the meantime, due to the lack of comprehensive cyber laws and inadequate training with digital forensics evidences, authorities do not have sufficient back up to prosecute cybercriminals. The delay in enacting laws is allowing the fast development of cyber crime activity, empowered by the growing availability of technology and cyber crime tools in Maldives.

vii. The mechanism for regional cooperation across national boundaries to solve and prosecute cyber crimes is complex and slow, mostly because the legal framework for the prosecution of cyber criminals is inadequate. Investigations and prosecutions of cyber criminals are technically and legally complex and it is difficult to manage the speed of information gathering.

---

48 **PGP** stands for Pretty Good Password; **SSL** stands for Secure Sockets Layer; **SSH** stands for Secure Shell Tunneling

49 See www.idrc.ca/en/ev-140978-201-1-DO_TOPIC.html last accessed on: 7 July 2010.

50 See www.idrc.ca/en/ev-140978-201-1-DO_TOPIC.html last accessed on: 7 July 2010.

viii. Legal protection of intellectual property rights especially software is also very weak.

Recommendations

i. Stakeholders should expedite the process of amending or passing of cyber laws because delays give cyber criminals the chance to exploit legal loopholes. Such legal framework should be able to address not only national issues, but also facilitate international cooperation. ITU-IMPACT would support and assist Maldives to ensure that national cyber laws would be developed within international cooperation principles.

ii. The rapid changes in technology and attack vectors require amendment of outdated cyber laws in order to combat cybercrime and it is highly recommended that the Maldivian Government expedites the process of passing the necessary laws.

iii. It is important to develop and implement awareness campaigns to educate users, law enforcement, and policy makers about cyber laws, the impact of cybercrime and measures of combating it. The national CIRT can take on the leading role of creating cybersecurity awareness campaigns.

iv. Due to rapid changes in technology there is a need to create laws which are technology neutral in order to cater for the dynamic nature of ICT technologies. This is the best way to combat cybercrime effectively.

v. While there is a definite need for a CIRT capability, the need for cybercrime legislation is currently a more immediate requirement. A national CIRT capability should at least be developed in parallel with drafting and passing of cyber laws. Without cyber laws a national CIRT cannot perform its duties effectively.

2.4.4 ICT regulatory framework

This section discusses the key findings, issues, analysis and recommendations for ICT regulatory framework in Maldives.

Key Findings, Issues and Analysis

i. Maldives's regulatory body of telecommunications is the Communications Authority of Maldives (CAM). Created in 2003, among other duties CAM is responsible for approval of operating licenses to telcos, ensuring the provision of qualitative and efficient telecommunication services throughout the country including the regulation of the Internet. CAM also advises the Government on information and telecommunication policy and creates an environment conducive to fair competition and developing the sector in line with the national policies and regulations. CAM is not only the regulator, but also a facilitator and promoter of coordinated and sustainable growth and development of the Maldives communications sector.

ii. The main regulation that CAM endorses is the 2003 Presidential Decree, the Maldives Telecommunications Regulation 2003.

iii. However, these regulations do not efficiently cater for the Internet.

iv. Some of Maldives' Internet traffic is non-local and highly decentralised, such traffic like the one routed through VSAT backbones from overseas is outside the control of the Government.

v. The (.mv) Internet country code top-level domain for the Republic of Maldives is administered by Dhiraagu Pvt Ltd. Mainly due to the unavailability of an online registration service, a whois lookup and large maintenance cost, Maldivian ccTLD is used predominantly by government agencies and large businesses. Smaller companies and organizations prefer generic TLDs such as .com and .net.

vi. Many of the websites in Maldives don't use the (.mv) domain, and many local web sites are not hosted in Maldives.

vii. The ITU/IMPACT expert did not observe any applications of security standards such ISO/IEC 27001, ISO/IEC 27002 and ISMS on government infrastructure.

Recommendations

i. The regulators, such as CAM, must be equipped with personnel with cybersecurity technical knowhow to handle matters related to national cybersecurity. These people can drive the national agenda for protection and regulation of CNII by forming working groups or forums for cybersecurity where they can collaborate with various stakeholders within the government.

ii. CAM and NCIT should encourage the use of relevant standards and best practices.

iii. The representatives from CAM acknowledged that the country has not had access to training in the area of cybersecurity standards and regulatory frameworks. They are looking forward to being given opportunities to evolve in that area, especially for key personnel in government agencies.

2.4.5 Critical National Information Infrastructure (CNII)

CNII is a term used by governments to describe information assets that are essential for the functioning of a society and economy. The alarming rise of premeditated attacks with potentially catastrophic effects to interdependent networks and information systems across the globe has demanded that significant attention is paid to critical information infrastructure protection initiatives of a sovereign country. This section discusses the key findings, issues, analysis and recommendations for the Maldives CNII.

Key Findings, Issues and Analysis

i. Listed below are the critical sectors in Maldives identified by the stakeholders during the interview sessions:

- banking and finance,
- information and communications,
- power and energy,
- health services,
- water and food services,
- national defence and security,
- transport,
- government, and
- emergency services.

ii. There is no defined cybersecurity strategy in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber attack on the critical national infrastructure.

Recommendations

i. Since the CNII sectors are well defined, Maldives should start formulating national strategies such as a National Cybersecurity Policy (NCP) to safeguard its CNII sectors. References can be made to frameworks such as National Cybersecurity Framework[51] that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

[51] A generic National Framework for CIIP. www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

ii. The NCP should recognise the critical and highly interdependent nature of the CNII and aim to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. The policy should be developed to ensure that the CNII are protected to a level that commensurate the risks faced[52].

iii. Terms of reference for the NCP should include, but not be limited to:

- standard cybersecurity systems across all elements of the CNII,
- strong monitoring and enforcement of standards, and
- the development of a standard cybersecurity risk assessment framework for the country.

2.4.6 Constituency / stakeholder participation

A constituency is the specific community that the national CIRT is established to serve. Stakeholders are the people who will be involved in the planning, strategising and decision making of the national CIRT. Stakeholder organizations can also be a part of the constituency. This section discusses the key findings, issues, analysis and recommendations for constituency and stakeholder participation in forming the MvCIRT.

Key Findings, Issues and Analysis

i. The major stakeholders that expressed their enthusiasm to cooperate and contribute to the national CIRT project are: the Ministry of Civil Aviation and Communication (MCAC), the Office of the National Security advisor (CAM) that reports directly to MCAC, NCIT, the Department of National Registration (DNR), the Maldives Police Service (MPS), Maldives National Defense Service (MNDF), and the Attorney General's Office (AGO). Input and cooperation from the ISPs association and telecommunication operators, among others Dhiraagu, will be needed for the success of the implementation.

ii. The stakeholders recognized the urgent need to establish a national CIRT, the MvCIRT, and are willing to give their full support. Representatives from CAM recommended that CIRT services be offered to government and other public institutions at the initial stage. However, their concern is that the private sector and the general public are also in dire need of an organization that responds to their incidents. It was therefore emphasized that MvCIRT should grow rapidly in order to accommodate the general public, or acquire the capacity to set up other decentralized CIRTs.

iii. It was agreed that the CIRT should also give priority to Critical National Information Infrastructure (CNII).

iv. The stakeholders acknowledged that the ultimate goal of the national CIRT is to become independent and autonomous.

v. A national CIRT will be needed for the general public in order to give consumers confidence in online transactions. The Maldives population needs a reliable organization that guarantees some level of safety and tracking of offenders/cybercriminals with the rapid growth of Internet services in the past few years and years to come.

Recommendations

i. One of the critical success factors of a national CIRT is the active participations from stakeholders and constituencies in information sharing and coordination work. The involvement from these parties should start from the very beginning, as early as the planning stage of the MvCIRT

[52] International CIIP Handbook: An Inventory and Analysis of National Protection Policies. www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

establishment. Once established, the MvCIRT has a burden of earning and nurturing the trust of the stakeholders and the constituencies.

ii. Constituents need to understand that the establishment of MvCIRT is imperative and will benefit them in dealing with cybersecurity incidents at the national level. The active participation of the stakeholders and constituents can be gained by ensuring and demonstrating that the privacy and confidentiality of their information will never be compromised and will be protected to the best of its ability.

iii. The recommended and targeted type of service MvCIRT will be providing to its constituents is Hybrid Services. However, covering the private sector can be a very intense challenge without the adequate experience. It is then recommended that the CIRT reaches a certain maturity level, before it starts rendering its services to institutions from the private sector. Basically, there are three kinds of services provided by a CIRT to its constituents: Bounded, Unbounded and Hybrid.

2.4.7 Local cybersecurity expertise

One of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise. Many CIRTs failed because of this. This section discusses the key findings, issues, analysis and recommendations for local cybersecurity experts in Maldives.

Key Findings, Issues and Analysis

i. From the information gathered and research conducted by the ITU/IMPACT expert, it can be concluded that the number of locally produced cybersecurity experts in Maldives is still low.

ii. A good number of individuals have general computer science qualifications. This is mainly attributed to the fact that universities, colleges and other local training institutions did not offer cybersecurity-specific courses.

iii. There is also a pool of local experts in Maldives who are actively involved in open source software development, the Maldives Open Source Society (MOSS). This society has individuals with technical skills who are willing to contribute in the establishment of a national CIRT for Maldives.

iv. The idea of hiring foreign cybersecurity experts is not favoured due to the lack of trust when it comes to sensitive governmental information.

v. All the stakeholders and constituent organizations recognized that there is a high need for training of individuals in cybersecurity. However, those with IT and networking background in stakeholders' organizations could be eligible to undertake cybersecurity courses.

Recommendations

i. The most pressing matter at the moment is the establishment of the national CIRT and getting the right technical expertise to operate it. This can be achieved by collaborating with local experts like the Maldives Open Source Society (MOSS) or sending identified candidates for appropriate training and seminars, either locally (if available) or abroad.

ii. To establish the national CIRT, stakeholders should conduct a talent search to identify the right people with the right attitude and qualifications to man the CIRT. Training needs assessments should also be conducted to identify the right set of courses that the identified personnel should sign up to.

iii. MCAC in collaboration with Ministry of Education (MOE) and MCST should strive to improve the level of awareness and the security skill-sets of the local ICT experts by sending them for identified trainings and education programmes.

iv. The ministries such as MOE together with MCAC and the proposed national CIRT can develop a cybersecurity-specific syllabus that can be made available in local colleges and universities.

v. Occasionally the proposed national CIRT should conduct awareness programmes in public places and also in government offices to increase levels of awareness.

vi. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programmes relevant to cybersecurity areas with college and university students. The research programmes can be coupled with rewards such as scholarship or employment to encourage more participation.

vii. ITU in collaboration with IMPACT could assist in developing local expertise by leveraging scholarship programmes that are available for countries through its partnership with various world-renowned training providers.

2.4.8 Cybersecurity education and training

As discussed, one of the stumbling blocks of establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise due to the limited availability of cybersecurity education and training programmes in Maldives. This section discusses the key findings, issues, analysis and recommendations for cybersecurity education and training.

Key Findings, Issues and Analysis

i. Cybersecurity education in Maldives is limited to occasional seminars, workshops, short courses by international organizations and regional conferences that some of the participants have attended in the past. A part from that, proper cybersecurity courses or subjects are not available at national universities.

ii. More often than not, the local institutions will have to depend on foreign expertise in developing courses such as computer science.

iii. Some of the local students and IT experts are aware of cybersecurity certification courses overseas, but they don't know how to have access to them, or lack the financial means to take the courses without a sponsor as the cost is often too high for them. Local institutions haven't understood yet the importance of sponsoring students to take cybersecurity courses.

Recommendations

i. One of the most important elements in establishing and sustaining a national CIRT is the competency of the personnel. Training and human capacity development programmes must be in place to have locally produced experts.

ii. Through partnerships and MoUs, the Government can bring in various cybersecurity training providers and make the courses easily accessible to the people. Scholarship programmes can also be offered to encourage the Maldivian people to venture into cybersecurity areas.

iii. It is imperative for Maldives to start including cybersecurity into the syllabus of higher education institutions. This has to be done before it is too late due to the rapid development and outreach of latest technologies within the country. Stakeholders such as Ministry of Education, MCAC and NCIT should collaborate to make this happen.

iv. ITU in collaboration with IMPACT could assist Maldives and the stakeholders to design courses and promote research programmes.

2.5 Readiness assessment: Nepal

This section contains all the key findings from the assessment including, key issues, analysis and recommendations for the enhancement of the cybersecurity situation in Nepal. These findings, issues, analysis and recommendations are based on the information gathered during the on-site assessment and general research conducted by the expert.

2.5.1 ICT infrastructure

This assessment component focuses on identifying whether there is sufficient ICT infrastructure to justify the formation of a national CIRT and whether there is a high level of usage and reliance on ICT and Internet to support basic communications in Nepal.

Key Findings, Issues and Analysis

i. From the on-site meetings and interviews conducted, the following information was gathered:

ii. Internet access remains limited in Nepal, especially in rural areas. In 2009, there were approximately 625,800 Internet users in Nepal which is only 2.1 per cent of the entire populations. Mobile cellular usage is higher in comparison to the fixed telephone lines in the ratio of 9:1. Indeed, low levels of access are responsible for Nepal's ranking of 142 globally on the ITU 2009 ICT Development Index[53].

iii. Nepal completed the installation of a national optical fibre backbone which stretches from east to west; all of Nepal is connected to India via several connecting points. The Indian Government funded this project for the most part. The completion of the optical fibre network is considered essential as it provides the backbone for telecommunication services, including Internet services. Nepal Telecom was also funded by the Chinese Government to complete a fibre optic project along the 115-kilometre Arniko Highway linking Kathmandu to Khasa, which borders China in the north. These two backbones enhance Nepal's global communications capability because they link the country the major communication gateways of the world. The completion of the fibre optic backbone has provided a cheaper and reliable alternative to the expensive satellite communications and as a result some new ICT services have been introduced, for example e-banking, e-education and e-government.

iv. Various arms of government have made significant progress in deploying ICT in e-government solutions. These solutions can be categorised into both e-government and e-governance solutions. In the category of e-government, several departments are transforming their operations by deploying ICT. For instance, e-village forum has been developed and it's in use in most of the districts in Nepal.

v. E-commerce in Nepal is just starting. Some banks have tied up with a host of third party vendors for e-shopping and e-payment services to allow online purchases and payments from all leading online shopping portals in the country. There are also various Nepali web-portals that carry out e-commerce for example; Muncha.com and musicnepal.com both carry out business electronically.

vi. There are several local ICT companies in Nepal that develop and provide e-commerce technology and services. The Nepali IT market consists of hardware and software services, including business process outsourcing (BPO) services, call centres, software development, and creating solutions. Although the ICT industry is small compared to the ICT industry in more developed countries, there are companies, such as Mercantile, HiTech Valley, GeoSpatial, Serving Minds, D2Hawkeye and Yomari, which are managed by visionary leaders and are successfully providing products and services consistent with international standards. However, in Nepal the Internet is still mainly used for activities such as to send and receive emails, to find out the latest news, to do online research, to watch or download videos, to access social networking sites etc.

vii. Banks have also started to offer Internet banking services and facilities to their clients. The banking sector makes heavy use of ICT to provide improved customer service with some banks using Very Small Aperture Terminals (VSATs) or public leased lines to interconnect their branch offices and ATMs. Travel agencies and hotels have also started practising online reservations. There are similar advances in other business sectors too.

[53] See:www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf

viii. There are over 44 licensed Internet Service Providers (ISP)[54] in the country providing Internet connectivity through various access methods: dial-up, leased line, broadband, VSAT, GPRS and wireless hotspots. VSATs are used in rural development projects where other forms of communication are not considered feasible. Remote villages in mountainous regions are connected to each other using this technology.

ix. Mobile phone usage is the most common mode of communication in Nepal, however, landline telephone usage is very low. The stakeholders reported that use of mobile phones has become a routine. While making voice calls and sending SMS are the most popular uses of mobile phones in Nepal, new innovative uses of mobile phones have emerged, for example; use of mobile phones to conduct financial transactions such as fund transfers and bill payment bills. The first mobile banking services in Nepal were introduced by Laxmi Bank[55].

x. The Nepal Stock Exchange (NEPSE) has granted brokers permission to start online trading of shares through the Wide Area Network, thus paving the way for online transactions in the Nepali stock market. The new service allows selected stock brokers to place orders, sell, or buy shares from their office via the Internet without going to the capital market.

xi. The lack of infrastructure and the lack of a reliable supply of electricity, constrain the adoption of ICT in rural areas. The main obstacle to using the Internet is the limitations or outdated telecommunication infrastructure. For instance; there is existence of outdated last mile connectivity[56]. This has led ISPs to invest in expensive back-up satellite systems and passing additional costs to users.

xii. Most of the investment in last-mile connectivity is concentrated in the large urban areas, where the majority of the current users reside. Furthermore, the cost of bandwidth is a universal constraint to Internet use. There is a concentration of ICT infrastructure and Internet usage in urban areas, compared to rural towns and other parts of the country. However, efforts are being made to spread technology to rural areas.

Recommendations

i. The decision makers at governmental and ministerial levels need to consider allocating sufficient priority to security, reliability and availability of systems in all ongoing ICT infrastructure projects. The principle of defence in depth should also be adopted by the government in all the projects related to ICT security. Nepal is at the stage of incorporating new ICT technologies to its Critical National Information Infrastructure (CNII) and this transition needs systems to be designed with adequate security.

ii. In order for the new fibre optic backbone to deliver all the expectations, last-mile connectivity needs upgrading to be able to deliver broadband Internet access to consumers at affordable prices.

iii. Training and education need to be carried out to improve ICT usage. Outreach programmes must also be developed to sensitize the public about the benefits of using the Internet. This will increase the number of people who use the Internet.

iv. Ensure even penetration of ICT throughout the country by investing in infrastructure for the rural areas.

v. Awareness on the current government ICT initiatives needs to be heightened so that public use of these applications increases and gains widespread support.

---

54 www.nta.gov.np/en/licenseelist/

55 www.nepalitimes.com/issue/2010/06/18/BIZBRIEF/17176

56 **Last mile connectivity** refers to the link between the user and the service provider.

vi. Improving the overall readiness, availability and reliability of ICT infrastructure by including mirror sites and backups is necessary to provide reliable infrastructure for IT operations. This provides redundancy which helps to minimise any chance of disruption to critical applications in case of a cyber attack.

vii. The implementation of and continuous improvement of the cybercrime legislation is needed to complement the ICT readiness.

viii. An acceptable set of standards for equipment, applications and security policies can be established to ease ICT management and efficiency.

ix. The responsible entities, the private sector and the government are encouraged to collaborate together in order to formulate a coordinated ICT investment strategy for all parts of the country.

x. It is also recommended that the government needs to focus its efforts to build ICT infrastructure in rural and remote areas including through its Rural Communications Development programmes.

xii. Encourage private sector to participate in development of infrastructure in rural and remote areas by providing incentives for investments such as tax rebates, license fee rebate, and infrastructure sharing for stimulating investment.

2.5.2 Cyber threats affecting Nepal

The need for CIRT services has already been highlighted in chapter 1. Mitigating and eradicating cyber threats affecting a country is one of the critical factors when establishing a national CIRT. This section discusses the key findings, issues, analysis and recommendations concerning cyber threats affecting Nepal. The findings in this section are based on stakeholder accounts and information provided by some key personnel. Often there were no supporting documents to substantiate their facts.

Key Findings, Issues and Analysis

i. The types of attack affecting Nepal are similar to those affecting other countries in the region and other parts of the world. These include malicious software (malware), phishing scams, electronic fraud, web defacement and email account hacking. It was reported that both server-side attacks and client-side attacks have been experienced by computer systems.

ii. In Nepal spam email is a common way to distribute malware as attachments or via links to malware hosting sites. This has led to infection of many computers owned by users, businesses and government with malware. Most of this malware is obtained from infected foreign websites as "drive-by downloads"[57] but also infection through opening infected email attachments.

iii. It was reported that social engineering scams such as the famous "419 scams"[58] are very common. These have caused major financial losses to unsuspecting victims and businesses.

iv. The Nepal Police have a cyber crime cell that handles local cyber incidents. Cases have been reported to the Nepal Police concerning libellous statements published on websites that damage the reputation of public figures, for example, the case of Home Minister Bhim Rawal. Slanderous emails and posting of obscene images on the Internet have also been reported in Nepal. Often, these activities involve defaming public figures.

v. It was reported that email hacking and phishing attack cases are increasing. Several victims have fallen prey to computer hackers because most of the members of the public are unaware of cybersecurity.

---

[57] A **'drive-by download'** is a programme that is automatically downloaded to your computer, without your consent or even your knowledge.

[58] For definition of 419 scam, see: http://en.wikipedia.org/wiki/Advance-fee_fraud

vi. It was reported that there is no systematic or coordinated mechanism to identify, detect or deter cyber threats within the government sectors. The private sectors have their own mechanisms but the information is often not shared with the government sectors.

vii. The Nepal Police Force has received cases related to electronic fraud but lacks a proper monitoring system to deal with these cases. There is also a lack of adequate training and skills to perform complex electronic investigations e.g. digital forensics and static malware analysis.

viii. There is a failure to adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organizations to connect to the Internet. The stakeholders identified a lack of appropriate security controls and mechanisms in place and also the lack of ability to monitor and detect attacks when they happen.

ix. Other sophisticated security apparatus like Intrusion Detection Systems (IDS), Host-based Intrusion Prevention Systems (HIPS) and Intrusion Prevention Systems (IPS) are not used to safeguard critical network components.

x. Based on the information gathered, there is no clear defence strategy in place in case of a major cyber attack on government infrastructure. Currently, web defacements are quite common in the country. This includes several defacements of government websites and business websites. Most of the interviewees have no clue of what to do in the event of a cyber crisis in Nepal.

xi. It was reported that data theft from companies is quite common in Nepal. This data is obtained through hacking and also by use of electronic media. This is an infringement of intellectual property. A case of this nature was reported to the Nepal Police Force by an IT company.

xii. Other cases reported to the Nepal Police by the general public include; complaints of harassment by phone calls, sending of obscene SMS, and call bypassing.

Recommendations

i. It is clear from the above findings that the setting up of a national CIRT as a focal point in managing incidents and a coordination centre to manage all the information sharing and information flow for cybersecurity is crucial. Awareness of the need to report all incidents to this central point is vital. The CIRT will also provide knowledge of available best practises that can be shared and implemented on their respective networks.

ii. One of the main issues faced by Nepal is that it lacks the means or mechanism to detect the kinds of malicious traffic that are flowing into or are targeting the country. This can be tackled with the implementation of sensor networks (honeypots) at ISPs and international gateways to capture malicious traffic that target the country's systems. These sensors are decoy systems that will trick attackers into thinking that they are attacking real systems and this will enable the operators of the sensors to capture information like malware, originating sources of attacks and network traffic information for further detailed study and trend analysis.

iii. Stakeholders need to adequately manage the confidentiality, integrity and availability of ICT infrastructure, information systems and computers used by people and organizations to connect to the Internet. Network operators and service providers such as NT and NTA need to take technical measures to secure their network access.

iv. Outreach programs need to be developed to increase public awareness about the dangers associated with cyber threats. I recommend the use of training and education to teach users basic steps for dealing with IT security issues.

v. Establish a national CIRT so that it can take on the role of central coordinating body. It is also recommended that in the future, large organizations that are responsible for the country's critical national infrastructure should establish their own CIRTs in collaboration with the national CIRT. The CIRTs will be known as sector CIRTs and they will coordinate with the national CIRT in matters related to cybersecurity agenda of the country and the same time become constituents of the national CIRT.

vi. The national CIRT should record cybersecurity incident complaints and create a database of cybersecurity offenders. This data can be used by the national CIRT, law enforcement agencies and regulatory bodies to identify and make trend analysis. This data can also be examined together with other agencies like other national CIRTs, INTERPOL, immigration departments, forensics bureau, police and other institutions like banks and so forth that will help in tracking cyber criminals.

vii. Once the CIRT has been setup, it is strongly encouraged to gain membership with international organizations such as FIRST (Forum of Incident Response and Security Teams), IMPACT and regional CIRT establishments. These organizations are very experienced in coordinating and collaborating in cybersecurity matters and will provide the national CIRT with a good platform to share information.

viii. Develop and/or update the legal framework to make Nepal less favourable as a cybercrime haven for criminals. We recommend that the government together with its agencies drafts and passes cybercrime laws which can be used to criminalise all forms of electronic fraud.

ix. It is recommended that private businesses, especially the banks, start working together with the police to fight cybercrime. This can be made easier by the banks sharing information regarding bank frauds with the police. The police need to also keep this information confidential in order to build trust between the two parties. A special task force can be formed which will be constituted by local banks, international banks operating in Nepal, credit card issuers and businesses which rely heavily on credit cards to manage the risks associated with credit cards.

x. Government agencies and ministries may deploy secure communication infrastructure by employing tools such as encryption and GRC (Governance, Risk and Compliance). Encryption can be chosen from a vast variety of algorithms and technologies such as PGP, TrueCrypt, RSA, SSL and SSH to secure their communications[59].

2.5.3 Cybersecurity legal framework

Mitigating and eradicating cyber threats affecting a country cannot be done by just using technologies and services. It has to be coupled with a robust and up to date legal framework to cater for the dynamic nature of ICT environments and cybercrime tactics. This section discusses the key findings, issues, analysis and recommendations concerning the cybersecurity legal framework in Nepal.

Key Findings, Issues and Analysis

i. The NTA is the Telecommunication Authority of Nepal. NTA, an autonomous body, was established in February 1998 in accordance with the Telecommunications Act 1997 and the Telecommunications Regulation 1998. Its objectives include;

- to create a favourable and competitive environment for the development, expansion, and operation of telecommunication services with the participation of the private sector, and
- regulate acceptable quality of telecommunication services of all types making them affordable and accessible to all for Nepal's overall development.

ii. In December 2006, Nepal promulgated the Electronic Transaction Act, also known as the Cyber Law, which legalizes all electronic transactions and digital signatures. The law also defines and sets penalties for computer and cybercrimes, such as hacking, piracy, and computer fraud.

iii. The Supreme Court started treating email correspondence as legal for judicial purposes. Earlier, only correspondence via facsimile and postal mail was considered authentic for judicial purposes.

[59] PGP stands for Pretty Good Password; **SSL** stands for Secure Sockets Layer; **SSH** stands for Secure Shell Tunneling.

iv. The Kathmandu Metropolitan Police Crime Division (KMPCD) has set up a separate Cyber Cell to deal with criminal cases involving cyber technology.

Recommendations

i. Stakeholders should expedite the process of amending or passing of cyber laws because delays give cyber criminals the chance to exploit legal loopholes. Such a legal framework is able to address not only national issues, but also facilitate international cooperation. ITU in partnership with IMPACT would support and assist[60] Nepal to ensure that national cyber laws would be developed consistent with the principles of international cooperation.

ii. The rapid changes in technology and attack vectors require amendment of outdated cyber laws in order to combat cybercrime and it is highly recommended that the Nepal Government expedites the process of passing the necessary laws.

iii. It is important to develop and implement awareness campaigns to educate users, law enforcement and policy makers about cyber laws, the impact of cybercrime and measures of combating it. It is recommended that the national CIRT takes on the leading role of creating cybersecurity awareness campaigns.

iv. Due to rapid changes in technology there is a need to create laws which are technology neutral in order to cater for the dynamic nature of ICT technologies. This is one of the the best ways to combat cybercrime effectively.

2.5.4 ICT regulatory framework

This section discusses the key findings, issues, analysis and recommendations concerning the ICT regulatory framework in Nepal.

Key Findings, Issues and Analysis

i. The Ministry of Information and Communication (MOIC) has jurisdiction over major ICT areas such as licensing, and has long and consistent relations with the ITU and the APT.

ii. Nepal's regulatory body of telecommunications is the Nepal Telecommunication Authority (NTA) and requires approval from MOIC for its ICT initiatives. Nepal Telecommunications Authority was established on March 4, 1998 as an autonomous regulatory body within the framework of the Telecommunication Act 1997 and Telecommunication Regulation 1997.

iii. The function and duties of NTA among others are to regularize and systemize telecommunication services and to suggest the Government of Nepal on the policy, plan and program to be adopted by the government for the development of telecommunication services.[61]

iv. Relevant acts and regulations for information technology and communications are the Telecommunications Act 1997, Telecommunications Regulations 1997 and Telecommunications Policy 2004.

v. The Government of Nepal has developed the Telecommunication Policy, 2060 (2004) to create a favourable environment in order to make telecommunication services reliable and accessible to all people at reasonable cost throughout the Kingdom of Nepal in collaboration with the private sector in order to support the social and economic development of the country.

vi. The .np domain (ccTLD) is administered by the Mercantile Communications Pvt. Ltd. Mercantile Communications Pvt. Ltd is the internet registry for .np domain names. The majority of the web

[60] See ITU Cybercrime Legislation resources – www.itu.int/ITU-D/cyb/cybersecurity/projects/cyberlaw.html

[61] See Nepal Telecommunications Authority Management Information System – www.nta.gov.np/articleimages/file/NTA_MIS_18.pdf

sites in Nepal don't use the .np domain, and many local web sites are not hosted in Nepal. This is due to bandwidth and infrastructure limitations.

Recommendations

i. Responsible entities such as NITC, HLCIT and regulators, such as NTA, should employ staff with cybersecurity technical skill sets to deal with the issues relating to national cybersecurity. Technically competent manpower can drive the national agenda for protection and regulation of Critical National Information Infrastructure (CNII) by forming working groups or forums for cybersecurity where they can collaborate with various stakeholders within government.

ii. It is recommended that rural communications development programmes are supported to ensure universal access of ICT services throughout the country.

iii. It is recommended that NITC continues to encourage the use of relevant standards and best practices.

2.5.5 Critical National Information Infrastructure (CNII)

CNII is a term used by governments to describe information assets that are essential for the functioning of a society and economy. The alarming rise of premeditated attacks with potentially catastrophic effects on interdependent networks and information systems across the globe has demanded that significant attention is paid to critical information infrastructure protection initiatives of a sovereign country. This section discusses the key findings, issues, analysis and recommendations for the Nepal CNII.

Key Findings, Issues and Analysis

i. Listed below are the critical sectors in Nepal identified by the stakeholders during the interview sessions:

- banking and finance,
- information and communications,
- power and energy,
- health services,
- water and food services,
- national defence and security,
- transport,
- government, and
- emergency services.

ii. There is no defined cybersecurity strategy in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber attack on the critical national infrastructure.

Recommendations

i. Since the CNII sectors are well defined, Nepal needs to start formulating national strategies such as a National Cybersecurity Policy (NCP) to safeguard its CNII sectors. References can be made to frameworks such as National Cybersecurity Framework[62] that comprises legislation and regulatory, technology, public-private cooperation, institutional, and international aspects.

[62] A generic National Framework for CIIP.

www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

ii. The NCP must recognise the critical and highly interdependent nature of the CNII and aim to develop and establish a comprehensive programme and a series of frameworks that will ensure the effectiveness of cybersecurity controls over vital assets. The policy must be developed to ensure that the CNII sectors are protected to a level that is commensurate with the risks faced[63].

iii. Terms of reference for the NCP should include, but not be limited to:

- standard cybersecurity systems across all elements of the CNII,
- strong monitoring and enforcement of standards, and
- the development of a standard cybersecurity risk assessment framework for the country.

2.5.6 Constituency / stakeholder participation

A constituency is the specific community that the national CIRT is established to serve. Stakeholders are the people who will be involved in the planning, strategising and decision making of the national CIRT. Stakeholder organizations can also be a part of the constituency. This section discusses the key findings, issues, analysis and recommendations for constituency and stakeholder participation in forming the NpCIRT.

Key Findings, Issues and Analysis

i. The national CIRT initiative has been welcomed by all stakeholders and constituencies, who have also recognised the need to improve the level of awareness and security skills of ICT personnel within the country.

ii. It was agreed that the CIRT should also give priority to Critical National Infrastructure.

iii. A national CIRT will be needed for the general public in order to give consumers confidence in transacting online.

iv. The Nepal Government is preparing to form an Information Technology Emergency Response Team (ITERT) under the Ministry of Science and Technology to test and security-audit Nepali websites before putting them on the internet. Upon receiving approval from the IT Ministry of Science and Technology, the Office of Controller of Certification (OCC) will establish ITERT which will have a specific mandate to respond to computer security incidents.

v. The MoIC, HLCIT, CAN, Nepal Police and the OCC have been undertaking initiatives in safeguarding cyberspace. However, the coordinated mechanism amongst these agencies needs to be improved so that the threat handling strategy can be put in place to resolve cyber incidents systematically.

vi. HLCIT provides crucial strategic direction and helps formulate appropriate policy responses for the development of ICT sector in the country.

vii. The Internet Service Provider's Association of Nepal (ISPAN) is the umbrella organization for ISPs. ISPAN is committed to advocate and support a healthy Internet industry in the country. It works closely with telecom operators, ministries involved in ICT-related matters, and various other organizations on various issues that affect the implementation of the ISP projects.

viii. CAN assists in the utilization, enhancement and promotion of computers and information technology within Nepal and helps to develop strategies to meet the necessary requirements for the development of literacy and skills regarding computer science. It also provides and protects the necessary rights and privileges, benefits to individuals, institutions, companies and organizations affiliated to the activities of CAN.

---

[63] International CIIP Handbook: An Inventory and Analysis of National Protection Policies. www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

Recommendations

i. One of the critical success factors of a national CIRT is the active participations from the stakeholders and the constituencies in information sharing and coordination work. Involvement of these parties should start from the very beginning, as early as the planning stage of the CIRT establishment. Once established, the CIRT has a burden of earning and nurturing the trust of the stakeholders and the constituencies.

ii. Constituents need to understand that the establishment of the national CIRT is imperative and will benefit them in dealing with cybersecurity incidents at the national level. The active participation of the stakeholders and constituents can be gained by ensuring and demonstrating that the privacy and confidentiality of their information will never be compromised and will be protected to the best of its ability.

iii. The recommended type of service the NpCIRT would provide to its constituents would be, in this case, Hybrid Services. However, initially, services will be more bounded to government agencies and ministries. Once it has reached a certain level of maturity, it shall start offering its services to anyone requesting them.

iv. The stakeholders should harmonize their work to coordinate strategies in setting up a national CIRT in Nepal. This will prevent duplication of work and it will create a systematic way of doing things especially in handling security incidents.

v. The stakeholders should leverage the expertise of CAN to drive the information security initiatives.

2.5.7 Local cybersecurity expertise

One of the challenges for establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise. Many CIRTs tend to fail due to lack of technical expertise. This section discusses the key findings, issues, analysis and recommendations concerning local cybersecurity experts in Nepal.

Key Findings, Issues and Analysis

i. From the information gathered and research conducted by the ITU/IMPACT expert, it can be concluded that there are no locally produced cybersecurity experts in Nepal. Universities and colleges are not producing local cybersecurity expertise because they lack cybersecurity-specific courses in their syllabus.

ii. It is challenging to find competent cybersecurity experts who are trained adequately since there is a small pool of highly skilled ICT personnel in the country. This can also be attributed to the fact that most of the local ICT experts are working in other areas of ICT other than security. This could also be due to the very high cost associated with sponsoring candidates for overseas trainings.

iii. The idea of hiring foreign cybersecurity experts is not favoured due to the lack of trust when it comes to sensitive governmental information.

iv. All stakeholders and constituent organizations recognized the need for training of individuals in cybersecurity. However, those with IT and networking backgrounds in some stakeholders' organizations could be eligible to undertake cybersecurity courses.

Recommendations

i. The most pressing thing at the moment is the establishment of the national CIRT and getting the correct technical expertise to operate it. This can be achieved by sending the identified candidates for appropriate training and seminars, be it locally (if available) or abroad. This does not have to wait until the right set of education programmes, or training are made available within the country (which is discussed in the next section).

ii. NITC in collaboration with the national CIRT needs to strive to improve the level of awareness and the security skill-sets of the local ICT experts by sending them for identified training and education programmes.

iii. Local universities in collaboration with other stakeholders can develop a cybersecurity-specific syllabus that can be made available in local colleges and universities.

iv. The national CIRT must strive to conduct awareness programs in public places and also in government offices to increase levels of awareness. The constituency and stakeholders must also play a role of awareness to make it more effective.

v. To impart the culture of cybersecurity, stakeholders can also embark on activities such as research programmes relevant to cybersecurity areas with college and university students. The research programmess can be coupled with rewards such as scholarship or employment to encourage participation.

vi. ITU, in partnership with IMPACT, can also play a very important role in developing local expertise by leveraging scholarship programmes[64] that are available for countries through its partnership with various world-renowned training providers.

vii. To establish the national CIRT, the stakeholders should conduct a talent search to identify the right people with the right attitude and qualifications to man the CIRT. Training needs assessments should also be conducted to identify the right set of courses that the identified personnel should sign up to.

2.5.8 Cybersecurity education and training

As discussed in section 4.7, one of the challenges for establishing a sustainable CIRT is the availability of locally produced cybersecurity expertise due to the lack of cybersecurity education, training programs and policies and strategies to act as drivers of education initiatives within the country. This section discusses the key findings, issues, analysis and recommendations for cybersecurity education and training in Nepal.

Key Findings, Issues and Analysis

i. Since Nepal lacks cybersecurity expertise, the local institutions will have to depend on foreign expertise in developing cybersecurity related courses.

ii. Some computer security related courses are organized by computer training institutes regarding hacking; however a lack of skilled trainers has been noted in these institutes.

Recommendations

i. Establishment of good practice/ conduct and building of a cybersecurity culture will complement the activities of the national CIRT and cybersecurity as a whole. Training and human capacity development programs need to be in place in order to have locally produced experts.

ii. Through partnerships and MoUs, the responsible entities in Nepal can bring various cybersecurity training providers into the country and make the courses more accessible to people. Scholarship programs can also be offered to encourage the Nepal people to venture into cybersecurity areas.

iii. Nepal needs a cybersecurity syllabus for higher education institutions because of the rapid development and penetration of the latest technologies within the country. Stakeholders should collaborate to make this happen.

ITU, in collaboration with IMPACT, can also play a very important role in helping the country and the stakeholders to design courses and promote research programmes.

[64] www.impact-alliance.org/services_centre_training_partner.html

CHAPTER 3
ACTION PLAN TO ESTABLISH A CIRT

Based on the studies conducted and data collected, a holistic three-phase approach to establish a CIRT is proposed. Figure 1 below gives an overarching view of the three phases involved (see also tables below).

Figure 6 – Proposed CIRT implementation timeline

3.1 Phase 1: Basic CIRT infrastructure and services

This phase will focus on setting up basic CIRT services which will include triage, handling and requests. At the end of this phase, CIRT will be able to provide the services listed below to its constituencies:

- reactive services: incident response and handling (both remote and on-site), alerts and warnings, vulnerability response, and
- proactive services: announcements and basic awareness, education and training.

IMPACT can offer a solution called CIRT-Lite which comes with technical components such as an incident management system, mailing list, public portal and advice. The CIRT analysts and manager will also be provided with basic CIRT training both in management and technical issues.

CIRT will also be given access to the IMPACT Global Response Centre (GRC) Portal which hosts aggregated threat information from various sensors across the globe. The IMPACT GRC Portal also provides a collaborative platform for cybersecurity experts from all over the world to pool their resources in combating cybercrime.

IMPACT could also play an active role to transfer knowledge and skills to CIRT. To achieve this, IMPACT has identified an attachment program which will enable the CIRT analysts to be physically attached with IMPACT GRC for specified timeframes to have the real-world and hands-on experiences in handling cybersecurity incidents.

As part of the continuous improvement process, IMPACT could also assist in identifying a training roadmap for the CIRT analysts to develop the necessary and required skill-sets.

3.2 Phase 2: Enhanced CIRT services

This phase will concentrate on setting up enhanced CIRT services. After operating for more than six months, in addition to the Phase 1 services above, CIRT can opt to provide the services listed below for its constituencies:

- reactive services: incident response coordination, vulnerability response coordination and threat analysis,
- proactive services: vulnerability analysis and technology watch, and
- security quality management: advance awareness, education and training.

IMPACT could conduct a training needs analysis and will help CIRT to identify the right people to attend the right combination of cybersecurity training.

3.3 Phase 3: Advanced CIRT services

The third and final phase will focus on setting up an advanced CIRT services. Once in operation for more than 12 months, in addition to the Phase 1 and 2 services above, CIRT can opt to provide the services listed below for its constituencies:

- proactive services: security audits and assessments,
- reactive service: forensics analysis, and
- security quality management services: risk analysis, security consulting.

Upon completion of this phase, CIRT will be able to provide full-fledge cybersecurity services and solutions to its constituencies.

3.4 CIRT services to constituencies

Since CIRT is still at its infant stage, it is recommended that it starts with basic proactive and reactive services for its constituents. However, all the possible services CIRT can provide have been broken down into three phases. CIRT can provide the services based on its maturity level and readiness. The following tables set out the integrated plan for the type of services CIRT can provide to its constituents in each stage.

Phase 1:

Service	Descriptions
Announcements and Warnings	Disclosing details of ongoing threats and steps that can be taken to protect against those threats. Involves notifying or alerting any newly discovered information about cyber threats and vulnerabilities to the constituency with a recommended course of action and guidance on how to protect the system. Announcement and warning types are: • heads-up, • alert, • advisory, and • guideline.
Remote Incident Response	Providing technical advice about how to handle security incidents when they occur in order to mitigate harm and recover from the incident. Advice is usually provided via telephone or email (remotely).
On-site Incident Response	Providing on-site technical support and advice about how to handle security incidents when they occur in order to mitigate harm and recover from the incident. Usually this kind of service is rendered out for critical level incidents.
Vulnerability Response	Assess the appropriate action required to respond to newly-discovered vulnerabilities; to assess their severity and impact; decide whether to issue warnings about them or verify or investigate their severity/impact further. Generally, this approach relates to vulnerability information already in the public domain.
Basic Awareness, Education and Training	Conduct public awareness programs in a small scale. Basic computer emergency response training and fundamental cybersecurity best practices.

Phase 2:

Service	Description
Incident Response Coordination	Act as a coordination point at national level or regional level between parties affected by a security incident. To be able to provide this service, CIRT must establish trusted relationships with various parties and agencies at national, regional and global levels.
Advance Awareness, Education and Training	Conduct large scale public awareness programs such as conferences at national or regional levels. Conduct advance level computer emergency response training and cybersecurity best practices.
Vulnerability Response Coordination	In consultation with IMPACT Global Response Centre, coordinate the responsible disclosure of information about software / hardware vulnerabilities within an appropriate time frame. The timing is designed to minimize adverse consequences of premature disclosure by ensuring the vendor has time to develop and release a patch to coincide with the notification, where possible.
Threat and Vulnerability Analysis	The analysis of computer and network threats and vulnerabilities to determine what their technical impacts may be and how best to mitigate them; to identify new emerging trends or changes in attacker modus operandi; or provide advice about general cybersecurity trends.

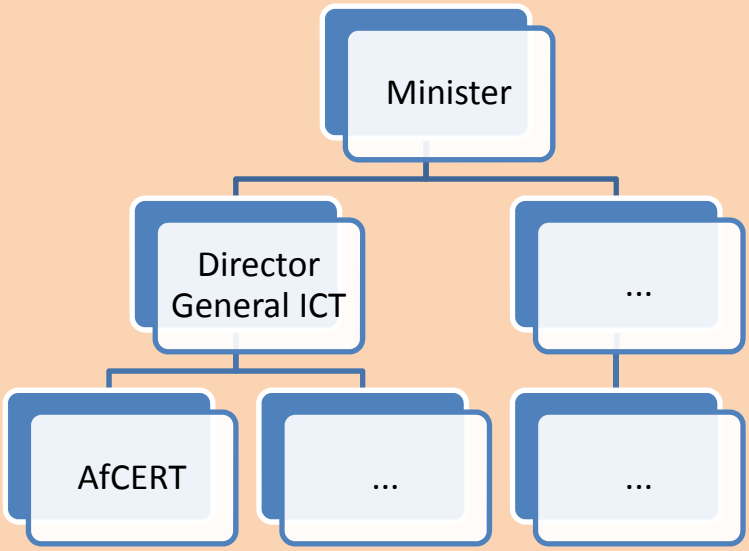
Phase 3:

Service	Description
Forensics Analysis	Conduct digital forensics analysis on digital evidence and artefacts in accordance with local legislation. It is a reactive measure where the CIRT analysts will investigate the damage and possibly identify the perpetrator.
Security Assessments and Audits	Consulting service to provide an assessment report on the security of an organization's information systems / networks; highlighting any weaknesses and suggesting methods to improve security. The kind of services include risk analysis, business continuity and disaster recovery planning, security consulting and possibly product evaluation or certification.

3.5 CIRT reporting structure

Figure below shows a proposed reporting structure of CIRT within the Ministry of Communications and Information Technology (MCIT). It is proposed that CIRT placed under the responsibility of ICT Directorate Division which is more relevant to the nature of services of CIRT. This reporting structure will also give CIRT the required empowerment to carry out its duties and roles.

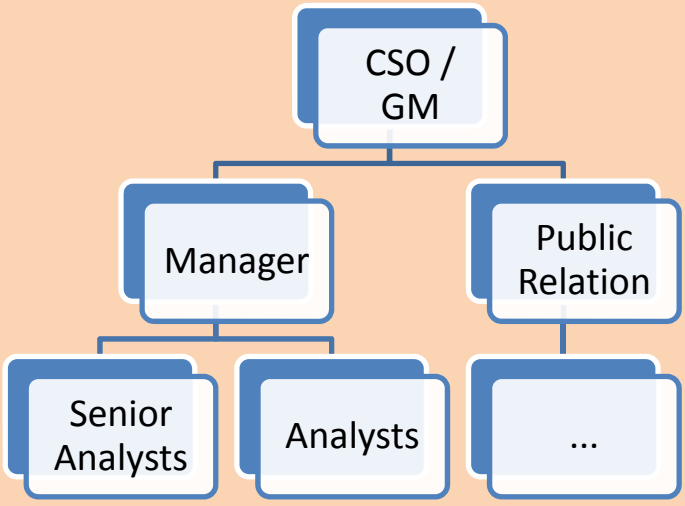
Figure 7 – A sample CIRT reporting structure



3.6 CIRT organizational chart

Figure below shows the internal organizational chart of CIRT. A Chief Security Officer (CSO) or a General Manager (GM) will be appointed to manage the whole CIRT team.

Figure 8 – CIRT organization chart



Please refer to Appendix 4 for the Terms of Reference of the Chief Security Officer, the job descriptions for the manager and the analysts and in section on Human Resources below.

3.7 Risk analysis

Risk analysis is a technique to identify and assess factors that may negatively affect the success of achieving a goal. It is very important to address several areas during the planning, implementing and operating stages. The figure and table below offer some proposed risk analysis:

Figure 9 – Risk analysis: threat levels

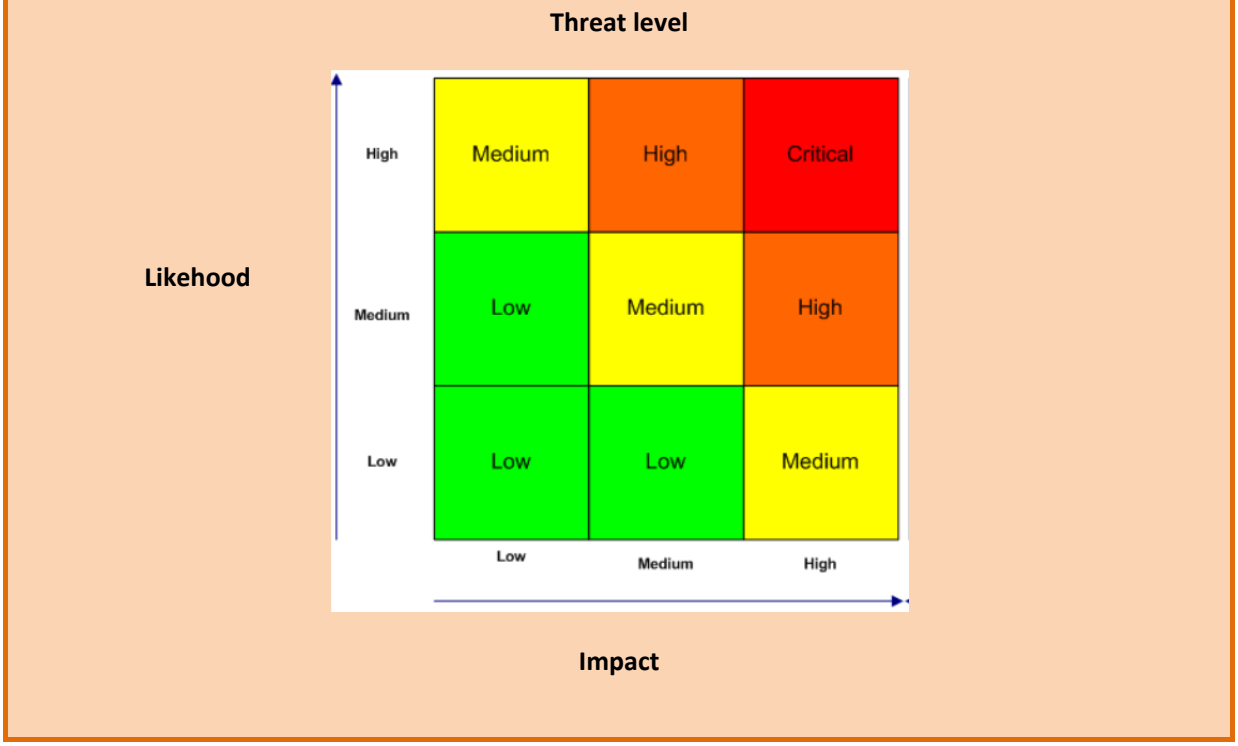


Table 3: risk analysis

No	Area	Risk	Impact	Likelihood	Mitigation
1.	Human Resources	The national CIRT unable to find staff with sufficient technical skills and knowledge.	Low	High	Generally, candidates have basic practical technical knowhow on Internet and computer technologies. In-house or external training can be arranged to increase competency levels.
2.	Human Resources	A technical staff member becomes unavailable, compromising CIRT operations.	High	Medium	After a few months in operation, the national CIRT should start duplicating the efforts and hire a few more technical staff to ensure that a critical task is not dependent on a single staff member.

No	Area	Risk	Impact	Likelihood	Mitigation
3.	Human Resources	Once trained and experienced, staff members are offered more attractive positions elsewhere.	High	Medium	This can be tackled by having a good staff retention program in place. Continuous learning programs, opportunities to participate in conferences and workshops, and good career path will ensure staff remaining loyal to the organisation.
4.	Financial	Unable to secure a funding for the sustainability of the CIRT.	High	Low	It is unlikely that the government will not continue its support in sustaining the CIRT operation. However, the CIRT should be working out a plan for self-sustenance in the 2nd year of its operation. The plans can include activities such as charging a nominal annual fee to its constituents and also extending its services to private sectors which will be charged a certain annual fee.
5.	Facilities	Physical damage to the CIRT premise due to war or vandalism	High	Low	It is unlikely that a war will breakout but physical vandalism is possible. The national CIRT should plan for business continuity and disaster recovery.
6.	Facilities	A malfunction in computer systems or on the network appliances render the CIRT services unavailable for the CIRT analysts	Medium	Medium	A good back-up procedure will solve this issue. A manual procedure for recording data when systems are unavailable will also solve this issue.
7.	Facilities	Unavailability of power supply	High	Medium	Frequent power cuts could be a problem in urban areas of Bangladesh. Therefore back-up solutions such as Uninterruptible Power Supply (UPS) will mitigate this issue.
9.	Governance	Constituents or stakeholders do not feel that the CIRT can be trusted	High	Low	Signing of MoUs and NDAs will greatly help to mitigate this issue.

3.8 CIRT institutional and organizational requirements and arrangements

Stakeholders

The following table gives the key CIRT stakeholders in ABBMN.

Table 4: Key CIRT stakeholders

Country	Stakeholders
Afghanistan	Ministry of Communications and Information Technology Ministry of Communications and Information Technology Afghanistan National Data Centre Afghanistan Telecommunication Regulation Authority Afghanistan National Police Afghanistan Central Bank Supreme Court of Afghanistan Ministry of Interior National Directorate of Security
Bangladesh	Bangladesh Telecommunication Regulatory Commission (BTRC) Ministry of Science and Information and Communication Technology (MoSICT) Ministry of Home Affairs Ministry of Posts and Telecommunications (MoPT) Law enforcement agencies
Bhutan	Ministry of Information and Communication (MoIC) Department of Information Technology (DIT), Bhutan InfoComm and Media Authority (BICMA) Royal Bhutan Police Law enforcement agencies
Maldives	Communication Authority of Maldives (CAM) National Centre for Information Technology (NITDA) Department of National Registration (DNR) Maldives Police Services (MPS) Maldives National Defense Service (MNDF) Attorney General's Office (AGO) Maldives Open Source Society (MOSS)
Nepal	Ministry of Information and Communications (MoIC), Ministry of Science and Technology (MOST), Nepal Telecommunication Authority (NTA) High Level Commission for Information Technology (HLCIT), Office of Controller of Certification (OCC), National Information Technology Center (NITC), Nepal Police, Computer Association of Nepal (CAN) Internet Service Providers' Association of Nepal (ISPAN)

Constituencies

The following table gives the key CIRT constituencies in ABBMN.

Table 5: Key CIRT constituencies

Country	Constituencies
Afghanistan	Ministry of Communications and Information Technology Ministry of Interior Afghanistan National Data Centre Afghanistan National Police Afghanistan Telecommunication Regulatory Authority National Directorate of Security Afghanistan Central Bank Supreme Court of Afghanistan Ministry of Foreign Affairs Ministry of Agriculture, Irrigation and Livestock Ministry of Commerce and Industry Ministry of Counter Narcotics Ministry of Education Ministry of Higher Education Ministry of Finance Ministry of Mines Ministry of Public Health Ministry of Rural Development Ministry of Rural Rehabilitation and Development Ministry of Transport and Civil Aviation Ministry of Women's Affairs
Bangladesh	All government agencies, and critical national infrastructure operators.
Bhutan	All government agencies, and critical national infrastructure operators
Maldives	All government agencies, and critical national infrastructure operators.
Nepal	All government agencies, and critical national infrastructure operators.

Services to Constituents

This section describes the services recommended for CIRT, based on its evaluated constituent requirements. Technical staff members will occupy the CIRT coordination centre at all times during business hours (9:00am to 6pm, Sunday to Thursday). The staff will be under the direction of the CIRT General Manager.

CIRT should start small, utilising the available resources, increasing in size as more resources are allocated to the team. It is important to start small because this is the best way for the team to build experience and capability which are vital for the CIRT team's sustainability. This is also the best approach because it enables CIRT to get the necessary buy-in from the government; to provide continued financial and policy support throughout the growth phase of CIRT. This type of commitment is vital for the growth and sustainability of the CIRT team.

The following are the initial services that CIRT will provide to its constituents when it is operational:

Incident Handling, Response and Coordination

Incident response will be performed by CIRT. In the first instance, it will be implemented as a basic coordination service. CIRT staff will field phone calls and email from its constituents and facilitate communications between the requestor and the appropriate destination about computer attacks involving third parties. For example, if a constituent requires assistance from a Pacific Islands ISP, they can contact CIRT who will in turn contact the correct provider on the constituent's behalf. CIRT will act as a trusted intermediary between its constituents who need to contact external network providers, CIRTs, governments or other entities with security related information.

Security Advisories

CIRT Analysts will produce security advisories that target specific audiences. The types of security advisories will include:

- Security advisories for the general public. These advisories contain short information that is clear to the average home computer user, so that they may protect themselves online.
- Security advisories for business and government constituents. These will provide timely information for current activity that represents a threat to either business interests or to critical infrastructure.

Awareness

Awareness campaigns are very important to the sustainability of a CIRT. It is the only way the constituents will become aware of the existence of the national CIRT. This may take place in the form of advertising on television, websites or in print, and include media liaison and press releases, workshops, seminars and training sessions.

Advertising of CIRT constituents on the CIRT website may be done, however, this approach is risky because constituents from the private sector might not wish to be advertised because they would like to portray an image where they are viewed as independent of national monitoring. Private businesses prefer to be seen as neutral. Therefore before this is done, the team should make the necessary consultations with the constituents concerned and then evaluate the pros and cons of advertising constituents on their website.

However, this should not be an issue if the CIRT is going to serve only government agencies. Creation of a constituent email list is vital; this allows trusted communication between constituents and the CIRT team. This email list would only be open to staff of organizations which meet the criteria of CIRT constituents. 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 CIRT staff will also be required. This service is relatively easy to implement and provides a visible and useful initial engagement with constituents.

Other Potential Services

Since CIRT is still at its infant stage, it is recommended that it starts with basic proactive and reactive services for its constituents. However, all the possible services CIRT can provide have been broken down into three phases. CIRT can provide the services based on its maturity level and readiness. The following tables set out the integrated plan for the type of services CIRT can provide to its constituents in each stage.

Human Resources

It is recommended that a minimum of three staff be stationed at CIRT: the general manager and two analysts. The general manager will supervise the two analysts. Two analysts are necessary to ensure that

operations may continue with one staff member absent due to ill-health, leave or other CIRT related matters such as training, workshops or conferences.

Tables 6 and 7 show the job descriptions for the CIRT general manager and analysts.

Table 6: CIRT Manager

Position:	**CIRT Manager**
Supervisor:	Chief Security Officer (CSO)
Qualifications and Experience:	Bachelor's Degree or Master Degree in Computer Science/ ICT/ Engineering – Electronics, Telecommunications, Computer / any relevant area. Professional certification in any related field such as CISSP / GCIA / GCFA / CEH is an added advantage. Possess at least 5 (five) years of working experience in relevant field.
Personal Qualities:	Good managerial and interpersonal skills. Self-starter and has high sense of urgency in making deliverables and capable of protecting confidentiality of information. Able to prioritize tasks and manage time efficiently. Good personality with ability to work as a team player. Stress durable. Strong analytical skills. Willing to travel on short notice.
Technical Competence:	Possess high degree of interest in ICT security related areas. Sound knowledge on computer hardware. Knowledge of at least 2 operating systems (UNIX and Windows). Knowledge of Internet applications. Knowledge of security risks, threats and vulnerabilities. Knowledge of risk assessments. Knowledge on cryptographic technologies.
Areas of Responsibility and Accountability:	Reports to the CSO / GM of CIRT. Oversees, supervises and supports the entire workforce under the CIRT. Ensures service level commitments. To plan for the business continuity and disaster recovery of the operations. To advice the CSO / GM on manpower planning and resource allocation. To coordinate with other department heads / stakeholders on technical matters. To produce periodic or ad-hoc reports of high quality on the operations of CIRT. To develop, implement and maintain processes, procedures and guidelines to improve and increase the effectiveness of the operations of CIRT. To conduct knowledge sharing sessions among other technical personnel on lessons learnt or new findings. To be aware, comply with and ensure compliance with all CIRT's policies, procedures and guidelines.

Table 7: CIRT Analyst

Position:	**Analyst**
Supervisor:	CIRT Manager
Qualifications and Experience:	Bachelor's degree in Computer Science / ICT / Engineering – Electronics, Telecommunications, Computer / any relevant area. Professional certification in any related field such as GCIA / GCFA / CEH is an added advantage. Possess at least 1 (one) year of working experience in relevant field.
Personal Qualities:	Good interpersonal skills. Self-starter and has high sense of urgency in making deliverables and capable of protecting confidentiality of information. Able to prioritize tasks and manage time efficiently. Good personality with ability to work as a team player. Stress durable. Strong analytical skills. Willing to travel on short notice.
Technical Competence:	Possess high degree of interest in ICT security related areas. Sound knowledge on computer hardware. Knowledge of at least 2 operating systems (UNIX and Windows). Knowledge of Internet applications. Knowledge of security risks, threats and vulnerabilities. Knowledge of risk assessments. Knowledge on cryptographic technologies.
Areas of Responsibility and Accountability:	Reports to the CIRT Manager. To plan, execute, assess and monitor all tasks assigned under CIRT. To man the CIRT helpdesk and raise tickets for all confirmed probable incidents. To conduct risk assessment and security analysis on the reported incidents. To respond and provide support to the CIRT constituents. To produce periodic or ad-hoc reports of high quality for every incidents, security threats and vulnerabilities. To develop training modules and technical documentations. To conduct knowledge sharing sessions among other technical personnel on lessons learnt or new findings. To be aware and comply with all CIRT's policies, procedures and guidelines.

Policies and Procedures

All policies and processes must be documented. This will be produced by the CIRT staff and will inherit from sample IMPACT policies where appropriate. These policies should be produced:

- membership policy,
- security policy, and

- disaster recovery and business continuity policy.

CIRT must have standard internal operating procedures for its operations.

Promotional / Branding Materials

For marketing, brand recognition and for a professional image, CIRT should arrange a branding, prior to their establishment. Ideally, this would be done by professional designers and be available for use on the web site, business cards, letter heads and other communications of CIRT.

Awareness Campaigns

CIRT will need to announce its existence to its constituency. Awareness campaigns are very important to the sustainability of a CIRT. It is the only way the constituents will become aware of the existence of the national CIRT. This may take place in the form of advertising on television, website or print, and include media liaison and press releases, workshops, seminars and training sessions.

The following methods of communication may be considered to publicise the CIRT:

- direct communication via email and normal mail,
- advertising in print and electronic media,
- community events, such as public speaking engagements,
- unpaid radio and television interviews, and
- advertising on billboards.

3.9 Financial model

National CIRTs are generally not commercially profitable. CIRTs generally exist in a similar way as other public and emergency services. These services are not designed to make a profit, but instead work for the national benefit. The following sections describe the Capital and Operating Expenses for Afghanistan, Bangladesh, Bhutan, Maldives, and Nepal.

Capital Expense (CAPEX) Requirements

The projected capital expenses for a CIRT will include at least the following:

- Hardware (Servers, Switch, Router, Firewall, etc),
- Software to operate the CIRT (inclusive of planning, customisation, deployment, training and limited support),
- Marketing and promotion,
- Printing,
- Furniture fittings,
- Renovation of the CIRT premises, and
- Travel expenses, allowances etc.

Operating Expense (OPEX) Requirements

CIRT should also factor in its yearly operating expenses in its budgeting. Requirements for the OPEX will include:

- infrastructure and facilities, including service costs, office space rent, and other facility cost,
- salary (permanent and contract), including: Manager, analyst(s), office staff, and contractual personnel,

- travel,
- official visits and training,
- membership,
- governance, and
- official administrative costs, miscellaneous costs, and advertising costs.

Operating expenditure varies from country to country from USD 128’800 to USD 202’800.

Afghanistan

In the specific case of Afghanistan, the following elements were highlighted:

- Justifying budget requests for initiatives such as CIRT can be a daunting task in a country such as Afghanistan which still lacks ICT penetration and no clear evidence of cyber attacks.
- It is clear that there is strong support from MCIT and the government in general to fund the establishment of CIRT.

A budget proposal for the establishment of CIRT is understood to have been submitted to the Ministry of Finance of Afghanistan.

It is envisaged that for a public private partnership, a financial model needs to be created.

APPENDIX 1

Incident reporting form

CONTACT INFORMATION	
Name:	Incident number:
Title:	Date:
Agency:	Incident Date (mm/dd/yy): Time (hh:mm:ss am/pm/time zone):
Contact Number:	
Fax:	Email:

INCIDENT SUMMARY

Type of incident detected (check all that apply):

- ☐ Malicious code (Virus, Worm, Trojan)
- ☐ Denial of Service
- ☐ Unauthorized access
- ☐ Rogue access points (wireless)
- ☐ Loss of equipment
- ☐ Web defacement
- ☐ Unauthorized probe/information gathering
- ☐ System misuse
- ☐ Technical vulnerability
- ☐ Others (please specify):

Source information:

IP:	
Name and address:	
Internet service provider:	
Location:	

Target information:

Owner (System admin/user):	
IP:	
Level of information compromise:	
Operating system (including version):	

Number of Hosts Affected:

☐ < 10 ☐ 10 to 50 ☐ 50 to 100 ☐ > 100

Incident level:

- ☐ Low
- ☐ Medium
- ☐ High

Data classification:

- ☐ Public
- ☐ Restricted
- ☐ Confidential
- ☐ Secret
- ☐ Top secret

INCIDENT ASSESSMENT

Was system compromised?	
Is active attack currently on going?	
Suspicion of rootkit or keylogger compromise?	
Has compromised system used as a staging point (island hopping) for deeper attacks?	
Length of time system may have been compromised?	
Origin of attacks is from inside or outside?	

ADDITIONAL INFORMATION

Please provide additional information here:

_____
_____
_____
_____
_____
_____

INFORMATION DISCLOSURE

Who can this information be shared with:

☐ Other Agencies ☐ Law Enforcement ☐ IMPACT ☐ No sharing is authorized

SIGNATORY (CIRT/CIRT use only)

This report is received by:

Name:
Position:
Date (mm/dd/yy):
Time (hh:mm:ss am/pm):

APPENDIX 2

Advisory Template

VULNERABILITY

DETAILS

CVE/CAN Name	
Description	
First Sample Seen	
Discovery Date	
IMPACT Threat Level	
National Threat Level	
Affected System/Software	
Currently Known Exploits	
Solution	
References	
Credits	
Revisions	

DEFINITIONS

- Vulnerability: Identifier of the vulnerability.
- Description: Summary of the cause and potential effect of the vulnerability provided by IMPACT.
- First Sample Seen: Date of the first sample seen by national authority.
- Discovery Date: Date of the earliest known publically disclosed advisory.
- IMPACT Threat Level: Threat level assigned by IMPACT
- CIRT Threat Level: Threat level assigned by CIRT
- LOW – There is little chance of this vulnerability being actively exploited by malware.
- MEDIUM – There is a possibility of this vulnerability being actively exploited by malware.
- HIGH – There is a strong possibility of this vulnerability being actively exploited by malware.
- Affected System/Software: Vulnerable platforms and software versions.
- Currently Known Exploits: List of identities for known exploits, if applicable.
- Solution: IMPACT-supplied patch identifier and recommended solution, or workaround if applicable.

APPENDIX 3

CIRT Advisory Sample

VULNERABILITY	
APSB09-15 Security Advisory for Adobe Reader and Acrobat	
DETAILS	
CVE/CAN Name	CVE-2007-0048, CVE-2007-0045, CVE-2009-2564, CVE-2009-2979, CVE-2009-2980, CVE-2009-2981, CVE-2009-2982, CVE-2009-2983, CVE-2009-2984, CVE-2009-2985, CVE-2009-2986, CVE-2009-2987, CVE-2009-2988, CVE-2009-2989, CVE-2009-2990, CVE-2009-2991, CVE-2009-2992, CVE-2009-2993, CVE-2009-2994, CVE-2009-2995, CVE-2009-2996, CVE-2009-2997, CVE-2009-2998, CVE-2009-3431, CVE-2009-3458, CVE-2009-3459, CVE-2009-3460, CVE-2009-3461, CVE-2009-3462
Description	A critical vulnerability (CVE-2009-3459) has been identified in Adobe Acrobat and Adobe Reader 9.1.3 and earlier versions on Windows, Unix and OS X. This vulnerability allows remote attackers to execute arbitrary code on vulnerable installations of Adobe Acrobat and Adobe Reader. User interaction is required in that a user must visit a malicious web site or open a malicious PDF file.
First Sample Seen	10 October 2009
Discovery Date	08 October 2009
IMPACT Threat Level	High
National Threat Level	High
Affected System/Software	Adobe Reader 9.1.3 for Windows, Macintosh and UNIX Acrobat 9.1.3 for Windows, Macintosh and UNIX Adobe Reader 8.1.6 for Windows, Macintosh and UNIX Acrobat 8.1.6 for Windows, Macintosh and UNIX Adobe Reader 7.1.3 for Windows and Macintosh Acrobat 7.1.3 for Windows and Macintosh
Currently Known Exploits	Troj/PDFJs-DS – CVE-2009-3459
Solution	The official security patch for this vulnerability has not been released by the vendor as of the writing of this advisory. Adobe plans to releases updates for this issue on October 13, 2009. It will be available for download at this URL: http://get.adobe.com/reader/ As a workaround, it is advisable for users to disable the JavaScript feature in Adobe Acrobat and Adobe Reader.
References	www.adobe.com/support/security/bulletins/apsb09-15.html
Credits	Adobe
Revisions	14 October 2009 – Initial analysis written

APPENDIX 4

Terms of Reference for Chief Security Officer (CSO) of national authority

The CSO shall be appointed by the ICT Directorate of the Afghanistan Ministry of Communication and Information Technology (MCIT). The CSO shall be responsible and accountable for cybersecurity implementation, monitoring and improvement. Apart from security management, the CSO shall also establish strategic relationships with various relevant agencies and take part in strategic decision making matters related to cybersecurity of the nation.

The CSO is responsible for developing and maintaining an organization-wide cybersecurity program and as the focal point of the national authority, the CSO shall have the following responsibilities:

- overall procurement, development, integration, modification, operation and maintenance of the cybersecurity system;
- identifying the latest monitoring trends and developments within the scope of cybersecurity and serve as the advisory officer to the local government ministries and agencies regarding cybersecurity risks, countermeasure steps and industry best practices;
- reviewing externally released incident reports for completeness and she/he shall provide guidance for all matters requiring legal consultation prior to disclosure to the local or international law enforcement agencies;
- managing the identification, implementation and assessment of common security controls;
- developing and monitoring a formal procedure for reporting cybersecurity incidents and investigations;
- arranging and/or providing cybersecurity education and training to each and everyone within the national cybersecurity authority to ensure that everyone receives the requisite trainings;
- protection and preservation of all national cybersecurity authority assets such as the employees, servers, computers, network components, information (both in soft and hard forms) and other important systems;
- ensuring that the facility housing the national cybersecurity authority has sufficient security measures and controls to deter intrusion and unauthorised access. She/He will manage the physical security and safety of the premise;
- ensuring compliance with local regulatory requirements and standards as well as international standards where applicable; and
- establishing and implementing recovery plans which can be used by local government agencies in case of extreme attacks on local systems. These plans shall have a well documented implementation procedure that shall be used to initiate disaster recovery and business continuity.

APPENDIX 5

Membership policy

Objective

The objective of this policy is to provide guidance of the terms and conditions to become a member of the national cybersecurity authority.

Background

The national cybersecurity authority is a non-profit organization. The initial charter is to address the cybersecurity concerns of government agencies and ministries. Its services may be extended beyond the boundaries of government in the future subject to maturity and readiness. Locally, the national cybersecurity authority works closely with the relevant legal bodies, such as the police, regulatory authorities, and ministries of justice.

Membership Benefits

By becoming a member, government agencies or ministries will have access to timely threat and vulnerability alerts and priority access to incident management services not readily available to non-members.

Membership Policy

The membership is only open to government agencies and ministries.

The appointed member (also known as constituent) must nominate a focal point to the national cybersecurity authority who will treat this nominated person and restrict its communications to this person in matters pertaining to cybersecurity incidents.

It is the responsibility of the member to:

- comply with all reasonable requests made of it by the national cybersecurity authority to facilitate delivery of services;
- ensure that no unauthorised person or organization is able to access, use, copy or disseminate the materials and services which are offered exclusively to members;
- not breach any laws, either local or international, in the use of the national cybersecurity authority materials and services;
- not sell, transfer, distribute or provide copies of the materials to any third party organization unless such organization is a contractor or consultant of the member and the contractor or consultant agrees to abide by this membership policy and that use is limited to the provision of the contractor's or consultant's services to the member; and
- indemnify and hold the national cybersecurity authority and each and every member of its staff harmless from any loss, cost, expense or liability arising from any claims, demands or proceedings against them where such claims relate in whole or in part to use, misuse or attempted use of the materials and services provided by the national cybersecurity authority.

Handling of Member Information

The member warrants that it is the owner of any member information which it supplies to the national cybersecurity authority and that it has the necessary rights to supply this information.

Member information supplied to the national cybersecurity authority will be handled as confidential information and will:

- only be supplied to those national cybersecurity authority personnel who require access to the member information for the purposes of delivering the services, and
- not be disclosed to any other party without the member's express consent unless that disclosure is required by law.

No Warranty or Guarantee

The national cybersecurity authority will perform the services with due care and skill.

The national cybersecurity authority does not guarantee the member against any cybersecurity incidents or attacks.

Suspension of Services

Failing to adhere to all or a part of the policies in this document will result in suspension of services to the member until the necessary steps are taken to clear the dispute.

APPENDIX 6

Hardware and software specifications

Enterprise grade rack mount computers are recommended for the CIRT, to ensure reliability and redundancy. The CIRT shall require a variety of software operating systems and applications. As with many organizations, the CIRT shall require general office and productivity applications. Dedicated software tools may also be required for specific applications in CIRT operations.

Where possible, open source systems should be selected. However, commercial off-the-shelf systems are recommended if considered more suitable for the task or environment. This decision is based on the assumption that there will be sufficient technical skills within the CIRT, to install, configure and run open source systems, without the need for commercial support which a vendor may provide.

The hardware and software requirements are interrelated. For a CIRT to operate at optimal level from the beginning, it is important to start investing in some good CIRT automation tools which will cover, at least, modules such as **Incident Management**, **Public Portal**, **Mailing List** and **Advisory.** This set of tools will enable the newly established CIRT to kick start its operations and services. The table below shows the minimum hardware specifications for the national CIRT to host the above mentioned applications:

Items	Quantity
Back-end Server – 2U rack height, Intel Processor 2.0GHz, 8GB of RAM, 500GB of HDD (RAID 1), Network Interface Card Note: No operating system cost, since it would be LINUX installation	3
Firewall – (e.g. Cisco ASA 5505-UL-BUN-K9)	2
Router – (e.g. Cisco 2811)	1
Switch – (e.g. Cisco WS-C2960-24TT-L)	2
Computers / Notebooks/ Printers/ Photocopier/ Fax machine	According to the number of staff within the CIRT

APPENDIX 7

Premises

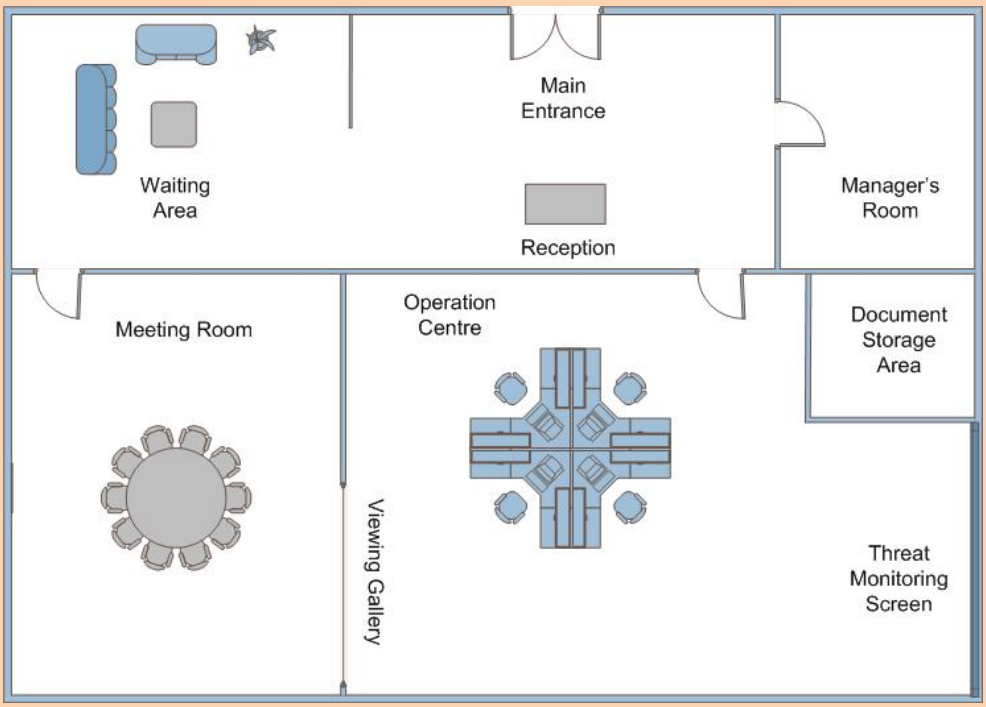
The national cybersecurity authority facility should be inspected for compliance with its requirements. It will operate as an entity within an official facility. The nature of its operations makes it necessary for these premises to have a higher level of security than the general space in which it is enclosed. To ensure separation of function, a physical security perimeter will be necessary; in practice, this will entail a separate office space.

The premises should have the following characteristics:

- a separate reception/waiting room for visitors,
- an operations centre where the analysts conduct day-to-day activities. Other functions, such as research, may be performed in this space,
- an office for the manager, large enough so that private meetings can be accommodated,
- the path from the reception area to this office should not transit the operations centre,
- a meeting room. Ideally the meeting room should have a viewing gallery where visitors can view the operations centre without entering inside, and
- a data storage area for documents and network equipment. This could incorporate rack space for ICT infrastructure (see IT Infrastructure).

Figure 6.1 shows a proposed high-level design for BtCIRT.

Figure 10: Proposed floor plan for a CIRT



APPENDIX 8

IT infrastructure

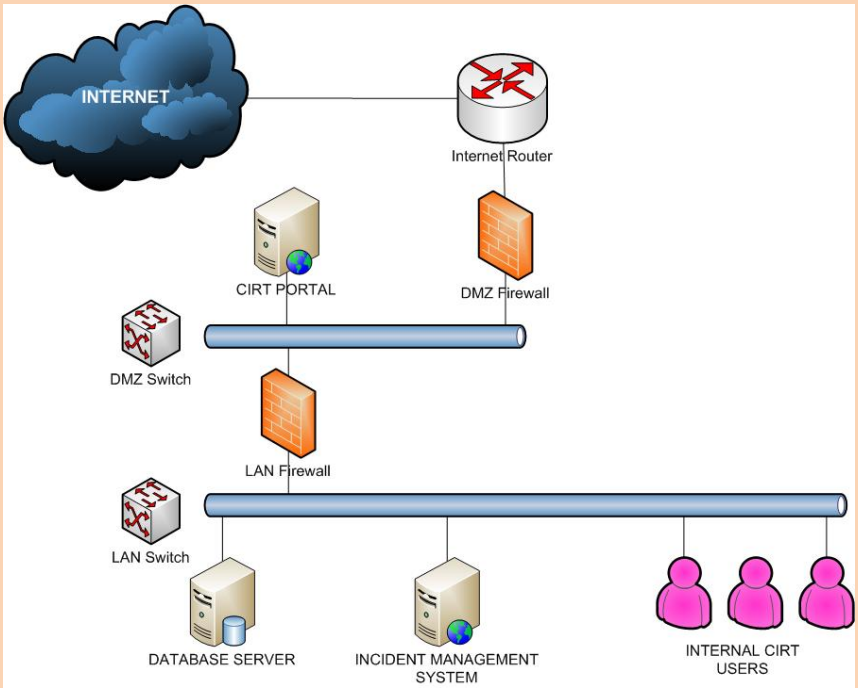
A dedicated IT infrastructure is required to ensure adequate data separation for investigations and coordination work. Some overlap with infrastructure may be appropriate for certain functions provided that adequate transparency and audit of operation is possible. Generally, the national cybersecurity authority should retain control of its own network border firewall, with a dedicated network connection like DSL or leased line. This means that the following assets should remain under the exclusive control of the national cybersecurity authority:

- network border firewall,
- primary computing hardware for operational data, and
- backup equipment for data.

Access to the ICT infrastructure should be restricted, either from within the secure perimeter or another secure space within the data centre of its building. A lockable server rack will be required for the machines and the rack must be located in a secure storage room.

The network design should be kept simple and practical. Figure 6.2 shows a proposed network topology.

Figure 11: Proposed network topology



The network can be as simple as the above diagram with a single public IP address. However, availability of more public IP addresses will provide an avenue for seamless scalability for the network to cater for more complex and dynamic constituencies.

A firewall/router will connect to the Internet. Network Address Translation (NAT) would be used to configure private networks behind this router. The network shall consist of:

- DMZ Firewall: hosting services which are to be accessed by clients external to the national cybersecurity authority (e.g. web server),
- Internal Servers: hosting services which are to be accessed only by staff (e.g. Incident Management System, Portal and Database), and
- LAN Switch: to provide LAN services to staff.

APPENDIX 9

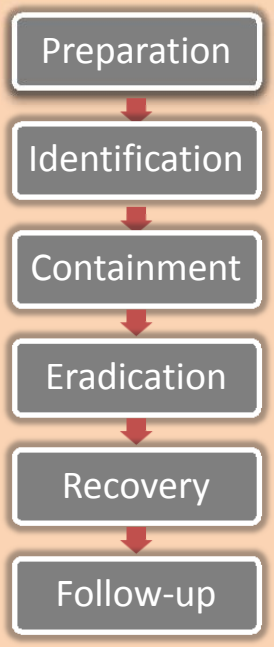
Proposed standard operating procedure (SOP)

Introduction

Security-related incidents can be caused by violations of policy and procedure, intrusions and also exploitation of system vulnerabilities. These events could result in compromise, damage or loss of confidentiality, integrity and availability of information and resources.

In an incident response process, it is very important for the Computer Incident Response Team (CIRT) to mitigate the incident as soon as possible to minimize loss of data and resources. The process should follow a proper guideline that is developed based on a well-defined incident response framework (as illustrated in Figure 1 below). The framework which comprises six phases ensures a consistent and systematic approach in handling such incidents. Each of the phases is elaborated in detail in section 5.

Figure 12: Six phases in incident response framework



Scope

The primary audience of this document includes those who may participate in the preparation, identification, containment, eradication, recovery and follow-up efforts.

Definitions[65]

Security-related incident	Any adverse event that threatens the security of information resources, including disruption or loss of confidentiality, integrity, or availability of data. Adverse events include, but are not limited to, attempts (successful or persistent) to gain unauthorized access to an information system or its data; unwanted disruption or denial of service; unauthorized use of a system; and changes to system hardware, firmware, or software characteristics without the owner's knowledge, instruction, or consent. Examples include insertion of malicious code (for example, viruses, Trojan horses, or back doors), unauthorized scans or probes, successful or persistent attempts at intrusion, and insider attacks.
Constituency	A group of people and/or organizations that have specific services offered.

Procedure

The workflow for the incident response process is depicted in Figure 3 below:

Preparation:

receive report

This is the preliminary phase of the incident handling process, during which the incident shall be reported via various means; authority portal, email, phone, fax or other available means.

The report received shall include a description of the incident and as much of the following information as possible; however, subsequent actions should not be delayed in order to gain additional information:

- name of reporting agency/partner,
- point of contact information including name, telephone, and email address,
- incident date and time, including time zone,
- source IP, port, and protocol,
- destination IP, port, and protocol,
- operating System, including version, patches, etc.,
- system Function (e.g., DNS/web server, workstation, etc.),
- antivirus software installed, including version, and latest updates,
- location of the system(s) involved in the incident, and
- method used to identify the incident (e.g., firewall, IDS, IPS, audit log analysis, system administrator).

The information provided by constituencies shall be used to complete the Incident Reporting Form. A unique incident number must be assigned to each case.

[65] The definitions are derived from Incident Prevention, Warning, and Response (IPWAR) Manual, USDOE, 205.1-1, Sep 2004 and also Handbook for Computer Security Incident Response Teams (CSIRT), 2nd Edition, April 2003.

Depending on the severity of the incident, it may not be always feasible for the reporting agency/partner to gather all the information prior to reporting. In this case, the team shall continue with the next step of the incident response process as further information is being collected.

Identification

Preliminary investigation and validity

When an incident is reported, a preliminary investigation shall be conducted to determine the validity of the incident. During this process, the team has to determine whether it is a real incident or a false alarm. False alarms can be triggered by many events such as system misconfiguration, ISP service interruption, network component failure.

If a valid incident is reported, section 5.2.2 is followed in order to identify the severity of the incident. If it is a false alarm, section 5.3.1 is followed to dismiss the alarm.

Identify severity of incident

Once it is confirmed that the incident is valid, the severity level of the incident shall be determined. The severity identification will help to determine the necessary actions that should be performed to remediate the incident.

The team can classify the incident severity by considering the affected users of the system, and also the classification of information at risk due to the incident. Some of the questions that can be asked to assist the team in determining the severity are listed in the Incident Reporting form.

Determining the level of severity shall be conducted by referring to the table below.

Table 8 – Incident severity and response time

Impact, activities and actions	Severity level		
	Low	Medium	High
Impact – Loss of system confidentiality, integrity, and availability.	Expected to have a limited effect on operations, assets, or individuals.	Expected to cause major damage to operations, assets, or individuals.	Expected to cause loss or severe damage to operations, assets, or individuals.
Activities	Monitoring activity of services that threaten information and resources	Interception of critical communication Disruption of non-critical services Unauthorized access and usage of information and resources	Unauthorized disclosure, modification or deletion of sensitive information Disruption of critical services
Information escalation	National cyberscurity authority	National cyberscurity and higher authority	National cyberscurity and higher authority
Maximum response time	72 hours	48 hours	24 hours

Report incident to IMPACT

If the team needs assistance in resolving the incident, a report can be made to the Global Response Centre (GRC) of IMPACT to request assistance in the remediation process.

The team can use the GRC portal to report the incident or by other means necessary; email, fax, or phone.

Remediation

Log incident and ignore

During the event where the reported incident is a false alarm, the team shall log the incident and take no further action other than contact the affected constituency to inform them of the end of the reported incident.

Remediate incident

In order to remediate the incident, the team is generally responsible to assist and/or to advice its constituency to:

- isolate the system,
- monitor the incident,
- warn the relevant constituencies affected by the incident and providing emergency instructions to them,
- report to relevant law enforcement agencies if necessary, and
- request additional resources from IMPACT or other relevant agencies.

The team shall decide whether it has the capacity and capability to resolve the incident on its own or seek assistance from IMPACT. If the team needs assistance, a report shall be made to IMPACT by any available communication channels such as GRC Portal, phone, email or fax.

The team shall send recommendations and suggestions to the reporting constituency to remediate the incident. The team shall ensure that the constituency is able to resume normal operations. Relatively simple incidents, such as attempted but unsuccessful intrusions into systems, require only assurance that the incident did not in any way affect system software or data stored on the system. Complex incidents, such as malicious code planted by insiders, may require a complete restore operation from clean backups or a complete reinstall of the operating system and software applications. It is essential to verify a restore operation was successful and that the system is back to a normal condition.

Follow-up

Notify IMPACT if necessary

Information on any part of the incident response process can be sent to IMPACT if the team believes that the information will benefit other parties around the world. The team shall decide the extent of information disclosure prior to releasing the information to IMPACT. The information shall only be shared after removing organization-specific and country-specific information.

Submit report to constituency

An incident report shall be created and disseminated to the constituency at the end of the incident response exercise. Some of the elements that should be included in the report are as follows:

- a description of the exact sequence of events,
- the type and severity of incidents,
- remediation measure put in place,
- assessment to determine if the remediation steps taken are sufficient, and
- recommendations need to be considered for improvement.

The report shall be reviewed by management prior to releasing it to the affected constituency. This is to ensure the document is properly prepared and contains sufficient information needed by the constituency.

Update knowledge base

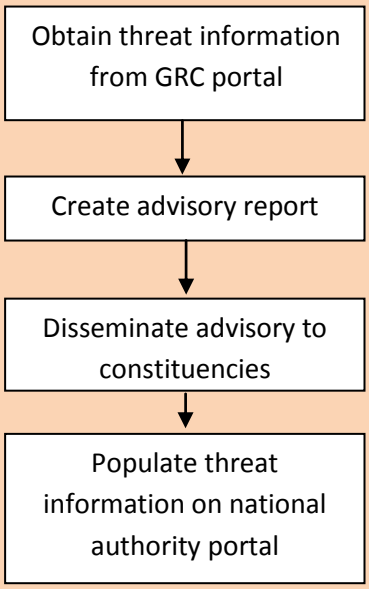
Once the reporting constituency resumes normal operations, the team shall update the knowledge base. Among other things to update are details on the incident, how it was remediated and lessons learnt, to improve on the identified areas and used as reference for future incidents.

Depending on the confidentiality agreement with the constituency, some information may be removed before being updated to the knowledge base.

Advisory to constituency

One of the important roles of the national cybersecurity authority is to provide threat advisories to its constituencies. The team shall follow the workflow depicted in Figure 3 below in order to disseminate threat advisories:

Figure 13: Advisory dissemination workflow



Obtain threat information from GRC of IMPACT

In order to provide advisories to its constituencies, national authority shall routinely review threat information from the GRC portal of IMPACT.

Create advisory report

Once the advisories are obtained, the team shall use the information obtained from GRC portal to create an advisory report for its constituencies. The advisory report shall be created by completing the Advisory Template in Appendix A2. An example of a completed advisory is given in Appendix A3.

Disseminate advisory to constituencies

Once the advisory report is completed, the CIRT shall disseminate the report to its constituencies via email.

Populate threat information on web Portal

The threat information can also be made available to its constituency and the general public by uploading the information to the portal.

Documentation

All details related to the incident response process shall be documented and filed for tracking and easy reference. This provides valuable information to unravel the course of events and can serve as evidence if prosecution is necessary. It is recommended that the following items be maintained:

- system events (log records),
- summary of incident (including how the incident occurred, category, severity and origin of the incident),
- incident response action taken (including the time that an action is performed), and
- communication with all external parties (including the person with whom the discussion was held, the date and time and the content of the communication).

List of acronyms, abbreviations and references – Afghanistan

AfCERT	Afghanistan Cyber Emergency Response Team
ATRA	Afghanistan Telecom Regulatory Authority
CERT	Cyber Emergency Response Team
CIRT	Computer Incident Response Team
CSIRT	Computer Security Incident Response Team
DDOS	Distributed Denial of Service
DOS	Denial of Service
DRM	Digital Rights Management
ICT	Information and Communication Technologies
ITU	International Telecommunication Union
ISP	Internet Service Provider
IMPACT	International Multilateral Partnership Against Cyber Threats
MCIT	Ministry of Communication and Information Technology
PKI	Public Key Infrastructure

References

a. CSIRT Services – www.cert.org/csirts/services.html

b. A step-by-step approach on how to setup a CSIRT – www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide

c. Computer Security Incident Handling Guide (NIST) – http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

d. Malaysia National Cyber Security Policy (NCSP) – www.nitc.my/index.cfm?&menuid=57

e. AusCERT – Creating and Managing Computer Security Incident Handling Teams (CSIRTs) – www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

f. Benefits of National CERTS – www.cert.org/archive/pdf/NationalCSIRTs.pdf

g. ITU ICT Development Index (IDI) 2010 – www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf

h. A generic National Framework for CIIP – www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

i. International CIIP Handbook: An Inventory and Analysis of National Protection Policies – www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

j. Afghanistan Telecom Regulatory Authority – www.atra.gov.af/

k. Implementation of WSIS Action Line C5 www.itu.int/wsis/c5/index.html

l. ITU Global Cybersecurity Agenda www.itu.int/osg/csd/cybersecurity/gca/

m. ITU Activities related to Cybersecurity www.itu.int/cybersecurity/

n. COP Guidelines www.itu.int/osg/csd/cybersecurity/gca/cop/index.html

List of acronyms, abbreviations and references – Bangladesh

A2I	Access to Information
BB	Bangladesh Bank
BdCERT	Bangladesh Computer Emergency Response Team
BdCIRT	Bangladesh Computer Incident Response Team
BTCL	Bangladesh Telecommunications Company Limited
BTRC	Bangladesh Telecommunication Regulatory Commission
BTTB	Bangladesh Telegraph and Telephone Board
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CNII	Critical National Information Infrastructure
DDOS	Distributed Denial of Service
DOS	Denial of Service
FIRST	Forum of Incident Response and Security Teams
GRC	Global Response Centre
ICT	Information and Communication Technologies
IIG	International Internet Gateway
IMPACT	International Multilateral Partnership Against Cyber Threats
IPLC	International Private Leased Circuit
ISP	Internet Service Provider
ITU	International Telecommunication Union
MoPT	Ministry of Posts and Telecommunications
MoSICT	Ministry of Science and Information and Communication Technology
PKI	Public Key Infrastructure

References

a. CSIRT Services – www.cert.org/csirts/services.html
b. A step-by-step approach on how to setup a CSIRT – www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide
c. Computer Security Incident Handling Guide (NIST) – http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
d. Malaysia National Cyber Security Policy (NCSP) – www.nitc.my/index.cfm?&menuid=57
e. AusCERT – Creating and Managing Computer Security Incident Handling Teams (CSIRTs) – www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf
f. Benefits of National CERTS – www.cert.org/archive/pdf/NationalCSIRTs.pdf
g. ITU ICT Development Index (IDI) 2010 – www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf
h. A generic National Framework for CIIP – www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
i. International CIIP Handbook: An Inventory and Analysis of National Protection Policies – www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
j. Bangladesh Telecommunication Regulatory Commission – http://btrc.gov.bd/
k. Implementation of WSIS Action Line C5 www.itu.int/wsis/c5/index.html
l. ITU Global Cybersecurity Agenda www.itu.int/osg/csd/cybersecurity/gca/
m. ITU Activities related to Cybersecurity www.itu.int/cybersecurity/
n. COP Guidelines www.itu.int/osg/csd/cybersecurity/gca/cop/index.html

List of acronyms, abbreviations and references – Bhutan

BoB	Bhutan of Bank
BtCIRT	Bhutan Computer Incident Response Team
BTL	Bhutan Telecom Limited
DIT	Department of Information Technology and Telecom
BICMA	Bhutan Infocomm and Media Authority
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CNII	Critical National Information Infrastructure
DDOS	Distributed Denial of Service
DOS	Denial of Service
FIRST	Forum of Incident Response and Security Teams
GRC	Global Response Centre
ICT	Information and Communication Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats
ISP	Internet Service Provider
ITU	International Telecommunication Union
MoIC	Ministry of Information and Communication
PKI	Public Key Infrastructure

References

a. CSIRT Services – www.cert.org/csirts/services.html

b. A step-by-step approach on how to setup a CSIRT – www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide

c. Computer Security Incident Handling Guide (NIST) – http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

d. Malaysia National Cyber Security Policy (NCSP) – www.nitc.my/index.cfm?&menuid=57

e. AusCERT – Creating and Managing Computer Security Incident Handling Teams (CSIRTs) – www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

f. Benefits of National CERTS – www.cert.org/archive/pdf/NationalCSIRTs.pdf

g. ITU ICT Development Index (IDI) 2010 – www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf

h. A generic National Framework for CIIP – www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

i. International CIIP Handbook: An Inventory and Analysis of National Protection Policies – www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

j. Bhutan Telecommunication Regulatory Commission – http://DIT.gov.bd/

k. Implementation of WSIS Action Line C5 www.itu.int/wsis/c5/index.html

l. ITU Global Cybersecurity Agenda www.itu.int/osg/csd/cybersecurity/gca/

m. ITU Activities related to Cybersecurity www.itu.int/cybersecurity/

n. COP Guidelines www.itu.int/osg/csd/cybersecurity/gca/cop/index.html

List of acronyms, abbreviations and references – Maldives

ADB	Asian Development Bank
CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CAM	Communication Authority of Maldives
CNII	Critical National Information Infrastructure
DDOS	Distributed Denial of Service
DNR	Department of National Registration
DOS	Denial of Service
FIRST	Forum of Incident Response and Security Teams
MvCIRT	Maldives Computer Incident Response Team
GRC	Global Response Centre
ICT	Information and Communication Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats
ISP	Internet Service Provider
ITU	International Telecommunication Union
MCAC	Ministry of Civil Aviation and Communication
MCST	Ministry of Communications, Sciences and Technology
MOE	Ministry of Education
MoHA	Ministry of Home Affairs
NCIT	National Centre for Information technology
PKI	Public Key Infrastructure
MPS	Maldives Police Service
MNDF	Maldives National Defense Service
MOSS	Maldives Open Source Society

References

a. CSIRT Services – www.cert.org/csirts/services.html

b. A step-by-step approach on how to setup a CSIRT – www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide

c. Computer Security Incident Handling Guide (NIST) – http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf

d. Malaysia National Cyber Security Policy (NCSP) – www.nitc.my/index.cfm?&menuid=57

e. AusCERT – Creating and Managing Computer Security Incident Handling Teams (CSIRTs) – www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf

f. Benefits of national CERTS – www.cert.org/archive/pdf/NationalCSIRTs.pdf

g. ITU ICT Development Index (IDI) 2010 – www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf

h. A generic National Framework for CIIP – www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf

i. International CIIP Handbook: An Inventory and Analysis of National Protection Policies – www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250

j. Communications Authority of Maldives – www.cam.gov.mv

List of acronyms, abbreviations and references – Nepal

CERT	Computer Emergency Response Team
CIRT	Computer Incident Response Team
CNII	Critical National Information Infrastructure
DDOS	Distributed Denial of Service
DOS	Denial of Service
FIRST	Forum of Incident Response and Security Teams
GRC	Global Response Centre
ICT	Information and Communication Technologies
IMPACT	International Multilateral Partnership Against Cyber Threats
ITU	International Telecommunication Union
ISP	Internet Service Provider
MOST	Ministry of Science and Technology
MOIC	Ministry of Information and Communication
PKI	Public Key Infrastructure
NTA	Nepal Telecommunication Authority
NITC	National Information Technology Center
HLCIT	High Level Commission for Information Technology
NpCIRT	Nepal Computer Incident Response Team
ISPAN	Internet Service Provider's Association of Nepal

References

a. CSIRT Services – www.cert.org/csirts/services.html
b. A step-by-step approach on how to setup a CSIRT – www.enisa.europa.eu/act/cert/support/guide/files/csirt-setting-up-guide
c. Computer Security Incident Handling Guide (NIST) – http://csrc.nist.gov/publications/nistpubs/800-61-rev1/SP800-61rev1.pdf
d. Malaysia National Cyber Security Policy (NCSP) – www.nitc.my/index.cfm?&menuid=57
e. Creating and Managing Computer Security Incident Handling Teams (CSIRTs) – www.first.org/conference/2008/papers/killcrece-georgia-slides.pdf
f. Benefits of National CERTS – www.cert.org/archive/pdf/NationalCSIRTs.pdf
g. ITU ICT Development Index (IDI) 2010 – www.itu.int/ITU-D/ict/publications/idi/2010/Material/MIS_2010_without%20annex%204-e.pdf
h. A generic National Framework for CIIP – www.itu.int/ITU-D/cyb/cybersecurity/docs/generic-national-framework-for-ciip.pdf
i. International CIIP Handbook: An Inventory and Analysis of National Protection Policies – www.crn.ethz.ch/publications/crn_team/detail.cfm?id=250
j. Nepal Telecommunications Authority – www.nta.gov.np
k. High Level Commission for Information Technology – http://hlcit.gov.np/
l. National Information Technology Center – www.nitc.gov.np/
m. Implementation of WSIS Action Line C5 – www.itu.int/wsis/c5/index.html
n. ITU Global Cybersecurity Agenda – www.itu.int/osg/csd/cybersecurity/gca/
o. ITU Activities related to Cybersecurity – www.itu.int/cybersecurity/
p. COP Guidelines – www.itu.int/osg/csd/cybersecurity/gca/cop/index.html
q. Ministry of Information and Communications (Nepal)- www.moic.gov.np/

International Telecommunication Union
Telecommunication Development Bureau
Place des Nations
CH-1211 Geneva 20
Switzerland
www.itu.int

Printed in Switzerland
Geneva, 2012

01/2012