Global
Cyber Security
Capacity Centre

Building Cyber-security Capacity in the Kingdom of Bhutan

Drafted by: Taylor Roberts

Global Cyber Security Capacity Centre

University of Oxford

Table of Contents

Building Cyber-security Capacity in the Kingdom of Bhutan

The Kingdom of Bhutan is undergoing a major shift with regards to its technological infrastructure. The government is updating its ICT Roadmap by June of this year, exploring an alternate submarine cable connection through Bangladesh and a new payment gateway, and is considering establishing a national data centre, among other initiatives. However, as Bhutan increases national investment into its ICT infrastructure, the risk of inadequate security mechanisms to protect these technologies simultaneously increases as well. It is important to understand the cyber-security capacity in Bhutan in order to invest effectively in both security and new technologies.

Through a Collaboration Agreement with The World Bank, The Global Cyber Security Capacity Centre has facilitated a self-assessment of cybersecurity capacity in the Kingdom of Bhutan. The objective of the self-assessment is to enable Bhutan to determine the areas of capacity the country might strategically invest in to become more cyber secure.

To conduct this type of assessment, the Capacity Centre developed Cyber Capability Maturity Model (CMM), which identifies five distinct dimensions of cyber-security capacity through which a country can self-assess capacity: Dimension 1: policy and strategy; Dimension 2: culture and society; Dimension 3: education, training and skills; Dimension 4: law and regulation; and Dimension 5: standards, organisation, and technology. Within each Dimension, several key factors of cyber-security capacity are identified that must be addressed. The CMM was developed based on extensive research into existing best practice, as well as in broad consultation with international experts across these five Dimensions. The assessment in Bhutan used the CMM to identify what stage of maturity the country is in, so that concrete areas of improvement might be identified. These stages are as follows:

- **Start-up**: At this stage either no capacity exists with respect to some factor, or it is only initially being considered. The start-up level may also reflect a thought or an observation about an issue, upon which no concrete action has yet followed.
- **Formative**: Some aspects of a particular cyber-security factor have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, efforts in this factor can be clearly evidenced.

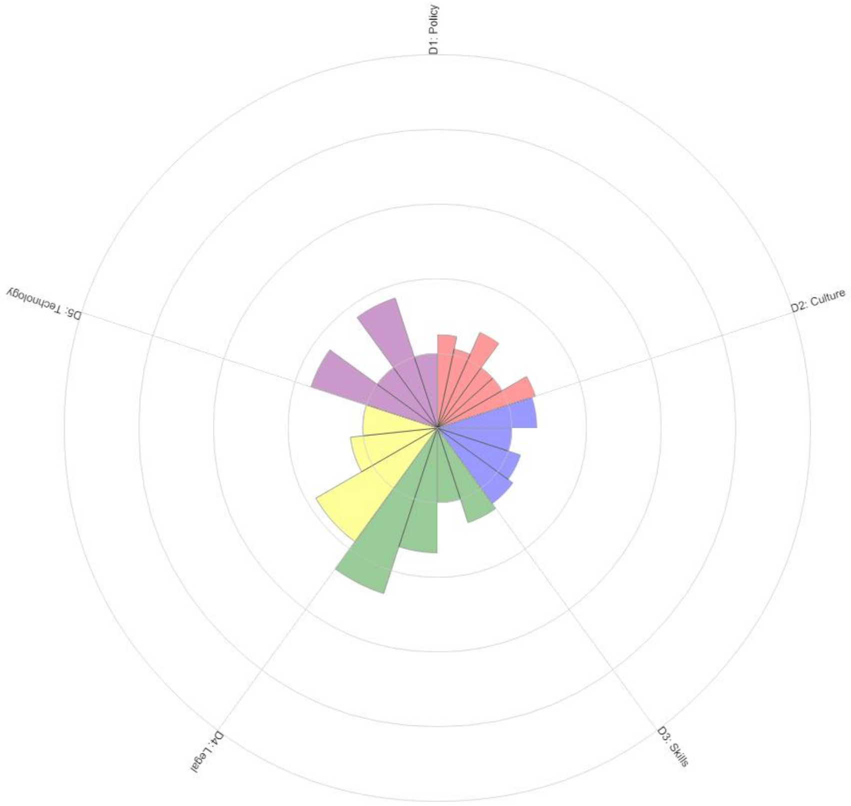
- **Established**: The elements of the factor are in place and working, with defined scope, roles and responsibilities. Consideration of the relative allocation of resources may not yet have been discussed as this stage, nor has trade-off decision-making been made concerning the relative investment priorities in the various elements of the factor.
- **Strategic**: This stage of capacity is concentrated on strategic decision-making. Choices have been made at a national level about which parts of the sub-factor are important, and which are less important for the particular organization/country. These choices posit an intended outcome once implemented, which take into account particular circumstances and other existing national goals. These decisions are reflected in strategic resource allocation.
- **Dynamic**: At the dynamic stage, there are clear mechanisms in place to refine strategy in the light of the prevailing circumstances, such as the technology of the threat environment, global conflict, or significant changes in one area of concern (e.g. Cybercrime or privacy). Dynamic entities have developed methods for evolving and changing strategies in a highly flexible manner. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are key features of this stage.

On March 9-11, 2015, the Capacity Centre, through a partnership with the World Bank, met with representatives from several key stakeholder groups to build a comprehensive picture of cyber-security capacity in Bhutan. These groups include: academia, criminal justice, a number of key ministries, members of the National Council and National Assembly, telecommunications, financial sectors, IT industries, and staff of the host team. During this assessment, each group responded on one or more Dimensions that were considered most relevant to their particular expertise and experience.

This report provides a detailed analysis of the different stages of cyber-security capacity in the Kingdom of Bhutan based on the evidence collected. Each Dimension and its respective factors will be assigned a current state of maturity, based on and accompanied by information gathered from the in-country assessment and supporting external research. The report also issues concrete recommendations for the consideration of Bhutan on how to improve its cyber-security capacity across the various Dimensions. It is up to the country, however, to decide which actions it will chose to pursue. Our intention with this assessment is to provide insights and recommendations that will assist Bhutan continue to build capacity in cyber-security but in more strategic, efficient and effective ways.

Assessment of Cyber-security Maturity

This section provides an in-depth look at several factors of cyber-security capacity within Bhutan, identifies current activities in these areas (if any) and assesses the current status of maturity. The following graphic depicts the raw results for the stages of maturity in each dimension.



The stages of maturity for each factor extend out from the middle as an individual bar, and each dimension is a fifth of the graphic, represented in different colours. For example, the red bar on the far left of the graphic represents the first factor, national cyber-security strategy, for dimension one, national cyber policy and strategy. The average of the different responses comprise the length of the bar, which indicates that this particular factor is just past the *start-up* stage of maturity.

This graphic indicates that all of the raw results of the assessment yield a maturity between *start-up* and *formative*, except for D3-4 (Private and State Owned Companies' Understanding of Cybersecurity). At least one factor of capacity in each dimension are definitively at the start-up level, which indicates that there are several opportunities for Bhutan to take advantage of its growing ICT sector through simultaneous investment in cyber-security capacity. The table below summarises the results from each factor with a brief description and includes existing policies, strategies, laws and other additional information where relevant, followed elaboration in the next section.

Table I: Assessment Results

Capacity Factor	*Stage of Maturity*	*Brief Description*	*Links*
D1-1 National Cyber-Security Strategy	Start-up	No national cyber-security strategy exists. BICMA to include a chapter on security. MoIC and DITT identified as informal leads on cyber-security.	Bhutan Information, Communications and Media Act 2006 – http://www.moic.gov.bt/daden/uploads/2014/04/actenglish2006.pdf Bhutan ICT Roadmap 2011 – Bhutan National eGovernment Master Plan – http://www.moic.gov.bt/daden/uploads/2014/04/Bhutan-eGov-Master-Plan.pdf eGovernment Interoperability Framework - http://www.dit.gov.bt/sites/default/files/page/2013/09/egif_summary_21460.pdf
D1-2 Incident Response	Start-up	BtCIRT still under development	
D1-3 Critical	Start-Up	CNI has not been identified. BICMA	

National Infrastructure		includes critical information infrastructure classification	
D1-4 Crisis Management	Start-up	No exercises conducted; DITT does some crisis management and pen testing	
D1-5 Cyber Defence Consideration	Start-up	Not identified as a priority	
D1-6 Digital Redundancy	Start-up	No data centre yet; TWAN as current backup network	TWAN Project - http://www.dit.gov.bt/content/thimphu-wan-twan
D2-1 Cyber-Security Mind-Set	Start-up	Awareness of cyber-security across society is low, corresponding with the risk profile for cyber	
D2-2 Cyber-Security Awareness	Start-up	No national campaign; some ad-hoc initiatives	Academy of ICT Essentials for Government Leaders - http://www.unapcict.org/academy
D2-3 Confidence and Trust in the Internet	Start-up	Low trust in provision of services, though the deployment of these services is still limited	G2C Services - https://www.citizenservices.gov.bt/
D2-4 Privacy Online	Start-up	Informal discussions have begun about data protection and privacy	
D3-1 National Availability of Cyber Education and Training	Start-up	A module at university and some ad-hoc training exists	
D3-2 National Development of Cyber-Security Education	Start-up	While the Ministry of Education is the lead for cyber security curriculum development, none has been developed at this point	
D3-3 Training and Educational Initiatives within Public and Private Sectors	Start-up	Ad-hoc training through DITT and internally in other organisations	

D3-4 Corporate Governance, Knowledge and Standards	Formative	Several boards have a foundational understanding of the importance of cyber-security, but limited strategic investment	
D4-1 Cyber-security Legal Frameworks	Start-up	BICMA revision to expand cyber-security legislation; penal code includes computer crime	Penal Code (See Chapter 31): http://www.judiciary.gov.bt/html/act/PENAL%20CODE.pdf
D4-2 Legal Investigation	Start-up	Police, prosecutors and judges all have limited capacity to investigate and prosecute crimes with digital evidence or cybercrimes	
D4-3 Responsible Reporting	Start-up	No responsible reporting mechanisms	
D5-1 Adherence to Standards	Start-up	Standards not nationally driven; where implemented, standards derive from parent organisations; risk perception limits investment	
D5-2 Cyber-Security Coordinating Organisations	Start-up	BtCIRT still under development; ad-hoc incident response at the moment	
D5-3 National Infrastructure Resilience	Start-up	Chicken-neck problem with submarine cable connectivity, but currently considering options	
D5-4 Cyber-Security Marketplace	Start-up	No cyber-security marketplace in Bhutan	

Cyber-security Capacity by Factor

Dimension 1: Cyber-security Policy and Strategy

D1-1: National Cyber-Security Strategy – *Start-up*

Currently, there is no overarching strategy through which the government of Bhutan coordinates its approach in cyber-security. Typically, a national cyber security strategy would, among other things, establish a lead agency or ministry responsible for cyber-security in the government, identify roles and responsibilities for all other ministries and public administration entities, set out strategic objectives the government wishes to achieve regarding certain cyber-security issues, and may speak to what resources can be utilised to achieve these objectives.

While Bhutan currently does not have such a document, the country does have other policies that help guide strategic thinking on issues related to cyber-security. The Bhutan Information and Communications and Media Act (BICMA) was first introduced in 2006 under the implementing authority of the Ministry of Information and Communication (MoIC). While the 2006 version of BICMA did not draw particular attention to cyber-security, there is currently a revised draft of BICMA (2015) that contains a chapter dedicated to security and particularly: protection of personal rights and security; blocking, interception or monitoring or decryption of any information; interference with data; power to authorise, monitor and collect traffic data or information; critical information infrastructure; and the Bhutan Computer Incidence Response Team (BtCIRT). There is also a subsequent chapter on data protection. This draft is scheduled for submission to the legislature during the winter session of parliament.

There are a few other ICT related polices that speak to security as well. The ICT Roadmap 2011 pointed out that, "As the Royal Government of Bhutan increases the utilisation of ICT, the need of an ICT Security programme to develop a secure environment" (pg 39). This roadmap is scheduled for revision in June of this year. The Bhutan eGovernment Master Plan also draws attention to the future role of Bhutan CIRT in managing cyber-security incidents. DITT and the MoIC launched the "Information Management & Security Policy" (IMSP) in April, 2009 and, while it has been circulated to all government agencies, it is not yet been fully implemented or followed by the relevant agencies. Finally, the e-Government Interoperability Framework (e-GIF) has a mention of security in relation to the e-GIF technical and information system architecture.

While not officially recognised as the coordinating organisation for cyber security, the Department of Information Technology and Telecommunications (DITT) with the MoIC was widely recognised by the participants as the most appropriate candidate for this responsibility. A representative of the Ministry of Foreign Affairs suggested that, in addition to a central department responsible for cyber-security, each ministry should have its own cyber-security officer so that a point of contact is easily established. Budget for cyber-security, at this point, is not centralised, but it was suggested that DITT also be responsible for the distribution of such budget.

D1-2: Incident Response – *Start-up*

An initiative has been launched in Bhutan to establish a computer incident response team (BtCIRT). This was started in collaboration with the International Telecommunications Union (ITU), and is now funded by the World Bank and in an open procurement for consultancy to set up this CIRT. DITT is responsible for the creation of the CIRT, though it was pointed out that, at this point, incident response is not coordinated between ministries, nor between the public and private sector. Each individual IT department will respond to each incident in isolation of other bodies, without a central registry of incidents. The Royal Bhutan Police was also identified as an authority for dealing with incidents when they occur, but are more responsible for investigation rather than recovery.

However, it is important to point out that several participants asserted that the rate of computer-related crimes in Bhutan is very low, many claiming that there have been no incidents to report. Therefore, a lack of centralised incident response may be in part because the necessity of such a body was not yet a priority.

It should also be pointed out that BtCIRT would be responsible for the coordination of incident response, but would not be the central organisation for coordinating all of cyber-security issues in the country. Its mandate would not be broad enough to cover the political, legislative, financial and other complex elements that would be required in the department coordinating cyber-security nationally. Adding additional directives to BtCIRT might hinder the organisation from efficiently managing cyber-security incident response.

D1-3 Critical National Infrastructure – *Start-up*

Critical national infrastructure in Bhutan has not yet been formally identified. When asked whether there was a list of companies, industries or organisations that are considered vitally important to the country’s infrastructure, most participants claimed that, given the time, they could produce a list that would likely look similar to a list drafted by other participants. This task would be made easier by the fact that most major infrastructure providers are state-owned (Bhutan Power Corporation, Bank of Bhutan, and others). The MoIC, in the draft BICMA act, has been tasked with designating and centralising the management of National Critical ICT and Media infrastructure. While this would not include all critical national infrastructure, this could serve as a foundation for establishing coordination with some of these organisations. Currently, however, there is no public/private partnership between CNI operators in the private sector and the public sector.

A concern was raised by many of the participants about the level of response planning and risk management within organisations that could be considered CNI. Some organisations rely heavily on DITT for consultation on how to protect their networks. Others are limited by budgetary constraints and may not have firewalls in place to protect their data. Finally, while response planning and risk management may be identified as a concern, it is not centrally managed.

D1-4 Crisis Management – *Start-up*

Crisis management in the form of national level exercises and simulations has not yet occurred. However, DITT has assisted in the coordination of some crisis management activities. For example, critical systems within government are backed up daily, and ICT divisions from several other organisations have conducted network resilience testing in coordination with DITT. In discussions with some participants, some raised the concern that, because there has not been a large scale incident to date, that there is not a broad perception for the need of such crisis management preparation. However, as one participant pointed out, the Ministry of Foreign Affairs website was hacked last year, which indicates that there is a need for enhanced crisis management, in the event that a more malicious incident were to occur.

D1-5 Cyber Defence Consideration – *Start-up*

Cyber defence is currently not a priority for Bhutan, as the military presence in the country is not extensive. The Royal Bhutan Army, led by the Royal King of Bhutan, is the major military presence in the country, and works frequently in coordination with the Royal Bhutan Police and the Anti-Corruption Commission. Some participants submitted that this would likely be the mechanism for coordination if cyber defence were to be considered in the future. Other participants believed that the group secretaries for national security at the Cabinet level would be best positioned to coordinate cyber defence. Still other participants claimed that the Ministry of home and cultural affairs is the de-facto lead on National Security

D1-6 Digital Redundancy – *Start-up*

National redundancy planning is still ad-hoc, though there are some initiatives in the planning stages. For example, as previously mentioned, the revisions to the BICM Act intend to include a national data centre so that there is a centralised location for data back-up. Current data back-up is manual and dependent on each organisation or entity. Additionally, all agencies and organisations were meant to operate on two networks: the ISP and Thimphu WAN (TWAN), but several participants were concerned about the resilience of TWAN, asserting that if the ISP were to go down, TWAN would be unable to appropriately meet the needs of the joined organisations.

Dimension 2: Cyber-security Culture and Society

D2-1 Cyber-Security Mind-Set – *Start-up*

The cyber-security mind-set of government, the private sector and civil society are all at the same *start-up* maturity level, with some deviation in certain industries and agencies. The participants in the assessments voiced their concern that government perception of cyber-security is founded on the belief that the cyber-risk profile of Bhutan is very low, nearly non-existent. Therefore, without a greater appreciation of future potential cyber-security risks, industry and academia feel there is not likely to be increased investment in this area. Most participants also felt that, with the growth of Government to Citizen (G2C) and E-commerce services, the government is in a prime position to begin strategic investment in cyber capacity.

Awareness of cyber-security in the private sector is a bit higher in the financial and ICT sectors, where online services are beginning to be offered to their customers, but promotion of cyber-security in the use of these services remains low. There is also a great challenge in raising the cyber-security mind-set of the general population. There have been a few instances where personal information or defaming statements published on social-media sites were successfully prosecuted, but due to a lack of cyber-security awareness, many people remain unaware of the illegality of such actions.

D2-2 Cyber-Security Awareness – *Start-up*

There is currently no national level awareness campaign seeking to raise the cyber-security awareness of the Bhutanese population. There are some ad-hoc initiatives typically coordinated by MoIC. For example, MoIC partnered with the United Nations Asian and Pacific Training Centre for Information and Communication Technology for Development (UN-APCICT/ESCAP) and the Royal Institute of Management to establish the “Academy of ICT Essentials for Government Leaders,” which focuses on providing government employees with foundational skill in ICT and has a module on network security, information security and data protection. Cyber-security, at this point, is not a part of the Academy’s curriculum.

The private sector also provides some ad-hoc awareness raising activities, sometimes in coordination with CISCO, but these do not extend to the national level. DITT is in communication with the Bhutan ICT and Training Association (BICTTA) and Bhutan Chamber of Commerce about the implementation of general ICT standards and, once these talks become more regular, could serve as the foundation for the implementation of a national cyber-security awareness campaign.

D2-3 Confidence and Trust in the Internet – *Start-up*

Trust in online services and the perception of cyber threats by users is limited in part due to low levels of cyber-security awareness. Those who do have a higher understanding and awareness of cyber-security, such as academics, are not as confident in the provision of online services. According to some participants, denial-of-service attacks on DRUKNET, an Internet service provider (ISP), are common and undermine trust in these services.

E-government services are just beginning to be delivered to Bhutanese citizens. The G2C services are in their second year of delivery and offer some public service delivery options, such as citizen details, jobs’ portal, and scholarship services. More sophisticated services are intended to be offered in the future. There were online tax services offered, without online payment mechanisms. However, manual submission of taxes is required who do not have online banking service facilities with Bank of Bhutan. There is a feedback mechanism on this site called “Voice of Customer” that would allow for continuous adaptation and enhancement of online services based on user feedback.

Most E-commerce services used by Bhutanese are sourced in India. According to some stakeholders, the lack of appropriate digital signatures legislation has inhibited the creation of an e-payments gateway necessary for domestic e-commerce in Bhutan. There is a memorandum of understanding between BICTTA and the Bank of Bhutan for the creation of an online banking application. However, there is very limited uptake of this service. This is in part because the login credentials need to be changed upon every time the application is accessed, making it very inconvenient. There is also little perceived trust in the security of the service by some of the participants.

D2-4 Privacy Online – *Start-up*

While informal discussions about online privacy have begun to take shape, there is no formal mechanism or policy that speaks directly to this topic. The revised BICMA is intended to speak to this is some way, but the private sector and civil society was only minimally included in its development, whilst some participants were unaware as to its application. Additionally, the Right to Information Bill was enacted in February, 2015 which speaks to, "aims at reinforcing and empowering the right of a citizen to public information with a view to foster citizen participation in governance, promoting government accountability, combating corruption, supporting fair and competitive business environment and upholding personal dignity." While the RTI Bill speaks to enhanced government transparency, it does not necessarily increase the privacy rights of the general citizenry. There have been some ad-hoc initiatives to raise employee's awareness of their privacy rights in the workplace. For example, Royal Insurance Corporation of Bhutan Ltd (RICBL) has some procedures in place to raise the awareness of its employees of their data protection and privacy policy. However, the perception is that the procedure is not as common in the private sector (RICBL) is state-owned).

Dimension 3: Cyber-security Education, Training and Skills

D3-1 National Availability of Cyber Education and Training – *Start-up*

Cyber security in a formal educational setting in Bhutan has not yet been developed. The RIM offers a diploma in the Information Management Systems which includes a module in Information Securities and Services. Other colleges offer network security and software development courses, as well as a bachelors in computer science. However, it was discussed among some of the participants that most IT professionals in Bhutan did not receive formal education in cyber security within the country.

There has been a bit more uptake of training initiatives in cyber-security. RIM offers Cisco Certified Network Associate (CCNA) security certification. Financial Institutions Training Institute (FITI) has also developed training courses on an ad-hoc basis if there has been an expressed need, but most of these offerings are in IT and ICT rather than cyber-security. Other private sector organisations offer similar ad-hoc training, sometimes in cooperation with an international partner, typically from India or Thailand. Many other cyber-security training initiatives are still idealised but not yet formally implemented. Bhutan Telecom, in cooperation with international organisations, hopes to bring together IT professionals in Bhutan this year in order to provide training that would include cyber-security. FITI discussed the possibility of training being offered to the financial/services sector to include cyber-security. The Royal Institute of Management in cooperation with the International Institute of Computer Science, Bangalore had prepared training for members of the criminal justice system, but did not result in practical training.

D3-2: National Development of Cyber-Security Education – *Start-up*

While the MoIC plays a pivotal role in the implementation of cyber-security, there is currently no mandate for developing cyber-security education within this or other ministries. Most of the stakeholders identified a need for accredited cyber-security curriculum within the university system, but most current curricula focus on IT rather than cyber-security.

D3-3: Training and Educational Initiatives within Public and Private Sectors – *Start-up*

Training initiatives within the public and private sector are still largely focused on IT professionals. DITT has attended training provided by the Korean Information Security Agency (KISA), but sharing information gained at such training remains difficult because of the highly technical nature of the training. Some financial institutions focus its cyber-security training on its IT specialists and therefore knowledge transfer is not prioritised, though some banks will circulate training information through email. Druk Punjab National bank, however, does provide foundational cyber-security training that is then followed by a test to ensure comprehension. In industry however, knowledge transfer in training is limited and usually only takes place over a long period of time.

D3-4 Corporate Governance, Knowledge and Standards – *Formative*

Board-level understanding of cyber-security is relatively advanced; during the assessment we were able to speak with a number of corporate-level board members, who explained that in many cases the board members are well aware of cyber-security risks. Some members of the financial sector have multiple board members who are information security specialists. The BICTTA, in their interactions with corporate leaders, have had the impression that these individuals are highly qualified and have an understanding of the relevance of cyber-security. However, the overall feedback of participants on board-level cyber-security engagement emphasised its reactive nature. Most board-members focus on disaster recovery and less on strategic investment. Most cyber-security decisions remain with the IT staff and CIO who may then inform the rest of the board.

Dimension 4: Legal and Regulatory Frameworks

D4-1 Cyber-Security Legal Frameworks – *Start-up*

There are several different types of legislation that are important to building cyber-security capacity that this assessment observed. One piece of legislation is ICT security legislation. At this point, there is no legislation in Bhutan that focuses on ICT Security specifically. As previously stated, the BICM Act would address cyber-security upon its update, but this is still in the draft stage. The development of BICMA was made in cooperation with most public sector stakeholders, including many financial institutions, utilities and law enforcement, so several stakeholders are aware that this update will contain some ICT security component. However, BICMA does not stipulate specific security standard requirements for organisations, but rather other aspects of cyber-security, listed in D1-1.

Article 7 of the Bhutanese constitution speaks to privacy as a fundamental right of the people, and participants have interpreted that to include online privacy as well as offline. The Bhutanese penal code also speaks to privacy online as well as offline (Chapter 30-31). Finally, the BICMA revisions will seek to ensure the protection of personal rights and security in its chapter on cyber-security. However, there was concern among law enforcement that overabundance of new legislation could complicate investigation, and prefer adding provisions to existing law.

While there is no unique cyber-security or cybercrime legislation, Chapter 31 of the penal code speaks to computer related offences, which include: protection of personal rights and security, grading of unlawful possession of computer materials, computer pornography, and grading of computer pornography. The civil and criminal procedural code, though does speak to the provision of evidence in a courtroom and, does not at this point include a cyber or digital component.

D4-2: Legal Investigation – *Start-up*

In the Royal Bhutan Police, there is one officer responsible for mobile and computer forensics, but the capacity to investigate of cybercrime has not yet been developed. The anti-corruption commission also has a digital forensics expert, as well as a digital forensics lab, but this authority also lacks capacity to investigate cybercrimes. The MoIC is frequently consulted for their technical expertise, though the police has only encountered three or four reports of cybercrime, and these are usually limited to phishing, peer-to-peer crimes, email hacking, and identity theft. This lack of reporting could be due to a low number of victims of cybercrime, or because awareness of cyber threats and potential disclosure mechanisms have not been made clear to the population.

Very few cyber cases have gone through the judicial system in Bhutan. The cases that have been brought to trial have been content related cases (such as defamation on Facebook or pornography), and getting information from service providers has been difficult during these cases. Additionally, there is no mutual legal assistance treaty in place that would aid in the investigation of cross border crimes, which, since most attacks emanate from outside the nation's borders, creates a barrier to proper prosecution of cases. However, as law enforcement participants pointed out, there is a lack of capacity across the judicial system, including law enforcement, prosecutors and judges. It was mentioned that the handling of electronic evidence is an area where training would be of particular value.

D4-3 Responsible Reporting – *Start-up*

At this point, there is no reporting requirements for critical infrastructure or other government organisations. Without an operational CSIRT and limited law enforcement capacity, many participants stated that DITT is the most frequent referral for cyber incidents.

Dimension 5 - Standards, Organisations, and Technologies

D5-1 Adherence to Standards – *Start-up*

The adoption and implementation of cyber-security standards in Bhutan has been mixed. The Information Management and Security Policy for the Royal Government of Bhutan was adopted by the Cabinet and the implementing authority was granted to DITT, but has not had as substantial an impact due to limited resources. The problem of limited resources to meet national or international security standards was echoed by several of the participant in the assessment. Utility organisations and other industries claimed that the perceived risk of cyber threats by their respective leadership has not yet justified substantial investment into security standard adoption. If investment has been made, it is typically in preventative technologies like firewalls, or because a parent company has mandated the adoption of corporate standards or policies, as is the case with several ISPs and financial institutions in Bhutan.

There are some standards in place for the procurement of IT within government, which also extends to the E-GIF, but these standards do not substantially include security. In the financial, telecommunication and private sectors, procurement is primarily dictated by price and function, rather than security standards. In some financial and telecommunication companies, vendors are chosen based on ISO certification, but this is not always the case. This is similar in software development; when vendors are selected to develop, for example, mobile banking applications, they are typically ISO certified. Other organisations will perform penetration testing on their software before deployment. At the government level, however, there is no security component within software development models.

D5-2 Cyber-Security Coordinating Organisations – *Start-up*

In terms of command-and-control and incident response organisations, members of the financial and private sectors, as well as ISP are not aware of any formal coordination mechanism within which to resolve cyber-security issues. All issues are currently dealt with in ad-hoc channels. For example, banks with parent organisations in other countries will report incidents to the authoritative party or, if it is a criminal issue, to the Bhutan Royal Police. ISPs, on the other hand, responded that they would cooperate with the telecommunications regulator before turning to the police. Other organisations, given the lack of formal mechanisms for coordination, will informally turn to the ISPs for assistance in resolving an issue.

D5-3 National Infrastructure Resilience – *Start-up*

The Internet infrastructure in Bhutan is now conducted through two entry points through India, and the backbone is owned by DITT, who is currently considering developing a security policy to enhance the resilience of this backbone. This backbone has limited redundancy, but the central core is not mirrored. Several participants put forward a potential problem with the submarine cables. Specifically, given that both cables enter the country at the same point, if there were to be a problem at that location, then the entire country would lose connectivity. To resolve this issue, DITT is exploring developing a third gateway through Bangladesh. Due to this challenge, Bhutan is highly dependent on its neighbours for its Internet infrastructure resilience.

D5-4 Cyber-Security Marketplace – *Start-up*

All participants in the assessment unanimously said that cyber-security technologies are imported from international vendors. While there is no cybercrime insurance market at this point, several participants indicated interest in evaluating the value of their data in order to make appropriate risk management decisions.

Recommendations

After an analysis of the information gathered through the assessment, the Global Cyber Security Capacity Centre has produced a set of recommendations for consideration by the Bhutanese government that aim to enhance the existing level of cyber-security capacity in the country. These recommendations cover aspects of all five Dimensions of cyber capacity, and are listed in order of Dimension. These recommendations are meant to advise the government of Bhutan on possible courses of action; it is up to the government to decide which course of action it will choose to pursue, if any.

Dimension 1 Capacity Gap – Use BICMA to provide a mandate for DITT to coordinate national cyber strategy

The proposed BICMA has several cyber-security elements to it. As this act has not been passed through parliament at this point, this would be an opportune time to officially designate DITT as the coordinator for cyber-security issues and, in particular, the lead in the development of a national cyber-security strategy. As the coordinator, DITT would need to distinguish itself from BtCIRT, so that it does not run the risk of conflating its policy making mandate with the core function of the CIRT, which is incident response. As DITT has already built relationships with other ministries, it would consult with these ministries to elucidate their roles and responsibilities in cyber-security. Additionally, since BICMA also discusses DITT's role in identifying critical information infrastructure, the strategy development process would need to include these organisations so that the risks posed to these entities are understood and represented.

The reason it is important that an agency has an official mandate to lead in cyber-security is so that cyber-security is not just a component of a larger communications bill, but rather so that cyber-security becomes an important consideration in its own right, which is particularly crucial as ICT investment continues to grow. Cyber-security needs to increase in profile to enhance the effectiveness of technological capacity.

Summary Points:

- **Use BICMA to designate DITT (or other agency) as cyber-security lead**
- **Lead agency begin developing national cyber strategy in coordination with other ministries and critical infrastructure**
- **Ensure role of CIRT as one component of cyber-security, not the sole responsible coordinating organisation of cyber-security**

Dimension 2 Capacity Gap – Support efforts to promote trust in online services

The void in trust in Internet reliability, e-government services, and e-commerce services should be filled, so that increased trust can serve not only as a foundation for the increased use of these services, but also as a platform for future cyber-security awareness raising efforts. ISPs should coordinate with government ministries to share information in a more transparent way and openly resolve issues that they may be having. This way, users will feel that the service providers are proactively responding to and preparing for potential incidents. There will need to be established communication links between the ISP's and the new CIRT, so that incident response is conducted rapidly.

The memorandum of understanding between BICTTA and the Bank of Bhutan for the creation of an online banking application should seek to not only create this platform, but support it in such a way so that its security is not cumbersome on users. This is a very positive relationship that should simultaneous produce effective technological solutions alongside practical security measures.

Finally, the G2C portal is a great tool for the promotion of e-government services. More emphasis on feedback on e-government services will ensure that future services reflect the operating environment in the public, private and civil sectors.

Summary Points:

- **Promote more transparent communication between the government, private sector, and ISP's in incident response**
- **Ensure e-commerce applications implement practical security measures**
- **Encourage e-government services feedback**

Dimension 3 Capacity Gap – create a cyber-security courses in computer science degrees and coordinate regular training programmes

Given the relative novelty of computer science degrees in Bhutan, it would not be prudent to invest an entire discipline uniquely for cyber-security. However, modules in information security or if possible, cyber-security, should be promoted across all universities with computer science degrees. This module needs to be developed in conjunction with ICT companies in the public and private sector, so that the substance of the course reflects real world security needs. Once this module has been tested repeatedly as an elective, including a cyber-security course as a degree requirement for computer science degrees would ensure that at least some foundation of security is embedded in the future IT leaders of the country.

Cyber-security training in Bhutan could be greatly enhanced by the planned initiatives presented by several participants. For example, if Bhutan Telecom does include a cyber-security element in a future training event, it would set a precedent for other organisations to do so as well. This event would need to ensure that IT professionals from all different sectors participate, and may even need to be required for some critical national infrastructure organisations. Finally, the Financial Institutions Training Institute (FITI) could coordinate a training for the various financial sector organisations to address the specific threats posed to this particular sector and establish future channels of communication between these parties.

Summary Points:

- **Enable information or cyber-security courses to be taught in all computer science**

programs, eventually leading to security as a required component for degrees.

- **Implement proposed training programs and ensure security focus**

Dimension 4 Capacity Gap – ensure passage of BICMA, amend the procedural code, and train judicial system

A prime opportunity for enhancing legal capacity in cyber security would be the passage of BICMA with the included cyber-security elements and the addition of the recommendation previously mentioned in Dimension 1. This would establish cyber-security as a core component of information communications moving forward. However, at the moment, the procedural code does not reflect updates to substantive law in this field. The procedural code should be amended to reflect the proper handling of digital evidence and the prosecution of computer-related offenses. The amendment process would need to involve all relevant organisations, especially the judicial system.

In conjunction with the amendments discussed above, it would be very beneficial for the judicial system to receive training on how to appropriately collect, maintain, and process digital evidence, as well as prosecute cases using such evidence. Since there is no dedicated cybercrime unit in the police force, it would be helpful for more than just the digital forensics experts in law enforcement to receive this training. If done in cooperation with DITT and one of the training centres, this enhanced capacity could also bridge coordination gaps with other ministries and organisations.

Summary Points:

- Pass BICMA with security chapter and privacy components
- Amend procedural code to include digital and cyber components
- Build capacity for the judiciary to successfully/efficiently process digital evidence

Dimension 5 Capacity Gap – Start dialogue to move toward security standard implementation for critical infrastructure

Adhering to international standards for cyber-security, such as ISO 27001 and others, can be difficult if the organisations implementing such standards do not value the risk of cyber threats highly enough to warrant necessary investment. Therefore, starting a dialogue among organisations with similar threat landscapes about the necessity of cyber-security investment according to prescribed standards is a good foundation to build on. Critical infrastructure, given their high importance to the security of the country, should be some of the first organisations involved in this dialogue. Securing these systems against intrusion, disruption or subversion would both enhance the security of the nation as a whole, and also provide an evaluation of cyber risk for other industries and organisations to follow.

Summary Points:

- Convene a dialogue among critical infrastructure to discuss implementation of international cyber-security standards
- Ensure BtCIRT is able to effectively manage incident response, including separating its role from the organisation responsible for all cyber-security

Conclusion

The Kingdom of Bhutan is in a very unique position; the government is considering several options for expanding its ICT infrastructure and service provision and, simultaneously acknowledging the importance of cyber-security in order to make effective investments. This grassroots approach to cyber-security, if approached through collaboration with industry and civil society, could serve as a force multiplier for ICT development in the country.

The Global Cyber Security Capacity Centre is funded by the United Kingdom Foreign and

Commonwealth Office and hosted by the Oxford Martin School
Oxford Martin School, University of Oxford,
Old Indian Institute, 34 Broad Street, Oxford
OX1 3BD, United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk