འབྲུག་བདེ་དོན་བཙུང་འཕེལ་དང་བདེ་བཙུང་དབང་འཛིན།

BHUTAN INFOCOMM AND MEDIA AUTHORITY

ROYAL GOVERNMENT OF BHUTAN

Study report on Cybersecurity

July, 2020

1. Background

Information and Communication Technology (ICT) has played a vital role in the evolution of modern societies and its progression in various fields. Apart from ICT's role in creating a platform for exchange of information during its early evolution, ICT now has become the backbone of modern social networks, business, advanced critical infrastructure and services including energy grids, transport network and healthcare systems.

In this modern world, we are heavily dependent on ICT infrastructure and digital technology but at the same time, we have become more vulnerable to the rapidly evolving cyber threats, cyber-attack, electronic fraud, disruption of service and damage to the property. Cyber-insecurity issues will affect the accessibility, confidentiality, integrity and availability of ICT infrastructure to the people and it may also hinder in leveraging digital technology to drive the country's economy.

Every country endeavours to create a secure, reliable and trusted digital environment to realise the full potential of the technology by incorporating the national security goal. By developing and implementing a National Cybersecurity Strategy, a nation can improve the security of the digital infrastructure and ultimately contributes towards the socio-economic prosperity of the nation.

Cybersecurity is the collection of tools, policies, security concepts, security safeguards, guidelines, risk management approaches, actions, training, best practices, assurance and technologies that can be used to protect the cyber environment and organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment[1]

2. Legal Provisions on Cybersecurity, Data Protection and Protection of Online and Offline Privacy

Legal provisions of Cybersecurity under Information Communication and Media (ICM) Act of Bhutan 2018;

1. Chapter 17 of the ICM Act encompasses provision on Protection of Online and Offline privacy.

   i. Section 336 of the Act states an ICT and Media facility or service provider and vendors shall respect and protect the privacy and sensitive personal information of the users or consumers.

[1] The International Telecommunication Union (ITU), The World Bank, Commonwealth Secretariat (ComSec), the Commonwealth Telecommunications Organization (CTO), NATO Cooperative Cyber Defence Centre of Excellence (NATO CCD COE). 2018. Guide to Developing a National Cybersecurity Strategy – Strategic engagement in Cybersecurity. Creative Commons Attribution 3.0 IGO (CC BY 3.0 IGO)

ii. Section 337 of the Act states an ICT and Media facility or service provider and vendor shall put in place a privacy policy easily accessible from the website and from other mediums.

2. Chapter 20 (Cybersecurity) of the ICM Act of Bhutan, 2018;

i. Section 375 of the Act provides protection of personal rights and security to the citizens in the cyber world.

ii. Section 376 and 377 of the Act states that the minister may ,by warrant of the court, issue directives to relevant agencies or department to block, intercept ,decrypt or monitor any information in interest of sovereignty, security, harmony and defence of Bhutan or friendly relations with foreign States. The procedure and safeguards for blocking access by the public, interception or monitoring or decryption may be carried out in accordance with the Rules and Regulations issued by the Minister.

iii. Section 379 and 380 of the Act states power of minister to authorize, monitor and collect traffic data or information

iv. Section 381of the Act states that the ministry may, in consultation with the Authority, declare any ICT and media infrastructure as Critical information Infrastructure.

v. Section 382 of the Act states that the Government shall by directives establish an agency called the Bhutan Computer Incident Response Team(BCIRT) which shall serve as national agency to coordinate cyber security activities and be a central point of contact on all cyber security matters pertinent to national security in the country.

vi. Section 383 of the Act states that the BCIRT shall establish policies and procedures required to implement its functions under this Act.

Chapter 21 (Data Protection) of the ICM Act of Bhutan 2018:

i. Section 384,385 and 386 of the Act describes the principles governing collection of data electronically and its disclosure.

3. Responsibility with MoIC and BICMA on the cybersecurity

The responsibility related to cybersecurity and data protection issue with MoIC and BICMA are as follow in the table given below:

MoIC	BICMA
1. The minister may, by warrant of the court, issue directives to relevant agencies or department to block, intercept, decrypt or monitor of any information in interest of sovereignty, security, harmony and defence of Bhutan or friendly relations with foreign States and in the interest of public order and for investigation of any offence under this Act. 2. To develop and issue Rules and Regulation for governing the procedure and safeguards for blocking access by the public interception or monitoring or decryption. 3. The Ministry has the power to authorize agencies or department to monitor and collect traffic data or information as and when required. 4. May declare any ICT and media infrastructure as infrastructure as critical Information Infrastructure with consultation with the Authority. 5. As per section 382 of the Act, Government shall by directives establish an agency called the Bhutan Computer Incident Response Team (BCIRT) which shall be a central point of contact on all cyber security matters pertinent to national security in the country. 6.BtCIRT shall establish policies and procedures required to implement its functions under the Act.	1. To monitor and collect traffic data or information if the minister direct to do so. 2. May recommend ministry on the critical information infrastructure. 3. To put in place license terms and conditions on data protection, legal interception, online and offline privacy while issuing licenses/permits to Telecom service providers, Internet service providers, network vendors or service providers.

4. Activities carried out by MoIC on Cybersecurity:

The activities carried out by DITT, MoIC on cybersecurity related are as follows;

1. DITT, MoIC in collaboration with Global Cybersecurity Capacity Center has drafted the study report titled "Building Cybersecurity Capacity in Kingdom of Bhutan" in 2015.

2. Formation of BtCIRT

- The Government (MoIC) has established an agency called Bhutan Computer Incident Response Team (BtCIRT) in year 2016 which is supposed to be a central point of contact on all cyber security matters pertinent to national security in the country.
- BtCIRT has maintained a separate website and Facebook page for facilitating Cyber incident reporting and latest cyber alerts and news.
- BtCIRT, since its inception in 2016 up until May 2020, has handled around 655 cyber incidents. 75% constitutes vulnerabilities in systems detected by the team, 12% comprising malware/bots and, 13% comprising other incidents such as phishing, ransomware, crypto mining, DDoS, information gathering, spam and, social media cases. More than 90% of the incidents recorded thus far have been detected by BtCIRT with proactive monitoring and security feed analysis, as opposed to only 10% of the incidents being reported by constituents[2].
- BtCIRT uses Traffic Light Protocol (TLP) for information classification. The Traffic Light Protocol (TLP) was created to encourage greater sharing of sensitive information. It is designed to improve the flow of information between individuals, organizations or communities in a controlled and trusted way.

3. Drafted the Cyber security strategy

- MoIC has drafted the cybersecurity strategy and the first task force meeting on cybersecurity was held from 18th may to 22nd may to draft the national cyber security strategy. The DITT has finalized the draft of national cyber security strategy (Bhutan) through the meeting which they are planning to publish very soon.

4. MoIC has conducted cyber security incident simulation exercise for high level official in collaboration with ITU in November, 2018.

[2] Draft National cybersecurity Strategy-2020, BtCIRT, DITT, MoIC.

5. Update on the draft national cyber security strategy

The first task force meeting on cybersecurity was held from 18th May to 22nd May, 2020 which was organized by DITT(Department of Information Technology and Telecom) ,MoIC. The first task force meeting on cybersecurity was to formulate the National Cybersecurity Strategy (NCS) of Bhutan. The National cybersecurity strategy was formulated with vision to ensure safe, secure and resilient cyber space for Bhutan. This vision is supported by three guiding principles: 1. Safe and secure cyberspace: 2. protection of fundamental rights: 3. balanced approach (international and regional best practices). Further, the draft NCS of Bhutan have seven strategic goals. The seven strategic goals of National Cybersecurity Strategy of Bhutan to achieve the aforementioned vision are:

1. National Cybersecurity Governance and Coordination for successful management and implementation of NCS
2. Legal Framework, Regulations and Policies to harmonize NCS with national economic Roadmap and other binding legislations.
3. Protection of Critical Information Infrastructure for resilient Bhutan.
4. Cybersecurity Awareness and Capacity Building to improve cybersecurity perceptions and empower every netizens.
5. Strengthen Incident Handling to be prepared and combat cyber-attacks.
6. Strengthen International and Local cooperation for cyber resiliency to harness knowledge and information, and collaboration.
7. Child Online Protection to save youth from being victims of online threats.

5.1 Some of the outcomes of the first task force meeting

The some of the outcomes of the first task force meeting on Cybersecurity are as follows:

- Identified the High- level ICT steering Committee as the Cybersecurity steering committee.
- Broadly identified the members from the agency to be working group members of Cyber security Technical working group, legal framework working group and Child online protection working group.
- Under draft NCS, the members have reflected the requirement/ appointment of Chief Information officer/focal in agencies dealing with Critical information infrastructure.
- The draft NCS requires the development of the National cybersecurity guidelines which shall address the identification, protection, detection, responses, recovery and security of the critical information infrastructure and the essential services of the nation.

- The draft NCS has formulated the action plans on determining risk assessment and management approach, Emergency and Business Continuity Plans (BCP), Development of Baselines for Cybersecurity Requirements, Establishment of Cybersecurity auditing and assurance measures Guidelines and Cybersecurity baseline for CII

- Inserted a provision on Cybersecurity Awareness and Capacity building with the Coordinated Cyber Security Awareness Campaigns and Capacity Building through Cybersecurity Awareness and Capacity Development in Schools, Capacity Development in Legal Enforcement Agencies, Continuous Improvement of Cybersecurity Handling Services, and Cybersecurity in Industry, R&D and Innovation in collaboration with RUB.

- To Strengthen Incident Handling through creation of sectoral computer incident response and teams (CIRTs), Incident Reporting, Response and Early Warning, introducing the Produce of Annual Incident Report and Information Sharing mechanism.

- Highlighted on protection of Critical Information Infrastructures (CIIs) through Identification of CIIs, Cybersecurity Culture within the operators of CIIs, Emergency Preparedness for CII (Incident Reporting for CIIs, and Contingency Plan for CIIs).

- To strengthen International and local cooperation to build cyber resiliency

- To strengthen child online protection through collaboration with stakeholders like BtCIRT, National Commission for Women and Children (NCWC), Ministry of Education (MoE) and ISPs.

6. Recommendations / Way forward

1. The Authority may come up with regulation tools to put in place important issues related to cybersecurity like privacy policy, data protection, and legal interception and baseline for critical information infrastructure for licensees like internet service providers, network service providers and network vendors.

2. To improve the data protection and privacy in the country, the Authority may have to revisit the terms and conditions under ICT facility and Service License, Code of practice on registration of SIM card and Consumer protection code for ICT and Media services.

3. Further, the Authority may mandate the ICT/media service provider to strengthen the protection of personal information of consumers by drawing clear terms of reference or undertaking on data protection especially to the employee dealing with consumer's personal information.

4. The Authority may work closely with BtCIRT team to put in place regulations related to Cybersecurity, Data protection and Online/Offline privacy.

5. To mandate the ISPs and Data Centre to establish the required technical standards and basic security controls and measures in their systems