CYBERSECURITY CAPACITY REVIEW

Bangladesh

August 2018

NRD Cyber Security

Global Cyber Security Capacity Centre

OXFORD MARTIN SCHOOL

UNIVERSITY OF OXFORD

TABLE OF CONTENTS

DOCUMENT ADMINISTRATION

Lead researchers: Ioannis Agrafiotis, Akvilė Giniotienė, Carolin Weisser

Reviewed by: Professor William Dutton, Professor Michael Goldsmith, Professor Basie Von Solms

Approved by: Professor Michael Goldsmith

Version	*Date*	*Notes*
1	*28 July*	*1st draft to Tech Board*
2	*2 August*	*2nd draft to BCC*
3	*14 August*	*Final draft to BCC*

LIST OF ABBREVIATIONS

ASEAN	Association of Southeast Asian Nations
BCC	Bangladesh Computer Council
BGD e-GOV CIRT	Bangladesh e-Government Computer Incident Response Team
BTRC	Bangladesh Telecommunication Regulatory Commission
CEO	Chief Executive Officer
CERT	Computer Emergency Response Team
CI	Critical Infrastructure
CIO	Chief Information Officer
CIRT	Computer Incident Response Team
CISO	Chief Information Security Officer
CMM	Cybersecurity Capacity Maturity Model for Nations
CSIRT	Computer Security Incident Response Team
GCHQ	Government Communications Headquarters
GCSCC	Global Cyber Security Capacity Centre
GOBISM	Government of Bangladesh Information Security Manual
ICTs	Information Communication Technologies
IDS	Intrusion Detection Systems
IoT	Internet of Things
ISPs	Internet Service Providers
ITU	International Telecommunications Union
MPTIT	Ministry of Ministry of Posts, Telecommunications and Information Technology
NCS	National Cybersecurity Strategy
NGO	Non-Governmental Organisation
NRD CS	NRD Cyber Security
PIN	Personal identification number
SMEs	Small and medium enterprises
SOC	Security Operations Center
WEF	World Economic Forum

EXECUTIVE SUMMARY

In collaboration with NRD Cyber Security (NRD CS), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') undertook a review of the maturity of cybersecurity capacity in Bangladesh at the invitation of the Bangladesh Computer Council (BCC). The objective of this review was to enable Bangladesh to gain an understanding of its cybersecurity capacity in order to strategically prioritise investment in cybersecurity.

Over the period 2-4 July 2018, the following stakeholders participated in roundtable consultations: academia, criminal justice, law enforcement, information technology officers and representatives from public sector entities, critical infrastructure owners, policy makers, information technology officers from the government and the private sector (including financial institutions), telecommunications companies and the banking sector. Remote follow-up interviews were conducted with representatives from civil society and international partners.

The consultations took place using the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five *dimensions* of cybersecurity capacity:

- *Cybersecurity Policy and Strategy*
- *Cyber Culture and Society*
- *Cybersecurity Education, Training and Skills*
- *Legal and Regulatory Frameworks*
- *Standards, Organisations, and Technologies*

Each dimension comprises *factors* which describe what it means to possess cybersecurity capacity. Factors consist of *aspects* and for each aspect there are *indicators*, which describe steps and actions that, once observed, define the state of maturity of that aspect. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to adapt dynamically or to change in response to environmental considerations. For more details on the definitions, please consult the CMM document.[1]

Figure 1 below provides an overall representation of the cybersecurity capacity in Bangladesh and illustrates the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' is placed at the perimeter.

1 Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition (assessed 25 February 2018)

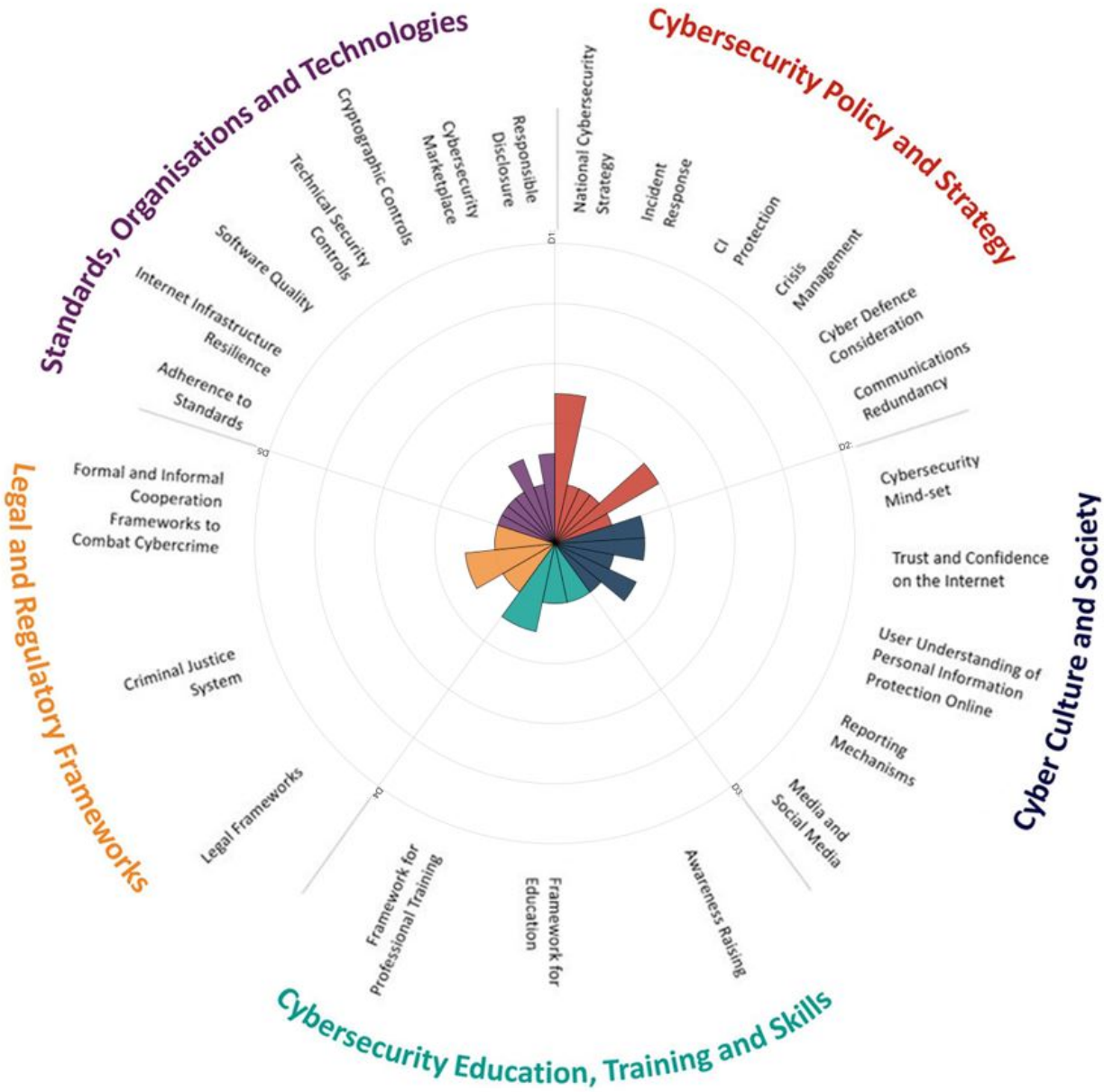

Figure 1: Overall representation of the cybersecurity capacity in Bangladesh

Cybersecurity Policy and Strategy

The People's Republic of Bangladesh published a National Cybersecurity Strategy (NCS) in 2014[2] including four strategic areas and a total of 11 actions focusing on public awareness raising, cybercrime mitigation, establishment of incident response capability, protection of critical infrastructure, national cybersecurity framework development, securing government infrastructure, cybersecurity skills and training development, and establishment of public-private partnership.

[2] http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf

Responsibility for the design, implementation, monitoring and revision of the strategy was not formally assigned, but the process had been and continues to be led by the Ministry of Ministry of Posts, Telecommunications and Information Technology (MPTIT). Even though a part of CMM review participants were not aware of the existence of National Cybersecurity Strategy of Bangladesh, they acknowledged that cybersecurity strategy and policy making process rests with the Ministry. The National Cybersecurity Strategy of Bangladesh is under review at the moment.

Currently, there is no national computer-related incident response organisation and the Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)[30] which is the leading authority for handling incidents within the public sector. In the private sector, only a very limited number of organisations which operate in the financial and telecommunications sectors has established security operations centers (SOCs).

The concept of cybersecurity in critical infrastructure (CI) in Bangladesh is still in its infancy. The NCS recognises CI but there no official procedures in place to identify which infrastructures are key and should be considered as part of CI. Coordination within CI owners and between CI owners and the government, in relation to cybersecurity threat and vulnerability disclosure, is absent.

We were not able to obtain a clear picture regarding crisis management, cyber defence and communications redundancy during the review.

Cyber Culture and Society

The interviews indicated that Internet users in Bangladesh too often "blindly" trust ICT and Internet services and do not have the skills to critically assess what they receive and see online and to appropriately gauge the security of the applications they use. It did not become clear from the consultations to which extent the government offers e-services. A somewhat different picture was revealed with respect to e-commerce services, which have become very popular in the country over the last years, making it to one of the booming sectors in Bangladesh (including those of international companies such as Uber). Participants acknowledged that trust levels of e-commerce services have increased because of the quality of the services experienced since they have been offered. Despite the proliferation of e-commerce services, the suppliers have not yet recognised the need for the application of security measures.

People in Bangladesh, in both the public and private sectors, have little or no understanding about how personal information is handled online and the issues surrounding the protection of personal information.

The consultations revealed that there are two main channels from the public sector for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents. One is the National CSIRT and the police. Victims can go to police or to a special branch to launch a complaint or contact the cyber call desk via phone, email or online portals. Another participant mentioned is going to local councils and unions, as well as NGOs and human rights organisations.

Cybersecurity reports about user problems on traditional and social media in Bangladesh are only ad-hoc. More often journalists cover bigger events such as international cyber attacks

and larger cybercrime cases such as the National Bank heist, but these reports are also limited by the lack of sophisticated technical cybersecurity knowledge on the part of those who produce those reports. Social media was seen by many participants as a risk for the nation as platforms such as Facebook and Instagram are perceived to have been misused often to share false information. However, participants also highlighted the role that the media could play in raising public awareness of the risks in cyberspace and e.g. to inform people about security and training opportunities.

Cybersecurity Education, Training and Skills

Awareness raising programmes are available but they are very ad-hoc and not specified for different target groups. The BGD e-GOV CIRT as part of BCC engages in the design of awareness campaigns and has adapted some of the Stop.Think.Connect materials and publishes material on its website but it was not clear from the consultations if they are targeted to specific target groups and if any metrics were applied. Participants also mentioned there were a number of initiatives supported by international partners but which have been discontinued.

The government has not yet realised the action item of the NCS and a coordinated National Cybersecurity Education Framework is not yet in place. Despite the government taken different initiatives to introduce cybersecurity qualification programmes and to increase the number of cybersecurity experts both are still very limited.

The need for training professionals in cybersecurity has been documented in the current NCS. However, there was also no evidence from the consultations if and to which extent initiatives were implemented. In the private sector, cybersecurity training is mandatory in some industries but for instance in the finance sector and as universities and training institutions the execution of policies is different between sectors. Participants emphasized the need to develop a national framework and procedures to implement cybersecurity frameworks across organisations regarding skills development.

Legal and Regulatory Frameworks

In Bangladesh, there is no sufficient legislative framework for ICT security. Partial legislation exists that address some aspects of cybercrime. Some parts of the National Cyber Security Strategy have been enacted but it does not provide actionable directives to different cybersecurity stakeholders.

The National Police has a cybercrime division. According to participants about 200 law enforcement officers (both female and male) based there and across the country have received training on cybercrime and digital evidence. Training is received on a regular basis from international partners and Training-of-Trainers initiatives aim to ensure knowledge exchange.

There is no effective training for prosecutors and judges and their expertise to deal with cybersecurity incidents is insufficient and according to participants there is currently only one judge who is able to handle cybercrime cases, according to participants.

Standards, Organisations, and Technologies

Bangladesh has established the Bangladesh Standards and Testing Institution[3] with a specific branch for information and technology sector standardisation where organisations, both private and public, can refer to for accreditation to ICT standards.

BCC in collaboration with NRD CS developed and published an information security guidance based on ISO 27001 and New Zealand information security manual[4], however, the public sector is segmented and each ministry decides on which security policies should be followed and there is no mechanism for audit control to identify the level of compliance.

However, several exceptions exist. Financial institutions are required to comply to the Guidelines for ICT security for Banks and Non-Bank Financial Institutions[5] and Integrated Risk Management Guidelines for Financial Institutions[6] issued by the Bangladesh Bank and major telecommunication providers has been operating based on ISO27001 principles since 2013. The main reason for the absence of standards across all ministries, as acknowledged during the sessions, is the limited budget dedicated to IT and the lack of cybersecurity experts.

Review participants did not raise any significant concerns regarding the resilience of internet infrastructure in Bangladesh. Telecommunication companies have a fully redundant infrastructure for the core network, the radio and the internet gateways. Internet penetration

An inventory of software used in public and in private sector, as well as a catalogue of secure software is currently absent in Bangladesh. The quality and performance of the currently used software, especially in the public sector, is problematic due to limited instances where pirated versions of Microsoft products are being used. Consequently, no policies can be followed on updating software products or monitor the functionality of applications. The information security manual designed by NRD CS, if adopted in full will provide the necessary policies for software quality.

The adoption of technical security controls in Bangladesh varies significantly across sectors and organisations. Participants suggested that the adoption and implementation of controls in government bodies is insufficient and inconsistently promoted, due to financial restrictions and limitations in human resources and lack of organisational structure. Security controls in most ministries are limited to password protection and in some cases the use of antivirus services, while there are no mechanisms in place to monitor compliance to security policies. In stark contrast, the recently deployed National Data Centre supervised by e-GOV CIRT monitors traffic for vulnerabilities, applies patching to outdated software and authenticates users before accessing the network.

The adoption and implementation of security controls is more widespread in the private sector. Telecommunication companies appear to a have more sophisticated approach to cybersecurity with the adoption of a wide range of technical controls and the implementation of regular audits.

[3] http://www.bsti.gov.bd
[4] https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/
[5] https://www.bb.org.bd/openpdf.php
[6] https://www.bb.org.bd/openpdf.php

Financial institutions only started to adopt controls tailored to their networks. Network-segmentation controls and monitoring tools are evident in this sector as well as the use of Intrusion Detection Systems (IDS) and elementary inventories of the hardware and software used in their networks. There are also some CI stakeholders that lack the level of sophistication that telecommunication companies have and rely solely on a foreign vendor for their security.

INTRODUCTION

At the invitation of Bangladesh Computer Council (BCC) and in collaboration with NRD Cyber Security (NRD CS), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity in Bangladesh. The objective of this review was to enable the country to determine areas of capacity in which the government might strategically invest in, in order to improve their national cybersecurity posture.

Over the period 2-4 July 2018, stakeholders from the following sectors participated in a three-day consultation process:

- Public sector entities
  - Bangladesh Computer Council (BCC)
  - Bangladesh Parliament Secretariat
  - Bangladesh Telecommunication Regulatory Commission (BRTC)
  - Banks and Financial Institutions Division
  - Election Commission Bangladesh
  - Ministry of Agriculture
  - Ministry of Chittagong Hill Tracts Affairs
  - Ministry of Culture Affairs
  - Ministry of Defence
  - Ministry of Disaster Management and Relief
  - Ministry of Expatriates' Welfare and Overseas Employment
  - Ministry of Finance
  - Ministry of Foreign Affairs
  - Ministry of Industries
  - Ministry of Law, Justice and Parliamentary Affairs
  - Ministry of Posts, Telecommunications and Information Technology
  - Ministry of Planning
  - Ministry of Religious Affairs
  - Ministry of Shipping
  - Ministry of Social Affairs
  - Ministry of Textiles and Jute
  - Ministry of Women and Children Affairs
  - Road Transport and Highways Division
- Private sector
  - Cisco Technology Bangladesh Limited
  - eGeneration Limited
  - Grameenphone
  - Huawei Technologies Bangladesh Limited
  - Information Systems Security Association of Bangladesh
  - Link 3 Technologies
  - Microsoft Bangladesh Limited
  - Robi Axiata
  - Spectrum Engineering Consortium Limited

  - Tech Valley Networks Limited
  - Thakral Information Systems Pvt. Ltd

- Criminal justice sector
  - Bangladesh Army
  - Bangladesh Police
  - Directorate General of Forces Intelligence (DGFI)

- Finance sector
  - Bangladesh Bank
  - Janata Bank
  - Rupali Bank

- Critical infrastructure owners
  - Bangladesh Power Development Board (BPDB)
  - Central Bank
  - Titas Gas

- Academia
  - ISACA Bangladesh
  - University Grants Commission (UGC)

- International community

DIMENSIONS OF CYBERSECURITY CAPACITY

Consultations were premised on the GCSCC Cybersecurity Capacity Maturity Model for Nations (CMM)[7] which is composed of five distinct *dimensions* of cybersecurity capacity.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. The table below shows the five dimensions with the five dimensions together with the factors of which they are comprised:

DIMENSIONS	FACTORS
Dimension 1 Cybersecurity Policy and Strategy	D1.1 National Cybersecurity Strategy D1.2 Incident Response D1.3 Critical Infrastructure (CI) Protection D1.4 Crisis Management D1.5 Cyber Defence D1.6 Communications Redundancy
Dimension 2 Cyber Culture and Society	D2.1 Cybersecurity Mind-set D2.2 Trust and Confidence on the Internet D2.3 User Understanding of Personal Information Protection Online D2.4 Reporting Mechanisms D2.5 Media and Social Media
Dimension 3 Cybersecurity Education, Training and Skills	D3.1 Awareness Raising D3.2 Framework for Education D3.3 Framework for Professional Training
Dimension 4 Legal and Regulatory Frameworks	D4.1 Legal Frameworks D4.2 Criminal Justice System D4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 Standards, Organisations, and Technologies	D5.1 Adherence to Standards D5.2 Internet Infrastructure Resilience D5.3 Software Quality D5.4 Technical Security Controls D5.5 Cryptographic Controls D5.6 Cybersecurity Marketplace D5.7 Responsible Disclosure

7 See Cybersecurity Capacity Maturity Model for Nations (CMM), Revised Edition, available at https://www.sbs.ox.ac.uk/cybersecurity-capacity/content/cmm-revised-edition.

STAGES OF CYBERSECURITY CAPACITY MATURITY

Each dimension comprises factors which describe what it means to possess cybersecurity capacity. Factors consist of aspects and for each aspect there are indicators, which describe steps and actions that once observed define which state of maturity this specific element of aspect is. There are five stages of maturity, ranging from the *start-up* stage to the *dynamic* stage. The start-up stage implies an ad-hoc approach to capacity, whereas the dynamic stage represents a strategic approach and the ability to dynamically adapt or change against environmental considerations. The five stages are defined as follows:

- **Start-up:** at this stage either no cybersecurity maturity exists, or it is very embryonic in nature. There might be initial discussions about cybersecurity capacity building, but no concrete actions have been taken. There is an absence of observable evidence of cybersecurity capacity at this stage.
- **Formative:** some aspects have begun to grow and be formulated, but may be ad-hoc, disorganised, poorly defined – or simply new However, evidence of this aspect can be clearly demonstrated.
- **Established:** the indicators of the aspect are in place, and functioning. However, there is not well thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the relative investment in this aspect. But the aspect is functional and defined.
- **Strategic:** at this stage, choices have been made about which indicators of the aspect are important, and which are less important for the particular organisation or state. The strategic stage reflects the fact that these choices have been made, conditional upon the state's or organisation's particular circumstances.
- **Dynamic:** At this stage, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances such as the technological sophistication of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations have developed methods for changing strategies in-stride. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are features of this stage.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out above, this report presents results of the cybersecurity capacity review of Bangladesh and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

The assignment of maturity stages is based upon the evidence collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and the professional judgement of GCSCC research staff. Using the GCSCC methodology as set out below, this report presents results of the cybersecurity capacity review of Bangladesh and

concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

METHODOLOGY - MEASURING MATURITY

During the country review specific dimensions are discussed with the relevant group of stakeholders. Each stakeholder cluster is expected to respond to one or two dimensions of the CMM, depending on their expertise. For example, Academia, Civil Society and Internet Governance groups would all be invited to discuss both Dimension 2 and Dimension 3 of the CMM.

In order to determine the level of maturity, each aspect has a set of indicators corresponding to all five stages of maturity. In order for the stakeholders to provide evidence on how many indicators have been implemented by a nation and to determine the maturity level of every aspect of the model, a consensus method is used to drive the discussions within sessions. During focus groups, researchers use semi-structured questions to guide discussions around indicators. During these discussions stakeholders should be able to provide or indicate evidence regarding the implementation of indicators, so that subjective responses are minimised. If evidence cannot be provided for all of the indicators at one stage, then that nation has not yet reached that stage of maturity.

The CMM uses a focus group methodology since it offers a richer set of data compared to other qualitative approaches.[8] Like interviews, focus groups are an interactive methodology with the advantage that during the process of collecting data and information diverse viewpoints and conceptions can emerge. It is a fundamental part of the method that rather than posing questions to every interviewee, the researcher(s) should facilitate a discussion between the participants, encouraging them to adopt, defend or criticise different perspectives.[9] It is this interaction and tension that offers advantage over other methodologies, making it possible for a level of consensus to be reached among participants and for a better understanding of cybersecurity practices and capacities to be obtained.[10]

With the prior consent of participants, all sessions are recorded and transcribed. Content analysis – a systematic research methodology used to analyse qualitative data – is applied to

8 Relevant publications:
Williams, M. (2003).Making sense of social research. London: Sage Publications Ltd. doi: 10.4135/9781849209434
Knodel, J. (1993). The design and analysis of focus group studies: a practical approach. In Morgan, D. L. SAGE Focus Editions: Successful focus groups: Advancing the state of the art (pp. 35-50). Thousand Oaks, CA: SAGE Publications Ltd. doi: 10.4135/9781483349008
Krueger, R.A. and Casey, M.A. (2009). Focus groups: A practical guide for applied research. London: Sage Publications LTD.
9 Relevant publications: J. Kitzinger. 'The methodology of focus groups: the importance of interaction between research participants.' Sociology of Health & Illness, 16(1):103–121, 1994.
J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.
E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, pages 1–13, 1982.
10 J. Kitzinger. 'Qualitative research: introducing focus groups'. British Medical Journal, 311(7000):299– 302, 1995.

the data generated by focus groups.[11] The purpose of content analysis is to design "replicable and valid inferences from texts to the context of their use".[12]

There are three approaches to content analysis. The first is the inductive approach which is based on "open coding", meaning that the categories or themes are freely created by the researcher. In open coding, headings and notes are written in the transcripts while reading them and different categories are created to include similar notes that capture the same aspect of the phenomenon under study.[13] The process is repeated and the notes and headings are read again. The next step is to classify the categories into groups. The aim is to merge possible categories that share the same meaning.[14] Dey explains that this process categorises data as "belonging together".[15]

The second approach is deductive content analysis which requires the prior existence of a theory to underpin the classification process. This approach is more structured than the inductive method and the initial coding is shaped by the key features and variables of the theoretical framework.[4]

In the process of coding, excerpts are ascribed to categories and the findings are dictated by the theory or by prior research. However, there could be novel categories that may contradict or enrich a specific theory. Therefore, if deductive approaches are followed strictly these novel categories that offer a refined perspective may be neglected. This is the reason why the GCSCC research team opts for a third approach which is a more blended one in the analysis of the data, which is a mixture of deductive and inductive approaches.

After conducting a country review, the data collected during consultations with stakeholders and the notes taken during the sessions are used to define the stages of maturity for each factor of the CMM. The GCSCC adopts a blended approach to analyse focus group data and use the indicators of the CMM as our criteria for a deductive analysis. Excerpts that do not fit into themes are further analysed to identify additional issues that participants might have raised or to tailor our recommendations.

In several cases while drafting a report, desk research is necessary in order to validate and verify the results. For example, stakeholders might not be always aware of recent developments in their country, such as whether the country has signed a convention on personal data protection. The sources that can provide further information can be the official government or ministry websites, annual reports of international organisations, university websites, etc.

11 K. Krippendorff. Content analysis: An introduction to its methodology. Sage Publications, Inc, 2004. H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.
K.A. Neuendorf. The content analysis guidebook. Sage Publications, Inc, 2002.
12 E.F. Fern. 'The use of focus groups for idea generation: the effects of group size, acquaintanceship, and moderator on response quantity and quality.' Journal of Marketing Research, Vol. 19, No. 1, Volume and Number? pages 1–13, 1982.
13 S. Elo and H. Kyng¨as. 'The qualitative content analysis process.' Journal of Advanced Nursing, 62(1):107–115, 2008.
H.F. Hsieh and S.E. Shannon. 'Three approaches to qualitative content analysis.' Qualitative Health Research, 15(9):1277–1288, 2005.
14 P.D. Barbara Downe-Wamboldt RN. 'Content analysis: method, applications, and issues.' Health Care for Women International, 13(3):313–321, 1992.
15 I. Dey. Qualitative data analysis: A user-friendly guide for social scientists. London: Routledge, 1993.

For each dimension, recommendations are provided for the next steps to be taken for the country to enhance its capacity. If a country's capacity for a certain aspect is at a formative stage of maturity then by looking at the CMM the indicators which will help the country move to the next stage can be easily identified. Recommendations might also arise from discussions with and between stakeholders.

Using the GCSCC CMM methodology, this report presents results of the cybersecurity capacity review of Bangladesh and concludes with recommendations as to the next steps that might be considered to improve cybersecurity capacity in the country.

CYBERSECURITY CONTEXT IN BANGLADESH

Bangladesh is home to over 87 million internet subscribers in 2018[16], significantly up from the 5.6 million users in the 2010 estimates from the International Telecommunications Union (ITU).[17] However, given the significant size of the nation's population, this only accounts for an Internet user rate of 18%. Such internet usage is predominantly made up of mobile-broadband subscribers with the 2017 ITU International Development Index detailing 17.79 mobile-broadband subscriptions per 100 inhabitants compared to 3.77 for fixed (wired)-broadband.[18] In terms of Social Media usage, Bangladesh has 25-30 million active Facebook[19] users, composed of 90% of 18-34 year olds, with female users accounting for only 25% of the total.

According to the World Economic Forum (WEF) 2016 report of the Global Information Technology[20]. Bangladesh is ranked 112 out of 139 nations surveyed on their Network Readiness Index, scoring values consistent with other lower-middle income group nations. Consistent with ICT indicators, the overall Bangladesh economy scores relatively low on the WEF 2017-18 Global Competitiveness Index[21], with inadequate supply of infrastructure, government inefficiency, and under skilled workforce identified as key factors to address in order to drive further improvements. However, since 2015 Bangladesh has been addressing some of the factors and improved its national competitiveness position from 107th to 99th place in the in the GCI rankings.

Despite this level performance, progress has been made with the Bangladesh government working with the World Bank to improve such conditions through the Integrated E-Government Project[22] in which ICT is designed to play an important role in driving economic growth and improving interactions between government, citizens, and industry. This project is consistent with other efforts by the government to prioritise the ICT sector to drive growth as detailed in its Digital Bangladesh[23] agenda which has been well received globally,

16 http://www.btrc.gov.bd/content/internet-subscribers-bangladesh-june-2018
17 ITU Internet users by region and country 2010-16 https://www.itu.int/en/ITU-D/Statistics/Pages/stat/treemap.aspx
18 ITU ICT Development Index 2017 https://www.itu.int/net4/ITU-D/idi/2017/index.html#idi2017economycard-tab&BGD
19 Facebook Audience Insights https://www.facebook.com/ads/audience-insights
20 World Economic Forum – The Global Information Technology Report 2016 http://www3.weforum.org/docs/GITR2016/WEF_GITR_Full_Report.pdf
21 World Economic Forum – The Global Competitiveness Report 2017-18 https://www.weforum.org/reports/the-global-competitiveness-report-2017-2018
22 World Bank – Integrated Digital Government Project http://projects.worldbank.org/P161086?lang=en
23 Centre for Research and Information - Bangladesh Digital Revolution http://cri.org.bd/publication/digital-revolution/Bangladesh%27s%20Digital%20Revolution.pdf

particularly for its emphasis on ICT for Inclusive Growth. Underpinning this focus on ICT is a National Cybersecurity Strategy[24] that outlines a vision for cybersecurity in the nation to 2021.

Despite such positive economic related outcomes driven by the ICT sector, the government has received international criticism related to freedom of the Internet, with the 2017 Human Rights Report[25] from the US State Department raising issues over governmental censorship, restrictions on access, and limiting press freedom.

Bangladesh has been active in engaging in regional cooperation and is a member of the South Asian Association for Regional Cooperation[26] and has also either signed or is in negotiation in six additional free trade agreements.[27]

24 Bangladesh National Cybersecurity Strategy http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf
25 US State Department – Bangladesh 2017 Human rights Report
https://www.state.gov/documents/organization/277521.pdf
26 South Asian Association for Regional Cooperation http://saarc-sec.org/about-saarc
27 Asian Development Bank - Asian Regional Integration Center https://aric.adb.org/fta-country

REVIEW REPORT

OVERVIEW

In this section, we provide an overall representation of the cybersecurity capacity in Bangladesh. Figure 2 below presents the maturity estimates in each dimension. Each dimension represents one fifth of the graphic, with the five stages of maturity for each factor extending outwards from the centre of the graphic; 'start-up' is closest to the centre of the graphic and 'dynamic' at the perimeter.

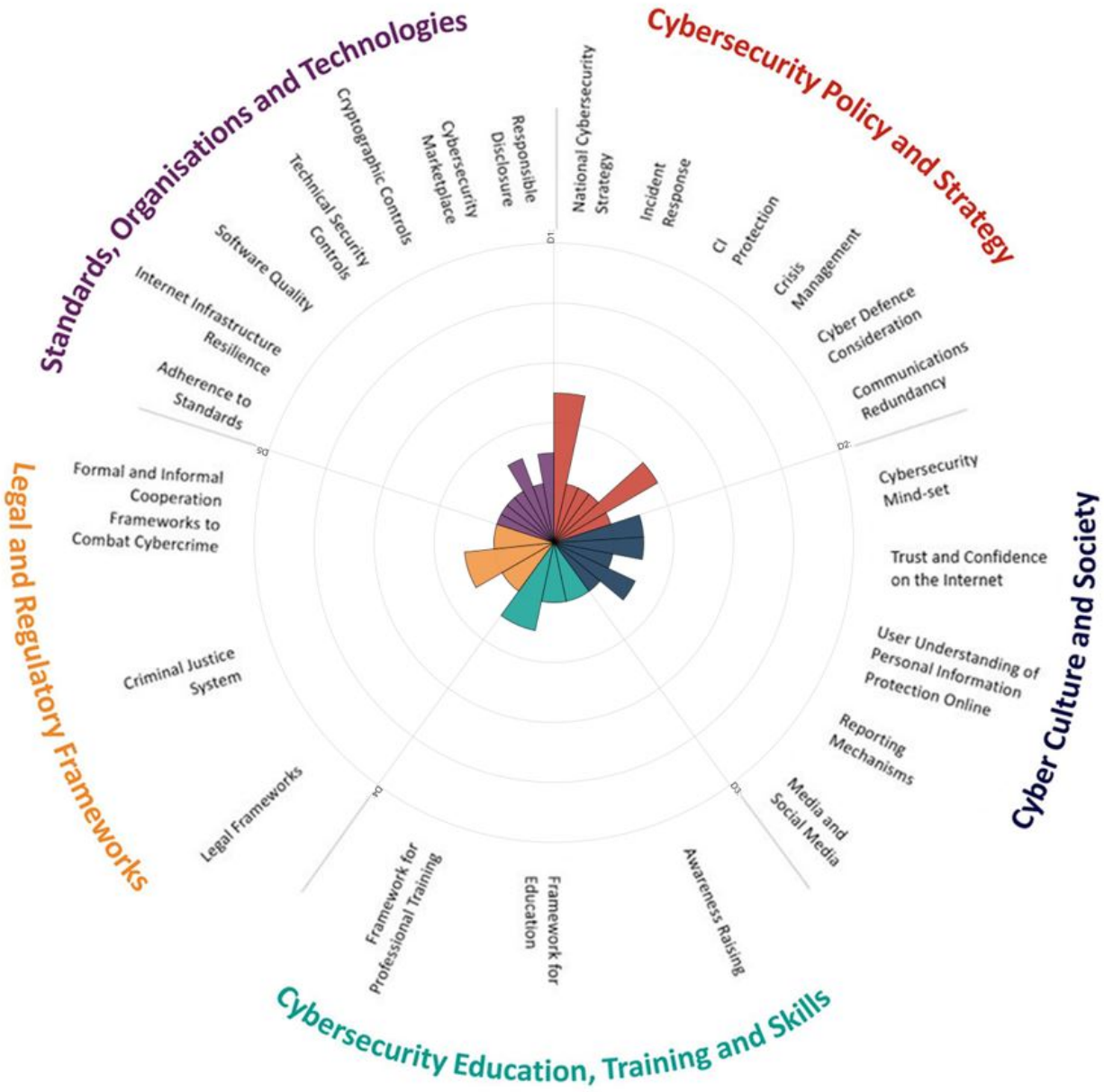

Figure 2: Overall representation of the cybersecurity capacity in Bangladesh

DIMENSION 1
CYBERSECURITY STRATEGY AND POLICY

The factors in Dimension 1 gauge Bangladesh's capacity to develop and deliver cybersecurity policy and strategy and to enhance cybersecurity resilience through improvements in incident response, crisis management, redundancy, and critical infrastructure protection capacity. The Cybersecurity policy and strategy dimension also includes considerations for early warning, deterrence, defence and recovery. This dimension considers effective policy in advancing national cyber-defence and resilience capacity, while facilitating the effective access to cyberspace increasingly vital for government, international business and society in general.

D 1.1 NATIONAL CYBERSECURITY STRATEGY

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government, because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key government and non-governmental cybersecurity actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities

Stage: Formative - Established

The People's Republic of Bangladesh published a National Cybersecurity Strategy (NCS) in 2014[28]. The central goal of the strategy vision of the strategy or the vision was "working collaboratively home and abroad, to manage all major cyber risks that affect us directly irrespective of their origin and type, thereby creating a safe, secure and resilient critical national information infrastructure for our economy and society". To achieve this goal, the strategy identified four strategic areas– the development of a comprehensive set of national cybercrime legislation that is regionally and globally applicable and harmonized, the implementation of measures to reduce vulnerabilities in software products through the deployment of accreditation schemes, protocols and standards, the definition of strategies for the capacity building mechanisms to raise awareness, transfer know-how and boost cybersecurity on the national policy agenda, and the development of a unified multi-stakeholder strategy for international co-operation in dealing with cyber threats. The strategy further translated these strategic areas into a number of actions within three strategic

[28] http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf

priorities inter alia legal measures, technical and procedural measures, and organizational structures.

A total of 11 actions were detailed in the National Cybersecurity Strategy and they included public awareness raising, cybercrime mitigation, establishment of incident response capability, protection of critical infrastructure, national cybersecurity framework development, securing government infrastructure, cybersecurity skills and training development, and establishment of public-private partnership.

All these actions were linked to national risks, priorities and objectives, as well as business development. National risks and threats were listed in the strategy and included espionage directed towards obtaining political intelligence, stealing intellectual property of commercial enterprises, unauthorized modification, distributed denial of services and disruption during patching of smart meters, phishing to facilitate credit card fraud, malware attacks.

Responsibility for the design, implementation, monitoring and revision of the strategy was not formally assigned, but the process had been and continues to be led by the Ministry of Posts, Telecommunications and Information Technology (MPTIT). Even though a part of CMM review participants were not aware of the existence of National Cybersecurity Strategy of Bangladesh, they acknowledged that cybersecurity strategy and policy making process rests with the Ministry.

Most of cybersecurity strategy actions are being financed through the Leveraging ICT for Growth, Employment and Governance project, implemented by the MPTIT. Significant progress has been observed in certain aspects of the implementation of the strategy, mostly those that fall within the remit of responsibility of the MPTIT. A draft Digital Security Act has been prepared to define Government's legal authority in cybersecurity and has been sent for Parliament's approval, national cybersecurity framework has been developed to define mandatory security standards. A government CERT has been established and provides services to its constituencies, assistance to financial sector and international partners, and a national critical information infrastructure was designated and cybersecurity risk management framework for critical information infrastructures is under development, cybersecurity laboratory was established, all government e-services are migrating to National Data Center which observes rigid security protocols, Software certification lab has also reached required level of maturity to test and certify all software before its deployment to government systems, law enforcement have established cybercrime units with digital forensic capabilities. Other implementation aspects of National cybersecurity strategy are lagging as they fall within the responsibility of other government ministries or agencies and the MPTIT has no mandate to monitor their progress.

An area of concern for all CMM review participants that hinder progress in cybersecurity initiatives is lack of awareness of the importance of cybersecurity at the management level, where cybersecurity is considered something technical, therefore resources are not provided for training and educating staff. There was a general agreement that Ministry of ICT is making a good progress in building national cybersecurity capacity and should continue to lead such efforts.

National Cybersecurity Strategy of Bangladesh is under review at the moment, the process initiated and led by the MPTIT. There are plans to run a multi-stakeholder consultation process and adjust and streamline the strategy with a focus on four main areas:

- Strengthening resilience of Critical Information Infrastructures
- Mobilizing business and community to make cyber space safer by countering cyber threats, combating cybercrime and protecting personal data
- Developing a vibrant cybersecurity ecosystem comprising of a skilled workforce, technologically advanced companies and strong research collaboration
- Stepping up efforts to forge strong international partnerships

D 1.2 INCIDENT RESPONSE

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

The "Digital Bangladesh"[29] project, as presented in 2014, reflects government's "Vision 2021" for a socio-economic transformation through the development of information communication technologies (ICTs). The project is an integral part of Bangladesh's national development and strategy and significant progress towards offering e-services to citizens and increasing the productivity of the public and private sector by adopting digital technologies had been achieved. Conversely, these developments have also resulted in an increasing number of cyber incidents[30], with most prevalent threats being ransomware attacks, DDOS, the unintended use of sources for cryptocurrency mining and the dissemination of misinformation and propaganda texts through social media.

Currently, there is no national computer-related incident response organisation and the authority that serves as the coordinating body for the reporting and management of cybersecurity incidents in the public sector is the Bangladesh e-Government Computer Incident Response Team (BGD e-GOV CIRT)[30]. In the private sector, only a very limited number of organisations which operate in the financial and telecommunications sectors has established security operations centers (SOCs) to respond to incidents with varying degrees of efficiency. For example, the Bangladesh Bank has established a hotline number where cyber incidents can be reported. Private organisations, however, are not obliged to report incidents to their respective regulatory body, prohibiting coordination and threat intelligence sharing within sectors (i.e., financial, telecommunication, transport).

Unfortunately, as participants suggested, there is no coordination between the private and public sector for incident response. Initial steps for establishing informal channels of communication are evident, as participants mentioned the existence of a small group of ICT experts from the police, the government, the military and financial institutions who share threat intelligence unofficially in an ad-hoc basis.

[29] Achieving Digital Bangladesh by 2021 and Beyond (2014). http://www.plancomm.gov.bd/wp-content/uploads/2015/02/18_Achieving-Digital-Bangladesh-by-2021-and-Beyond.pdf (last accessed 22/07/2018)
[30] https://www.cirt.gov.bd/incident-reporting/statistics/ (last accessed 22/07/2018)

The only established Computer Security Incident Response Team (CSIRT) as a leading authority for handling incidents within the public sector is the BGD e-GOV CIRT[30]. The main responsibility of this government agency, which is funded by the World Bank, is to monitor and manage the e-Government network and related infrastructure, including the National Data Centre. The e-GOV Computer Incident Response Team (CIRT) has acquired all the necessary equipment, including forensic software for data loss recovery and open source tools. Formal channels for reporting incidents are established, including e-mail, website or official letter for sensitive systems. Participants reported, however, that despite the e-GOV CIRT's efforts to promote these channels, employees in the public sector remain oblivious of how to report an incident. Once an incident is reported, there are clear procedures in place documenting which tools to use and how to analyse the data. Participants mentioned that the end result of an investigation is a report which provides information about the incident and is shared with the owner of the system into question.

The BGD e-GOV CIRT also engages in a range of initiatives from training to cyber exercises and the design of awareness campaigns. The training offered to its employees is regular, for a range of subjects and is accompanied either with certifications from well-established institutions such as GCHQ or it is based on material published by ENISA. The trainers have received training from the Korean CERT and have a dedicated budget at their disposal to participate in international conferences. The BGD e-GOV CIRT also offers training to other government organisations, as well as the police. Participants deemed that more than 60 people in the government were certified and 102 have requested to participate in the near future including police officers for forensic analysis training. The e-GOV CIRT is also a member of FIRST APCER, OIC-CERT and is in the process of accreditation to Trusted Introducer Family, therefore has channels of communication with other regional CERT teams.

Further resources are required for the e-GOV CIRT to fulfil its operational ability. Participants noted that the agency is operational only up to a certain time in the evening (5-6 pm) during working days, which significantly limits its incident handling capacity.

It is worth mentioning that according to participants, the new Digital Security Act has provisions for the creation of sector-based CERTs. Each sectorial CERT will report to a newly founded National CERT that will be tasked to share information amongst all CERTs in the country.

D 1.3 CRITICAL INFRASTRUCTURE (CI) PROTECTION

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Start-up

The concept of cybersecurity in critical infrastructure (CI) in Bangladesh is still in its infancy. The NCS recognises CI but there no official procedures in place to identify which infrastructures are key and should be considered as part of CI. Participants acknowledged that an unofficial list of identified CI assets is maintained by BCC. It was further suggested that a handful of organisations have developed basic software and hardware inventories. General risk management and emergency response frameworks are not present, with a few Internet Service Providers (ISPs), financial institutions and BCC being the exception by adopting European and US practices. Participants stipulated that significant progress will be achieved in the near future, due to the fact that NRD CS[31] has been tasked to develop and apply a national risk assessment based on ISO 27001[32], ISO 31000[33] and ISO 27005[34] within the next year.

Coordination within CI owners and between CI owners and the government, in relation to cybersecurity threat and vulnerability disclosure, is absent. There are no formal or informal channels for incident disclosure and reporting of incidents is not mandatory for any sector. Participants identified the need to establish legally what constitutes critical infrastructure as the first step before proceeding to the creation of an inventory. They further suggested that Bangladesh should establish an institution that will oversee the threat and vulnerability disclosure between CI stakeholders and ensure that CIs have the basic capacity to detect, identify, and respond to incidents.

It was mentioned that the new Digital Security Act will address all the aforementioned issues. It is worth mentioning that the English version we found evidence about the forthcoming national authority who will be responsible for the national cybersecurity strategy and will have the mandate to identify CIs. In order to improve the capacity of CIs in preventing detecting and handling incidents, NRD CS is in the process of installing sensors on the networks of 15 CI stakeholders. The aim is to create a common platform that will monitor and inform CIs of threats and vulnerabilities. NRD CS has further developed an information security guidance based on ISO 27001 and New Zealand information security manual[35]. This guide if enforced and fully implemented in all CIs has the potential to increase their capacity in detecting and preventing events.

[31] https://www.nrdcs.lt/en/
[32] https://www.iso.org/standard/69378.html
[33] https://www.iso.org/iso-31000-risk-management.html
[34] https://www.iso.org/standard/75281.html
[35] https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

D 1.4 CRISIS MANAGEMENT

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up

We were not able to obtain a clear picture regarding crisis management during our review. More specifically, the extent to which organisations consider cyber threats as part of crisis situations is uncertain. The most prominent incident that caused a major crisis in the financial sector and forced the Central Bank to develop better cybersecurity practices, was the $81 million heist that took place in 2016[36].

Participants suggested that not many developments in crisis management in cases of cyber-attacks have taken place since 2016, with some discussions on the need of national cyber crisis management taking place within the defence circles. A small number of CI stakeholders, as well as organisations from the finance sector hold business continuity exercises. Despite the fact that some Service Level Agreements are in place, ISPs have neither distinct instructions to run drills and simulations of cyber attacks, nor an obligation to maintain always a certain degree of availability for roaming in the case of interruption of their services.

To date, no crisis management plan has had a cybersecurity element. The e-GOV CIRT, however, has initiated a project namely "cyber gym" whose main task is to create a platform where CIs can simulate attacks on their network, enabling a range of exercises for crisis management. Participants mentioned that thus far the financial sector has participated in one exercise and they are in the process of developing more scenarios. This project can underpin national efforts to create a national cyber risk crisis assessment and can facilitate other CIs to train their employees in incident handling.

D 1.5 CYBER DEFENCE

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

[36] REUTERS, "Bangladesh Bank official's computer was hacked to carry out $81 million heist", (2016). https://www.reuters.com/article/us-cyber-heist-philippines/bangladesh-bank-officials-computer-was-hacked-to-carry-out-81-million-heist-diplomat-idUSKCN0YA0CH (last accessed 22/07/2018)

Stage: Formative

Cyber defence capacity in Bangladesh is at the formative stage. Currently, there is a cyber defence strategy. We were not able to identify the degree to which this strategy leads to an overarching policy that would provide a framework for managing cyber defence at the national level as it was not publicly available.

There are also signs of maturity in the way the military functions with regards to cybersecurity. The Ministry of Defence has established a military CERT, while the Military University offers technical course specialising in cybersecurity. Participants acknowledged that incident response procedures and mitigation planning have been developed, and a "decentrilised approach" has been adopted to better understand where threats originate. An Active Directory (AD) is established with in-house software as well as "off the self" applications. Regular IT audits take place and the military acquires penetration testers to identify vulnerabilities. Some participants reported slight issues with the Internet infrastructure, because Bangladesh depends on other countries for satellite back-up links.

Despite the sensitive nature of the information that it handles and the fact that the military is a "confined culture", participants acknowledged the need to establish a knowledge share platform with other CERTs and to create common training courses.

Currently, the military maintains a training institution in cybersecurity which offers a variety of courses, while trainers regularly attend regional seminars. It was encouraging to observe the determination of the Ministry of Defence and the Intelligence services to seek collaboration actively with other countries but most importantly with other governmental departments. Participants reported that a plethora of bilateral training agreements with neighbouring countries are in place, however, attempts to collaborate with NATO members have been unsuccessful thus far. There are informal channels of communication between the military and the e-GOV CIRT mainly for threat intelligence sharing. A decisive step for an effective communication would be the identification of the type of information to be shared through these channels.

D 1.6 COMMUNICATIONS REDUNDANCY

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Start-up

It was not possible to obtain a clear picture regarding communications redundancy during the review. Digital redundancy measures may be considered in an ad-hoc manner by private telecommunications organisations but emergency response assets are not mentioned in a

national emergency plan. Participants also mentioned the absence of exchange points in ISPs which hinders communication redundancy.

To increase capacity in this factor, better coordination of the various efforts regarding communications redundancy should be sought. Participants highlighted the need to ensure uninterrupted functionality of the systems and zero tolerance of network breakdown for Internet service providers.

RECOMMENDATIONS

Following the information presented during the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the Government of Bangladesh. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

NATIONAL CYBERSECURITY STRATEGY

R1.1 The revised national cybersecurity strategy should set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture.

R1.2 The revised strategy should be aligned with national goals and risk priorities to be effective and must provide actionable directives with corresponding metrics for every action to monitor progress.

R1.3 Allocate a budget and assign a government agency to oversee the implementation of the national cybersecurity strategy, considering existing roles and responsibilities.

R1.4 Expand the ICT group with participants from the telecommunication sector, financial and education sector, critical infrastructures, and private sectors (Cisco, Microsoft etc) and schedule regular meetings to discuss progress on the implementation of the strategy.

R1.5 Ensure that the information security standards developed by NRD CS are the minimum standards to be adopted for the public sectors and its implementation is included into the national cybersecurity strategy.

INCIDENT RESPONSE

R1.6 Identify government bodies and organisations in the private sector that are key to national cybersecurity.

R1.7 Create a national CSIRT with the mandate to collect incident information from all sectors and create CERTs for every critical sector (i.e., Finance, Telecommunications, Government, Military, Oil and Gas etc.)

R1.8 Create a mandate for a national cyber incident response detailing when and how organisations should report incidents. Reach consensus among stakeholders on architecture, interfaces, and standards for information exchange. Common standards promoted, for example, by the EU and the US are STIX and TAXII. Stakeholders should include private and public sectors, as well as the cybersecurity community at national, regional and international levels.

R1.9 Categorise and record national-level cyber incidents in a central registry hosted by the newly formed national CSIRT. E-Gov CIRT can potential act as a precursor until the national CSIRT is fully functional.

R1.10 The newly establish national CSIRT and sectorial CERTs should have clear processes, defined roles and responsibilities. Draft legislation that will expand on existing mandates to all CERTs. It should:

- *ensure high level of availability and business continuity,*
- *monitor incidents at a national level,*
- *provide early warnings, alerts, announcements, and disseminate threat intelligence to relevant stakeholders,*
- *respond to incidents,*
- *provide risk and incident analyses, and establish relationships with the private sector and other countries*

R1.11 Establish metrics to monitor and evaluate the effectiveness of all CERTs. In addition, enhance collaboration with the Association of Southeast Asian Nations (ASEAN), regional CERTs and other international bodies.

R1.12 Establish regular training for the employees of all CERTs and design metrics to assess the results of this training. Courses offered by e-Gov CIRT can underpin training for the other CERTs.

R1.13 Identify and document key incident response processes highlighting when and how different ministries and organisations should be involved.

R1.14 Establish a secure cyber information sharing network among national CERT, sectorial CERTs, CIIs and private sector where organizations can share cybersecurity information on a voluntary basis and which can be used as a line of communication in time of crisis.

CRITICAL INFRASTRUCTURE (CI) PROTECTION

R1.15 Develop and conduct a national risk assessment aiming to identify CI stakeholders and national threats.

R1.16 Develop and disseminate a list of CI assets with identified risk-based priorities.

R1.17 Establish a mechanism for regular vulnerability disclosure and information-sharing between CI asset owners and the government. Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CI operators.

R1.18 Identify internal and external CI communication strategies with clear points of contact.

R1.19 Establish information protection and risk management procedures and processes within CI, supported by adequate technical security solutions, which inform the development of an incident response plan for cyber incidents.

R1.20 Establish common procedures to measure and assess the capability of CI asset owners to detect, identify, respond to, and recover from cyber threats.

R1.21 Task regulators for every sector to mandate disclosure of incidents. Set thresholds for incident disclosure after consultations with private and public organisations from the respective sectors.

CYBER DEFENCE

R1.22 Ensure the development of a cyber defence component in the national security strategy. This component should consider the threats to national security that might emerge from cyberspace.

R1.23 Develop a communication and coordination framework for cyber defence in response to malicious cyber-attacks on military information systems and critical infrastructure.

R1.24 Assess and determine cyber defence capability requirements, involving public and private sector stakeholders. Conduct continuous reviews of the evolving threat landscape in cybersecurity to ensure that cyber defence policies continue to meet national security objectives.

COMMUNICATIONS REDUNDANCY

R1.25 Allocate appropriate resources for activities such as hardware integration, technology stress testing, personnel training and crisis simulation drills, but also ensure that redundancy efforts are appropriately communicated to relevant stakeholders.

R1.26 Establish a process, involving all relevant stakeholders, to identify gaps and overlaps in emergency response asset communications and authority links.

R1.27 Link all emergency response assets into a national emergency communication network with isolated but accessible backup systems.

R1.28 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.

R1.29 Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. Create outreach and education activities of redundant communications protocols tailored to the roles and responsibilities of each organisation in the emergency response plan.

R1.30 Allocate national cybersecurity exercise planning to e-Gov CIRT. Conduct and test a needs assessment of measures with consideration of a simple exercise scenario where multiple CI stakeholders are involved. Involve key stakeholders and think tanks, academia in the exercise planning process.

R1.31 Include cyber elements within existing emergency/crisis exercises.

R1.32 Identify metrics to evaluate the success of the exercise. Evaluate the exercises and feed the findings back into the decision-making process.

DIMENSION 2
CYBERSECURITY CULTURE AND SOCIETY

Forward-thinking cybersecurity strategies and policies entail a wide array of actors, including users. The days in which cybersecurity was left to experts formally charged with implementing cybersecurity have passed with the rise of the Internet. All those involved with the Internet and related technologies, such as social media, need to understand the role they can play in safeguarding sensitive and personal data as they use digital media and resources. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programmes for users – systems that can be used easily and be incorporated in everyday practices online.

This dimension reviews important elements of a responsible cybersecurity culture and society such as the understanding of cyber-related risks by all actors, developing a learned level of trust in Internet services, e-government and e-commerce services, and users' understanding of how to protect personal information online. This dimension also entails the existence mechanisms for accountability, such as channels for users to report threats to cybersecurity. In addition, this dimension reviews the role of media and social media in helping to shape cybersecurity values, attitudes and behaviour.

D 2.1 CYBERSECURITY MIND-SET

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up - formative

The review looked at users and experts in three institutional settings: government, private sector, and the general public. The majority of participants stated that cybersecurity is a priority for the government and that leading ministries have developed a cybersecurity mind-set. Participants attributed this to the country's focus on an ICT development plan for 2021

which is underpinned by the NCS, but also stated that the Bangladesh Bank 'cyber heist' in 2016 was a "wake-up call" for the government to prioritise cybersecurity. However, the progress of implementation depends on and differs between ministries, is very reactive and has not reached all levels and arms of key institutions. The digital culture is not deep enough and participants mentioned that the cybersecurity concept remains new and not entirely understood, particularly as the level of individual users. For example, staff often share passwords and use unlicensed or out-dated software. These practices are widespread due to a lack of resources and levels of awareness. However, some simple initiatives are being implemented regarding technical measures, such as password policies and firewalls and digital signatures, that will be introduced soon**.**

In the private sector, cybersecurity has not yet become a priority and there is little awareness of cyber risks and threats. Particular SMEs and commercial financial institutions were mentioned as not being ready to protect themselves and their customers. Participants suggested the need to work in a holistic way, and in a national initiative, to increase cybersecurity capacity across sectors. Existing efforts are limited to individual or international company efforts, mainly in businesses related to IT. In one model company, cybersecurity is embedded in the everyday practices of employees, the management and the product and service development, and regular training on cybersecurity issues is mandatory. However, this is exceptional. Representatives of the private sector also raised the issue that cybersecurity expertise and knowledge is often concentrated and has not permeated throughout the organisations, as it is mainly concentrated among staff that work on IT. Also, Chief Information Security Officers (CISO) or Chief Information Officers (CIOs) are not existing in many organisations.

The general public has a minimal recognition of the need to prioritise a cybersecurity mind-set. Although incidents occur, such as prominent cases of Facebook hacking, cyber bullying and fraud, users do not internalize those risks when they go online and therefore do not know or take proactive steps to improve their cybersecurity based on well identified threats.

D 2.2 TRUST AND CONFIDENCE ON THE INTERNET

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-up - formative

Overall, the interviews indicated that Internet users in Bangladesh too often "blindly" trust ICT and Internet services and do not have the skills to critically assess what they receive and see online and to appropriately gauge the security of the applications they use. Participants often referred to "fake news" which is spread via Facebook (the platform is perceived by many users in the country as synonymous with the "Internet"). Measures to promote a more learned level of trust in ISPs and operators of Internet infrastructure were not known to the

participants and there was no evidence that any initiatives are under development or likely to be implemented in the near future.

It did not become clear from the consultations to which extent the government offers e-services. Participants referred to around 1,000 citizen centric services as reflective of an increasing trend toward online services. Others mentioned that every ministry has some services online but not a comprehensive set. Across the country, Union Digital Centres areas are digital centres that are equipped with computer and printers and offer around 200 services as a mix of online / offline means for citizens to download and print forms to submit for various purposes. Also, one commercial bank offers authorisation services online and salary payments are communicated via text messages. According to participants, many if not most users are unfamiliar with those services or lack trust in them. There were no reasons provided for this distrust. Overall, no initiatives have been implemented yet to make these more secure in the eyes of users, nor is the government publicly promoting the necessary security environment.

A somewhat different picture was revealed with respect to e-commerce services, which have become very popular in the country over the last years, making it to one of the booming sectors in Bangladesh (including those of international companies such as Uber). Participants acknowledged that trust levels of e-commerce services have increased because of the quality of the services experienced since they have been offered. For instance, a service called Pathao provides access to cycles, bikes, cars. Consumers also can book train tickets and get groceries online.

Facebook is also a platform for e-commerce. In most cases payment continues to be done in cash on delivery as credit cards and other electronic payment methods are at early and rudimentary stages of use across the country. Many banks have mobile banking portals and apps for consumers to pay by phone. The online offerings for corporate banking are still limited, due to money laundering legislation, which makes large payments illegal. This chilling effect has not yet triggered a review the existing legislation, according to participants.

Despite the proliferation of e-commerce services, the suppliers have not yet recognised the need for the application of security measures to maintain and strengthen the trust levels in those services. None of the participants were aware of any companies including ISPs who are informing users of the utility of deployed security solutions and the terms and conditions for using their services. It was mentioned that some banks provide the users with basic guidance on how to keep their personal identification number (PIN) safe and how to use their credit card safely. Participants were also concerned that many companies do not have any framework to draw from on how to protect the data of their clients nor is there any national framework that they must comply with, in particular with respect to financial services.

D 2.3 USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

Stage: Start-up

This factor looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights

People in Bangladesh, in both the public and private sectors, have little or no understanding about how personal information is handled online and the issues surrounding the protection of personal information. Their knowledge about the relationships between privacy and security concerns is insufficient and discussions regarding the protection of personal information online has not permeated the public discourse or has been limited to civil society groups, and this is despite well publicised cases of data leaks, scams and bullying. Most Internet users are not well aware of their privacy rights and how to secure personal information when they use technologies like mobile phones, online services and social media. One symptom is that people usually share birth dates or images and other personal information easily, particularly in the context of e-commerce and social interactions. But participants also mentioned that users who may be aware of the potential risks still give away personal details to service providers. This is not uncommon elsewhere, since people often value some services more than their personal privacy. However, this behaviour can be understood in the Bangladesh context since the country does not have data protection legislation and the country has no well-established tradition of protecting personal information.

There was a recognition among participants in our discussions that citizens need to better understand what information is personal and how they should use this information with more circumspection. There is a need for Bangladesh policy-makers to build a strategy and a policy that is built on an understanding of personal information and how it needs to be secured. Users also need to understand how to protect their personal information.

2.4 REPORTING MECHANISMS

This factor explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Start-up - Formative

The consultations revealed that there are two main channels from the public sector for reporting online fraud, cyber-bullying, child abuse online, identity theft, privacy and security

breaches, and other incidents. One is the e-GOV CIRT and the police. Victims can go to police or to a special branch to launch a complaint or contact the cyber call desk via phone, email or online portals. Another participant mentioned is going to local councils and unions, as well as NGOs and human rights organisations. It was mentioned that 10,000 complaints have been raised at the police and the number is increasing and that an increasing number of cases were being brought to court. However, it was also stated that victims, mainly women, are hesitant to report cases as they fear this would continue their social defamation. An example was cases in which a victim and a criminal were in a relationship. After the break up, the criminal then leaks sensitive, defamatory videos to Facebook. Despite improved training of police officers, including female officers, in this area, such fears were said to prevent authorities from more thoroughly investigating cyber cases, where the cooperation of victims is critical.

There was no evidence that these channels are well coordinated or widely promoted and no channels were known from the private sector except for Facebook, but it was mentioned that Facebook was often reluctant to respond to reports.

D 2.5 MEDIA AND SOCIAL MEDIA

This factor explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspect speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up

Cybersecurity reports about user problems on traditional and social media in Bangladesh are only ad-hoc. More often journalists cover bigger events such as international cyber attacks and larger cybercrime cases such as the National Bank heist, but these reports are also limited by the lack of sophisticated technical cybersecurity knowledge on the part of those who produce those reports. Social media was seen by many participants as a risk for the nation as platforms such as Facebook and Instagram are perceived to have been misused often to share false information. However, participants also highlighted the role that the media could play in raising public awareness of the risks in cyberspace and in supporting the development of a cybersecurity mind-set, in particular because they reach the populations in smaller towns and rural areas. Social media could also be used in a more positive way, e.g. to inform people about security and training opportunities.

RECOMMENDATIONS

Based on the consultations, the following recommendations are provided for consideration regarding the maturity of *cyber culture and society*. These aim to provide possible next steps

to be followed to enhance existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

CYBERSECURITY MIND-SET

R2.1 Intensify efforts at all levels of government to promote understanding of cyber risks and threats.

R2.2 Design coordinated training programmes for employees in the public organisations in cooperation with the private sector. Trainings should include:

- web security (for e.g.: protection of personal information online, social media, social engineering, secure web browsing, malware, passwords)
- email security (for e.g.: identify a phishing email, sending an email securely)
- data security (for e.g.: handling and classifying sensitive information, back-up and recovery)
- mobile device security (for e.g.: portable data storage)
- remote access security if offered (for e.g.: working from home/while travelling)

R2.3 Consider educating the public through the Union ICT centres on the nature and consequences of cybercrime and cyberbullying.

R2.4 Consider in collaboration with NGOs and international partners providing the youth social programmes (for e.g.: in schools and universities) that will teach students about safe and responsible behaviour online (for e.g.: the risks of using social media), including how to prevent any uncompromising behaviour.

R2.5 Consider setting up a multi-stakeholder group (including business, government, law enforcement agencies, civil society and academia) to run joint projects and initiatives as well as facilitating on-going discussions on cybercrime and cybersecurity issues.

R2.6 Design online programmes and training materials (for e.g.: cybersecurity best practices, cyber threat landscape in Bangladesh, risk management) in consultation with the multi-stakeholder group and make them freely accessible for the public. This will equip the public with the right skills needed for their everyday use of the Internet and online services.

R2.7 Identify vulnerable groups and high-risk behaviour across the public, in particular children and women, to inform targeted, coordinated awareness campaigns.

R2.8 Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices.

R2.9 Develop programme and materials to train and improve cybersecurity practices in small and medium enterprises (SMEs).

R2.10 Enhance efforts in the private sector, in particular financial and telecommunications sectors and e-commerce services, to employ cybersecurity good (proactive) practices.

R2.11 Promote the sharing of information on incidents and best practices among organisations and across sectors to promote a proactive cybersecurity mind-set.

TRUST AND CONFIDENCE ON THE INTERNET

R2.12 Develop and implement campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content they consume social media or smart-phone applications.

R2.13 Promote the implementation of user-consent policies by Internet operators.

R2.14 Encourage ISPs to establish programmes that promote trust in their services based on measures of the effectiveness of these programmes.

R2.15 Ensure that security measures are in place for existing e-government services for businesses, public organisations and citizen.

R2.16 Implement security measures in any planned and future e-government services from the beginning to build trust and uptake by all users.

R2.17 When introducing e-government services for citizens promote their use through a coordinated programme, including the compliance to web standards that protect the anonymity of users.

R2.18 Employ processes for gathering user feedback within government agencies in order to ensure efficient management of online content.

R2.19 To promote trust of users in e-services inform users about the utility of deployed security solutions.

R2.20 Emphasise the need for security during the development and implementation of e-commerce services with (e.g.: use of SSL encryption, post trust certificates/logos of third-party authentication services on the homepage).

R2.21 Ensure that the private sector applies security measures to maintain and strengthen trust in e-commerce services, including informing users of the utility of deployed security solutions.

R2.22 Encourage that users can easily access the terms and conditions for using e-commerce services.

R2.23 Encourage Chief Executive Officers (CEOs) to use social media platforms in order to create trust with their customers and increase transparency. Customers more likely to use e-commerce services and products if the CEO uses social media.

R2.24 To promote trust of customers in e-commerce services, post customer reviews (both good and bad) and testimonials.

USER UNDERSTANDING OF PERSONAL INFORMATION PROTECTION ONLINE

R2.25 Establish programmes with Non-Governmental Organisations (NGOs) and support existing efforts by stakeholders to raise user awareness of online risks. Promote measures to protect privacy to enable users to make informed decisions on when and how to share personal information online.

R2.26 Develop and implement a data protection legislation, including monitoring mechanisms of its application.

R2.27 Encourage a public debate on social media platforms and in the traditional media regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

R2.28 Develop a Code of Practice on Protecting Personal Information Online in consultation with multiple stakeholders that can be distributed within the public (for e.g.: in primary and secondary schools).

The Code of Practice should include:

a) guidelines regarding Internet safety and the dangers of misuse of personal information online
b) why personal data is important, how it is processed and how can users protect their privacy

REPORTING MECHANISMS

R2.29 Establish coordinated mechanisms within the public and the private sector that allows citizens to report cybercrime cases, including online fraud, cyber-bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular for women and other vulnerable groups.

R2.30 Engage with the private sector and the third sector to establish alternative mechanisms, potentially with support from international partners within the public and the private sector that allows citizens to report cybercrime cases, including online fraud, cyber-bullying, child abuse online, identify theft, privacy and security breaches, and other incidents, in particular for women and other vulnerable groups.

R2.31 Provide manuals to educate the public, teachers and parents about the types of cybercrime that can be reported, how to exercise their rights when falling victim to such crimes and how to report it.

R2.32 Raise awareness about new and existing reporting channels among the wider public and across stakeholder groups and cooperate with the private sector in this regard.

R2.33 Consider setting up the option for reporting cybercrime anonymously (for e.g.: anonymous online forms) on the secure website of the Cybercrime Unit of the Police as an alternative to telephone number and email. Also offer the option to report via social media.

R2.34 Consider establishing the national cybercrime centre as the central point of contact for citizens and businesses in cases of cybercrime but also strengthen the capacity in the police stations across the country.

MEDIA AND SOCIAL MEDIA

R2.35 In cooperation with civil society and media organisations (traditional and social media) develop programmes and campaigns to raise awareness among media providers and leading social media actors, for instance during the dedicated cybersecurity awareness month or dedicated web or social media sites on this topic.

R2.36 Enhance the understanding of cybersecurity among media providers (in particular journalists) and facilitate a more active role of media in conveying information about cybersecurity to the public.

R2.37 Encourage media content providers to disseminate information on good (proactive) cybersecurity practice that users can pursue to protect themselves or to respond to cyber incidents. This could stimulate social media discussions on the topic.

DIMENSION 3
CYBERSECURITY EDUCATION, TRAINING AND SKILLS

This dimension reviews the availability of cybersecurity awareness-raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

D 3.1 AWARENESS RAISING

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-up

Awareness raising programmes are available but they are very ad-hoc and not specified for different target groups. The BGD e-GOV CIRT as part of BCC engages in the design of awareness campaigns and has adapted some of the Stop.Think.Connect materials and publishes material on its website but it was not clear from the consultations if they are targeted to specific target groups and if any metrics were applied. The ICT division of the Ministry of Communication has an awareness training initiative with a focus on school and colleges, and an awareness group initiative conducted a study regarding cybercrime in Bangladesh. Participants also mentioned one initiative which aims to build awareness among, mostly female, students (10,000) on how to use social media and to explain the risks associated with using those platforms. Participants mentioned there were a number of initiatives supported by international partners but which have been discontinued. Another awareness campaign was mentioned during the sessions which promotes the secure use of passwords and sharing of personal information; however, participants could further specify who the target groups were.

No awareness campaigns for executive were known to the participants but there was an agreement that for all the strategy management cybersecurity should be a priority.

Participants suggested that the government should take a more active role in driving and coordinating a national cybersecurity awareness programme. The awareness unit which was recently established at the BBC could take this function in cooperation with technical experts and other institutions in the country. For instance, participants emphasized the important role that traditional and social media could play in this regard. Also, the universities and other educational institutions were seen as playing a role in order to teach the younger generations, as students should be taught from a young age and civil society organisations and the private sector.

D 3.2 FRAMEWORK FOR EDUCATION

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up

Overall, the government has not yet realised the action item of the NCS and a coordinated National Cybersecurity Education Framework is not yet in place. Cybersecurity qualification programmes in Bangladesh are very limited. The more than 140 public and private universities, especially in Dhaka have cybersecurity offerings, less though in the remote universities. There are a few master programmes and the Bangladesh University provides a degree in Information Security. Another private university provides theoretical courses but not hands-on training. Despite the government taken different initiatives to increase the number of cybersecurity experts, also those in universities is still very limited. Few public universities run CISCO Academy and certification courses in cooperation with ISACA. Participants mentioned that there is not a lot of demand for any of the offerings as cybersecurity does not seem an interesting field to study. They suggested to start a national initiative with the aim to foster the uptake of certification courses.

Enrolment in courses related to cybersecurity is very limited. Participants argue that it a “chicken and egg” situation, because of the lack of job opportunities in the field which demotivates students to study cybersecurity. A participant from academia mentioned that only 5,000 of 30,000 graduates got jobs. Also, the private sector in particular small ICT companies are not attractive employers and many graduates aim to work for public sector institutions such the BCC. Others argued that the opposite, that because of the significant higher salaries in the private sector, those who are highly qualified, take on of the few cybersecurity related jobs in the big companies

On the primary and secondary school level students have one lesson in ICT, which does not over cybersecurity, despite many children and teenagers use smartphones.

Participants suggested to ensure that a cybersecurity career lifecycle should be facilitated on the national level, from pre-level, the entry level, to medium the medium level and the expert level, based on a needs assessment and embedded in the NCS.

D 3.3 FRAMEWORK FOR PROFESSIONAL TRAINING

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Start-up – Formative

The need for training professionals in cybersecurity has been documented at the national level. Action item 5 under the priority area 2 "Organisational Structures" of the current NCS includes among other elements, the adoption of a national cybersecurity skills framework, the assessment and delivery of cybersecurity certification examinations. There was no evidence from the consultations if and to which extent any of this was implemented. The Government has taken different initiatives, e.g. the ICT project provides training to the government officials since 2005 on a voluntary basis. In the private sector, cybersecurity training is mandatory in some industries but for instance in the finance sector and as universities and training institutions the execution of policies is different between sectors. Participants emphasized the need to develop a national framework and procedures to implement cybersecurity frameworks across organisations regarding skills development.

A challenge is that despite the increasing level of digitalization and the level of required expertise required in cybersecurity has not increased with the consequence that experts in cybersecurity are not hired.

Participants agreed that every ICT personnel should have cybersecurity training, in particular in government. The ICT Ministry should get the mandate for training. Many participants mentioned training offerings by vendors and international partners, including Cisco, Symantec Australia and the government of Korea which provided numbers of training for government officials. Also, some institutions run in-house training courses but it is limited to single organisation and not a coordinated national approach.

RECOMMENDATIONS

Following the information presented on the review of the maturity of *cybersecurity education, training and skills*, the following set of recommendations are provided to Bangladesh. These recommendations aim to provide advice and steps to be followed for the enhancement of

existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

AWARENESS RAISING

R3.1 BCC to coordinate and cooperate cybersecurity awareness efforts with key stakeholders, in particular including telecommunications and financial service providers, social media platforms, civil society and international partners.

R3.2 Develop a national cybersecurity awareness-raising programme, initiated and supported by the Government, with initial target groups focusing on the most vulnerable users, such as children and women, based on international good practice.

R3.3 Develop an Action plan based on the revised Bangladesh National Cybersecurity Strategy.

R3.4 Create a single online portal linking to appropriate cybersecurity information and disseminate materials for various target groups via the cybersecurity awareness programme and social media.

R3.5 Coordinate awareness-raising effort, for instance through a dedicated cybersecurity awareness month (e.g. Stop.Think.Connect.) and develop material for specified target groups and sectors, based on international good practice.

R3.6 Integrate cybersecurity awareness-raising efforts into ICT literacy courses and initiatives that could provide established vehicles for cybersecurity awareness-raising campaigns.

R3.7 Establish metrics and ensure that evidence of application and lessons learnt feed into existing and new developed programmes.

R3.8 Develop a dedicated awareness-raising programme for executive managers within the public and private sectors (in particular the financial and telecommunication sectors and companies which offer e-commerce services) as this group is usually the final arbiters on investment into security.

FRAMEWORK FOR EDUCATION

R3.9 Develop an Action plan for issues related to education based on the revised Bangladesh National Cybersecurity Strategy and define role and responsibilities for implementation.

R3.10 Develop qualification programmes for cybersecurity educators and start building a cadre of existing and new professional educators to ensure that skilled staff is available to teach newly formed (and existing) cybersecurity courses.

R3.11 Integrate specialised cybersecurity courses in the all computer science degrees at universities and offer specialised cybersecurity courses in universities and other bodies.

R3.12 Make an introductory course in Cybersecurity Awareness a component of ALL University courses.

R3.13 Create cybersecurity education programmes for non-specialists and make them available at universities and other bodies.

R3.14 Collect and evaluate feedback from existing students for further development and enhancement of course offerings.

R3.15 Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the private sector.

R3.16 Ensure that all cybersecurity education efforts are coordinated and optimized to maximize the available teaching capacity.

R3.17 Investigate the job market in cybersecurity and emphasize and advance the creation of more job opportunities.

FRAMEWORK FOR PROFESSIONAL TRAINING

R3.18 Train general IT staff on cybersecurity issues so that they can react to incidents as they occur.

R3.19 Identify training needs and develop training courses, seminars and online resources for targeted demographics, including non-IT professionals. Cooperate with the private sector to develop those offerings.

R3.20 Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.

R3.21 Document national training needs so that the professional needs of society can be adequately met.

R3.22 Develop metrics to evaluate the take up and success of cybersecurity training courses (e.g.: seminars, online resources, and certification offerings).

R3.23 Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.

R3.24 Establish regular mandatory training for IT employees and general employees regarding cybersecurity issues.

R3.25 Create specific measures to help government and companies to retain skilled cybersecurity staff.

R3.26 Ensure that professional cybersecurity certification courses are offered across sectors within the country.

R3.27 Establish job creation initiatives for cybersecurity within organisations and encourage employers to train staff to become cybersecurity professionals.

DIMENSION 4
LEGAL AND REGULATORY FRAMEWORKS

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

D 4.1 LEGAL FRAMEWORKS

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks; privacy; freedom of speech and other human rights online; data protection; child protection; consumer protection; intellectual property; and substantive and procedural cybercrime legislation.

Stage: Start-up

In Bangladesh, there is no sufficient legislative framework for ICT security. Partial legislation exists that address some aspects of cybercrime. Some parts of the National Cyber Security Strategy have been enacted but it does not provide actionable directives to different cybersecurity stakeholders.

The main legal framework at the moment is the Information and Communication Technology (ICT) Act, 2006 which was amended in 2009 and 2013 defines and amends certain parts of law relating to legal recognition and security of information and communication technology and related matters. According to the ICT Act the cybercrime shall be treated as non-cognizable

offence[37]. Beside that the Bangladesh the Penal Code, 1860[38], the Pornography Control Act, 2012 (pg.16)[39], and the Bangladesh Telecommunication Act, 2001 apply in the context of cybercrime but not exactly relate to cybercrime.

Participants often referred to the Draft Digital Security Bill which was drafted including multi-stakeholder consultations and publication on a website for comment. According to participants it is about to be passed in the Parliament for enactment and shall become a central piece of national cybersecurity legislation. It addresses major legislation deficiencies with respect to cybersecurity and shall define national critical information infrastructures and includes provision for sector based CSIRTs. Each of those will report to the national CSIRT and share information amongst all certs in the country. It also has a focus on digital certificate, a definition of digital information and defines punishment for hacking, impersonation etc. However, the bill has been highly criticised by civil society organisations and human rights advocates because of the lack of transparency of the drafting process on one hand. On the other hand, these groups point to the risks for freedom of expression, the unclarity of many parts of the Bill and the potential risks for users which may arise (e.g. unintended access and changes to computers which would be unlawful), the role of law enforcement and the duplication of restrictions which already exist as provisions in the Penal Code but with harsher punishments. According to participants, the concerns which were formally expressed are relevant and are going to acknowledged in the version which will be discussed in parliament.

Human rights are defined in the Constitution from 1972[40] but there are no references to cyber space.

In 2015, Bangladesh Bank issued sectorial regulation for cybersecurity through Guidelines on ICT security for Banks and Non-Bank Financial Institutions (2015)[41] that are applicable to all banking institutions. However, it is not clear whether these guidelines are effectively enforced.

Cyber incident reporting is voluntary in Bangladesh and there are no legal and regulatory frameworks for incident reporting obligations and responsible disclosure.

[37] United Nations Office on Drugs and Crime: Cybercrime Repository: Bangladesh. Information and Telecommunications Act (2006) https://www.unodc.org/cld/v3/cybrepo/legdb/search.html?lng=en#?c=%7B%22filters%22:%5B%7B%22fieldName%22:%22en%23legislation@country_label_s%22,%22value%22:%22Bangladesh%22%7D,%7B%22fieldName%22:%22en%23__el.legislation.crimeTypes_s%22,%22value%22:%22Cybercrime%22%7D,%7B%22fieldName%22:%22legislation.nationalLawArticle@title_s%22,%22value%22:%22Information%20and%20Telecommunication%20Act,%202006%22%7D%5D,%22match%22:%22%22,%22sortings%22:%22%22%7D (accessed 25 July 2018)

[38] Bangladesh Panel Code 1860 https://publicofficialsfinancialdisclosure.worldbank.org/sites/fdl/files/assets/law-library-files/Bangladesh_Penal%20Code_2010_en.pdf (accessed 25 July 2018)

[39] Bangladesh Pornography Control Act, 2012 https://docs.google.com/viewer?a=v&pid=sites&srcid=ZGVmYXVsdGRvbWFpbnxtYWtpdDR1c3xneDo2ZWM2MjRhNmE4MTFmODI5

[40] Bangladesh Constitution http://bdlaws.minlaw.gov.bd/pdf_part.php?id=367

[41] Bangladesh Bank: Guidelines on ICT security for Banks and Non-Bank Financial Institutions 2015, https://www.bb.org.bd/aboutus/regulationguideline/brpd/guideline_v3_ict.pdf (accessed 25 July 2018)

E-commerce is very popular in Bangladesh. Consumer protection is enacted through Consumers' Right Protection Act, 2009[42], but this law does not specifically address online fraud and other forms of cybercrime.

ICT procurement is governed by Public Procurement Act[43] adopted in 2006 and Public Procurement Rules (2008) contains no specific provisions for procurement of ICT services. Some of the private sector companies have their own ICT procurement policies with security provisions for software and hardware procurement.

Intellectual property protection is governed by the Customs Act (2016), Copyrights Act (2005)[44], Patents and Design Act (1911)[45] and Trademarks Act (2009)[46], but they do not contain specific provision for the protection of intellectual property of online products and services.

There is not Data Protection Legislation but participants mentioned it under the early stages of development. However, public discourse on data protection issues and multi-stakeholder consultations has not started. According to participants the General Data Protection Regulations (GDPR) of the European Union (EU) is not yet an issue in the country. Foreign banks mostly have their data outside the country and follow the regulation there.

Child protection is enacted through Children's Act (2013)[47], but it does not contain provisions for children online protection.

BCC has issued and made publicly available Government of Bangladesh Information Security Manual (GOBISM), which governs information security principles and controls for the protection of information which is intended for use by the system owners at government departments, agencies and organizations, but the level of awareness among government departments and its implementation is low.

Bangladesh has identified its CI, however, legal and regulatory frameworks are in the early stages of development and implementation.

[42] Directorate of National Consumer Rights: Consumers' Right Protection Act 2009 https://dncrp.portal.gov.bd/site/page/81410ae5-17d8-456c-8cff-4bbd8742d809/The-Consumers%E2%80%99-Right-Protection-Act,-2009- (accessed 25 July 2018)

[43] Government of the People's Republic of Bangladesh: The Public Procurement Act 2006: http://www.rhd.gov.bd/Documents/PPR/07%20-%20ThePublicProcurementAct2006(041207)45.pdf (accessed 25 July 2018)

[44] WIPO: Bangladesh Copyright Act http://www.wipo.int/wipolex/en/details.jsp?id=11172 (accessed 25 July 2018)

[45] Patents and Design Act (1911): http://bdlaws.minlaw.gov.bd/pdf_part.php?id=94 (accessed 25 July 2018)

[46] WIPO: Bangladesh Trademarks Act (2009) http://www.wipo.int/wipolex/en/details.jsp?id=7662 (accessed 25 July 2018)

[47] International Labour Organization: Bangladesh Children's Act (2013)[47], http://www.ilo.org/dyn/natlex/natlex4.detail?p_lang=en&p_isn=94284&p_country=BGD&p_count=137&p_classification=04&p_classcount=8 (accessed 25 July 2018)

D 4.2 CRIMINAL JUSTICE SYSTEM

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Start-up - Formative

The National Police has a cybercrime division. According to participants about 200 law enforcement officers (both female and male) based there and across the country have received training on cybercrime and digital evidence. Training is received on a regular basis from international partners like Spain, Japan, Korea, India and other international partners, and Training-of-Trainers initiatives aim to ensure knowledge exchange. In particular specific training on digital forensics and on security tools and activities is required since online banking will increase rapidly and participants anticipate the increase of cybercrime.

There is no effective training for prosecutors and judges and their expertise to deal with cybersecurity incidents is insufficient and according to participants there is currently only one judge who is able to handle cybercrime cases, according to participants.

D 4.3 FORMAL AND INFORMAL COOPERATION FRAMEWORKS TO COMBAT CYBERCRIME

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Start-up

Legal assistance in cybercrime investigation is enacted bilaterally with countries in the region and the USA through mutual legal assistance mechanisms or through INTERPOL. Discussions on Bangladesh becoming a party to regional or international instruments on cybercrime are at the very early stages and the country has not signed the Budapest Convention yet, for instance. Participants stated the exchange with other countries is very active also beside the formal agreements.

Information-sharing exchange with the private sector is a challenge. Participants expressed concern in particular regarding Facebook which is "the Internet" for many users and used to commit crimes, life threats and child abuse. Facebook is reluctant to give us data. Collaboration works only with the ISPs as it is formalised through the Bangladesh Telecommunication Regulatory Commission (BTRC). If we need to find the end user from an

ISP then we get the information from them. We are very much cooperating with local companies. We have problems with IP6 issues. We use IP4 and we have an increase in number of Internet users.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity *Legal and Regulatory Frameworks*, the following set of recommendations are provided to Bangladesh. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

LEGAL FRAMEWORKS

R4.1 Consider setting up a periodic process of reviewing and enhancing Bangladesh's laws relating to cyberspace to address the dynamics of cybersecurity threats (e.g.: hate speech online, cyber bullying).

R4.2 Revise and adapt the established legislative framework addressing cybersecurity and cybercrime regarding the comments and concerns from various stakeholder groups.

R4.3 Review the current Digital Security Bill to ensure offences cover cyber criminality and responsive to technological advances.

R4.4 Develop new legislative provisions through multi-stakeholder consultation processes on children's safety online, data protection, consumer protection online, intellectual property online and human rights online.

R4.5 Dedicate resources to ensure full enforcement of existing and new cybersecurity laws and monitor implementation.

CRIMINAL JUSTICE SYSTEM

R4.6 Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.

R4.7 Consider establishing institutional capacity building programmes for judges, prosecutors and police personnel from security agencies to acquire new ICT skills

needed for cybercrime investigations (for e.g.: digital evidence gathering) and effective ways of enforcing cyber laws.

R4.8 Consider establishing standards for the training of law enforcement officers and ensure to build trust in the confidentiality of the cases to encourage victims to report cybercrime cases.

R4.9 Dedicate sufficient human and technological resources in order to ensure effective legal proceedings regarding cybercrime cases.

R4.10 Consider requesting reliable and accurate cybercrime statistics from the National Police in order to better inform decision-makers about the current cybercrime threat landscape in Samoa when developing policies and legislations to address this matter.

FORMAL AND INFORMAL COOPERATION FRAMEWORKS

R4.11 Strengthen international cooperation to combat cybercrime based on existing legal assistance frameworks and enter further bilateral or international agreements.

R4.12 Facilitate informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular ISPs.

R4.13 Consider establishing a 24/7 point of contact within the Cybercrime Unit of the National Police in order to provide instant assistance for mutual legal assistance requests.

DIMENSION 5
STANDARDS, ORGANISATIONS AND TECHNOLOGIES

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

D 5.1 ADHERENCE TO STANDARDS

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up

Bangladesh has established the Bangladesh Standards and Testing Institution[48] with a specific branch for information and technology sector standardisation where organisations, both private and public, can refer to for accreditation to ICT standards.

BCC in collaboration with NRD CS developed and published an information security guidance based on ISO 27001 and New Zealand information security manual[49], however, the public sector is segmented and each ministry decides on which security policies should be followed and there is no mechanism for audit control to identify the level of compliance. This guide if enforced and fully implemented in all public agencies has the potential to increase their cybersecurity capacity.

However, several exceptions exist. BCC has been recently certified for ISO 27001. Financial institutions are required to comply to the Guidelines for ICT security for Banks and Non-Bank

[48] http://www.bsti.gov.bd
[49] https://www.gcsb.govt.nz/publications/the-nz-information-security-manual/

Financial Institutions[50] and Integrated Risk Management Guidelines for Financial Institutions[51] issued by the Bangladesh Bank and compliance audits are performed by the Bangladesh Bank inspection team annually. Some of major telecommunication providers has been operating based on ISO27001 principles since 2013. The main reason for the absence of standards across all ministries, as acknowledged during the sessions, is the limited budget dedicated to IT and the lack of cybersecurity experts. Participants deemed that a centralised institution tasked to mandate the implementation of a unified set of standards for all ministries and to execute regular audit controls is long overdue. Although BCC, in collaboration with NRD CS, have developed an information security manual and promote a uniform application of these practices across all ministries, the lack the mandate to enforce these standards.

Private sector is relatively more advanced regarding the specification, adoption, and auditing of standards for cybersecurity. Participants suggested that market needs are the driving force for the implementation of standards, especially in the finance sector with the requirements imposed by Visa and Mastercard for international transactions. ICT policy guidelines are available by the regulator for all financial institutions, whereas there is no guidance in other sectors for organisations. Across other sectors there are no requirements for organisations to adopt to specific standards nor regulators have the mandate to enforce specific ICT security policies and monitor compliance.

However, participants also mentioned that a lack of regulation to mandate the implementation of specific standards in the finance sector hinders efforts to improve the cybersecurity posture of all organisations. Most financial institutions try to comply with PCI DCC and remain oblivious to other international standards such as ISO 27001 by choosing to follow internally developed policies, with the exception of the Central Bank. Telecommunications organisations adopt standards in an ad-hoc manner based on their needs. There is a combination of international standards, such as ISO 27001 and NIST cybersecurity framework that companies usually set out to follow and it is the only sector where we observed that organisation opt for international standards.

Regarding the standards related to procurement of software, similar conclusions can be drawn. There are standards for procurement of software in the public sector, however these do not include guidelines for cybersecurity. As participants noted, the lack of standards is evident from the pirated versions of Microsoft products that are frequently used in the public sector. In the financial sector, organisations have elementary audit controls in place for purchasing software. The most advance sector is telecommunications where organisations follow standards for procurement covered by NIST. Mandatory security checklists with technical and admin controls are performed which provides an overview of the new risks that novel software may create. These risks are documented, mitigation practices are designed and managerial approval for purchase depends on the level of residual risk. Some participants mentioned that telecommunication organisations have clear processes on how to manage governance for the cloud services they utilise. These organisations have recently designed and deployed cloud-solution checklists to determine how to process, maintain and assess the risk in the cloud.

Focusing on standards in software development, there are no guidelines or protocols in place related to cybersecurity. Participants suggested that there are heterogeneous approaches to

[50] https://www.bb.org.bd/openpdf.php
[51] https://www.bb.org.bd/openpdf.php

testing in-house software development; the e-GOV CIRT can assist in testing government systems, while the financial sector has internal teams that do not necessarily follow a specific standard.

The discussions indicated that BCC with the help of NRD CS, the National Bank, the main telecommunications companies, as well as international organisations (Cisco) could take a lead in facilitating the broader adoption and implementation of cybersecurity standards, as well as in promoting coordination and harmonisation across sectors.

D 5.2 INTERNET INFRASTRUCTURE RESILIENCE

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Start-up

Review participants did not raise any significant concerns regarding the resilience of internet infrastructure in Bangladesh. Telecommunication companies have a fully redundant infrastructure for the core network, the radio and the internet gateways. Distribution points are resilient except in remote locations. Risks on resilience are assessed regularly and participants claimed that from a subscription point of view service level agreements are met. There are strict business continuity plans with flooding being considered as part of the physical risk.

Internet penetration is fairly limited, especially in rural areas, as costs are very high and service is not yet reliable. As participants suggested, fixed broadband market is underdeveloped with a small penetration rate. To our knowledge, there are no governmental projects in place to subsidise the cost of broadband development to economically unattractive areas (to ISPs).

In stark contrast to fixed broadband connections, mobile market in Bangladesh is fast growing and companies offer mainly 2G connections with only 23% of the country being covered by 3G signal. Due to the fact that access to Internet from mobile phones is very cheap, an overwhelming number of online services have been developed in the recent years. The majority of participants were satisfied with the mobile internet service.

ISPs may also monitor some services for cyber attacks and provide in certain incidents guidance on how to resolve the problem. They also offer certain customers protection from Distributed Denial of Services (DDoS); however, this service is rather limited in take-up.

D 5.3 SOFTWARE QUALITY

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

An inventory of software used in public and in private sector, as well as a catalogue of secure software is currently absent in Bangladesh. The quality and performance of the currently used software, especially in the public sector, is problematic due to limited instances where pirated versions of Microsoft products are being used. Consequently, no policies can be followed on updating software products or monitor the functionality of applications. The information security manual designed by NRD CS, if adopted in full will provide the necessary policies for software quality.

Participants indicated that monitoring and quality assessment is conducted in an ad-hoc manner in few private institutions, especially in the telecommunications and financial sectors. There are also initiatives on software development mainly in the telecommunication sector that rely on standards of software design; private organisations however, depend heavily on obtaining software from multinational companies. Testing practices also exist in the financial and telecommunications sectors for newly developed software; the focus, though in the majority of the organisations, is on functionality rather than security properties.

D 5.4 TECHNICAL SECURITY CONTROLS

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up

The adoption of technical security controls in Bangladesh varies significantly across sectors and organisations. Participants suggested that the adoption and implementation of controls in government bodies is insufficient and inconsistently promoted, due to financial restrictions and limitations in human resources and lack of organisational structure. Security controls in most ministries are limited to password protection and in some cases the use of antivirus services, while there are no mechanisms in place to monitor compliance to security policies. IT personnel do not have the authority to compel officials to attend training or hold them accountable for not following security policies.

Often departments maintain their own servers, but due to limited resources back-ups are not implemented, there is no monitoring of sensitive files and security responsibilities are delegated to simple users. In addition, unauthorised machines may obtain access to these servers, since there are no controls to maintain an inventory or authenticate access to these servers for laptops or Internet of Things (IoT) devices.

In stark contrast, the recently deployed National Data Centre supervised by e-GOV CIRT monitors traffic for vulnerabilities, applies patching to outdated software and authenticates users before accessing the network. Data is encrypted in data centres and regular back-ups take place. The redundant data base is located in a different region to the main data base, complying to ISO 270001. However, these controls may be void since many end-user computers may contain pirate versions of Microsoft's operating systems. Focusing on email exchange in the government, official email accounts are typically not used for official communications, with users preferring private Gmail accounts instead. There are initiatives by BCC aiming to promote the use of the official email for governmental communications.

Participants voiced their concerns over the lack of personnel and the absence of training for the existing IT employees. Finally, of particular concern is the complete absence of evaluation metrics for determining the effectiveness of the existing technical controls. This is due to the fact that monitoring practices, which may allow such evaluations, as well as the detection and prevention of incidents, are scarce.

The adoption and implementation of security controls is more widespread in the private sector. Telecommunication companies appear to a have more sophisticated approach to cybersecurity with the adoption of a wide range of technical controls and the implementation of regular audits. Most organisations have established an SOC and use SIEM tools to create alert tickets for events. Automated software patching is available and monitoring controls for the successful completion of the update is present. Metrics on how often patching fails, as well as duration between the detection of the vulnerability and the installation of the update are considered to determine effectiveness of this control. Further stringent KPIs are present for the end-user machines. Participants also mentioned the use of two firewalls for the internal network traffic and the boundary perimeter respectively. Access control across all systems is performed and the use of IPS is adopted to collect logs and determine anomalous activities. End point detection and response solutions provide a granular level of alerts for users who opt to use their own device or mobile phones. Online mail exchange protection is present and maturity model assessments are conducted regularly by well-established consultancies such as KPMG and EY. Finally, penetration testing is provided by foreign companies.

Financial institutions only started to adopt controls tailored to their networks. Network-segmentation controls and monitoring tools are evident in this sector as well as the use of Intrusion Detection Systems (IDS) and elementary inventories of the hardware and software used in their networks. There are also some CI stakeholders that lack the level of sophistication that telecommunication companies have and rely solely on a foreign vendor for their security.

Due to the fact that regulators do not mandate a minimum set of controls for each sector to implement, private organisations have no incentive to adopt security controls. Participants suggested that legislation requiring organisations to implement specific controls would convince board members of private organisations to invest in security controls and enhance

their cybersecurity posture. Since there are no regulations in place to require the implementation of controls as well as auditing for compliance, mechanisms to assess the effectiveness of these controls are lacking.

D 5.5 CRYPTOGRAPHIC CONTROLS

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Start-up - Formative

Cryptographic controls in the public sector are applied both to data at rest and data in transit but only for the National Data Centre. The use of digital signatures is possible in Bangladesh but is not a common practice. Regarding the private sector, there is no standard cryptographic approach in place. The financial sector uses encryption to store personal information and for their web services. In the telecommunication sector, encryption is applied on the application level, communications use the SSL protocol, the majority of laptops are encrypted and third-party communications utilise VPN.

D 5.6 CYBERSECURITY MARKETPLACE

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

No domestic market for the supply of cybersecurity technologies nor for any insurance products has yet been developed in Bangladesh. There are few domestic commercial cybersecurity products since a small number of local companies offer antivirus services, while there are no cyber-insurance offerings in the market. During the review participants representing financial institutions suggested that they have started preliminary discussions on cyber insurance policies, even as extension of current business continuity policies that do not cover cyber, however the premiums offered by international insurance companies forbid the purchase of such policies.

D 5.7 RESPONSIBLE DISCLOSURE

This factor explores the establishment of a responsible-disclosure framework for the receipt and dissemination of vulnerability information across sectors and, if there is sufficient capacity, to continuously review and update this framework.

Stage: Start-up - Formative

No responsible disclosure policy or framework has been established in the public or private sectors. Participants suggested that due to lack of regulations regarding disclosure of incidents, the private sector is hesitant in providing information for cyber-attacks. As it was noted, organisations believe that disclosure of incidents will lead to reputation damages, especially in the telecommunications and finance sector. Similar conclusions can be drawn for gas companies that handle SCADA systems, where there are no reporting mechanisms in place.

There exist however, formal and informal reporting mechanisms for people to indicate incidents. The e-GOV CIRT maintains a website for government employees to report incidents, financial institutions provide a mechanism to their clients to report fraud, whereas citizens can visit police departments to report any type of online misconduct. Formal and informal channels of communication for sharing information are established between ISPs and law enforcement agencies. ISPs are obliged to store transition logs for six months and IP data for 10 years. Law enforcement agencies can request any information without the use of a warrant which is of great concern for human rights defenders.

RECOMMENDATIONS

Following the information presented on the review of the maturity of cybersecurity Standards, Organisations, and Technologies, the following set of recommendations are provided to Bangladesh. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity, following the considerations of the GCSCC Cybersecurity Capacity Maturity Model.

ADHERENCE TO STANDARDS

R5.1 Adopt a nationally agreed baseline of cybersecurity-related standards and good practices across the public and private sectors, including standards in procurement and software development. Consult with experts from all sectors and from the international community.

R5.2 Facilitate formal and informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders, in particular with ISPs.

R5.3 Task regulators to mandate the implementation of a nationally agreed baseline of standards, including on procurement processes and software development.

R5.4 Establish or assign an institution responsible for the implementation, auditing and measurement of the success of standards across public and private sectors. Apply metrics to monitor compliance and establish periodic audits.

R5.5 Promote discussions on how standards and good practices can be used to address risk within critical infrastructure supply chains by both government and infrastructure organisations. Promote the adoption of international IT standards, in particular during procurement and software development

R5.6 Establish mandatory requirements for the adherence of standards, by appointing security officers that will be held responsible for the implementation of these standards.

R5.7 Draft legislation to enforce disciplinary actions for policy violations.

R5.8 Streamline clear guidelines regarding cybersecurity for the procurement of hardware and software.

R5.9 Promote the awareness and implementation of standards among SMEs.

INTERNET INFRASTRUCTURE RESILIENCE

R5.10 Establish or assign an institution responsible to enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors, especially between telecommunication companies.

R5.11 Establish Exchange points

R5.12 Establish or assign an institution responsible to identify, implement and perform auditing of technology and processes deployed for Internet infrastructure.

R5.13 Identify and map points of critical failure across the Internet infrastructure.

R5.14 Encourage investment in new technologies, especially on IPv6 to increase Internet infrastructure resilience.

R5.15 Introduce Service Level Agreements for ISPs and telecommunications.

SOFTWARE QUALITY

R5.16 Develop a catalogue of secure software platforms and applications within the public and private sectors.

R5.17 Develop an inventory of software and applications used in public sector and Critical Infrastructure.

R5.18 Develop policies and processes on software updates and maintenance.

R5.19 Gather and assess evidence of software quality deficiencies regarding their impact on usability and performance.

R5.20 Establish or assign an institution to elicit common requirements for software quality and functionality in a strategic manner across all public and private sectors.

R5.21 Prohibit and remove pirated software from the government's infrastructure.

TECHNICAL SECURITY CONTROLS

R5.22 Encourage ISPs and banks to offer anti-malware and anti-virus services to citizens.

R5.23 Develop processes for reasoning about the adoption of more technical controls based on risk assessment methodologies across the public domain. Use the information security policies NRD CS have developed for BCC to guide the minimum required list of controls.

R5.24 Establish metrics for measuring the effectiveness of technical controls across the public and private domain.

R5.25 Establish or assign an institution responsible for identifying the need for and deployment of cybersecurity technical controls such as SANS 20, CESG 10 steps and PAS 55 across the public domain.

R5.26 Promote cybersecurity best practice for users.

R5.27 Designate an authority, within the government sector, to be responsible for the strategic decisions on technical controls that will supervise end-to-end all networks and will promote the adoption of a unified framework for security controls in the public sector. Consider the adoption of controls to enhance physical security in data centres. Designate an authority for every sector to have the mandate to ensure a minimum set of technical controls for CI stakeholders within this sector.

R5.28 Keep technical security controls up-to-date within the public and private sector, monitor their effectiveness and review on a regular basis.

R5.29 Conduct penetration testing for the public and private sectors, the results of which should inform the deployment of technical controls.

R5.30 Replace all pirated versions of software with licensed products.

R5.31 Create authentication processes for users signing in to critical networks in the public sector.

CRYPTOGRAPHIC CONTROLS

R5.32 Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest and in transit, according to the international standards and guidelines.

R5.33 Raise public awareness of secure communication services, such as encrypted and signed emails.

R5.34 Raise public awareness of secure communication services, such as encrypted and signed emails.

R5.35 Establish or assign an institution responsible for designing a policy, aiming to assess the deployment of cryptographic controls according to their objectives and priorities within the public and private sector.

CYBERSECURITY MARKETPLACE

R5.36 Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological products.

R5.37 Promote the sharing of information and best practices among organisations to explore potential cyber-insurance coverage.

RESPONSIBLE DISCLOSURE

R5.38 Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution, and an acknowledgment report.

R5.39 Establish or assign an institution responsible for supervising the process of responsible disclosure and ensure that organisations do not conceal this information.

R5.40 Develop a system to facilitate the sharing of threat-intelligence amongst critical infrastructure partners and ISPs. Promote sharing of threat-intelligence in the financial sector and incentivise companies to actively participate in it.

R5.41 Encourage the sharing of technical details of vulnerabilities among critical infrastructure providers and ISPs.

R5.42 Promote the existing methods for incident reporting in the public sector as well as the technical material published by the e-Gov CIRT.

R5.43 Define notification requirements for all sectors. These requirements should not only consider thresholds about availability of services but should also consider incidents that target the integrity and confidentiality of data.

ADDITIONAL REFLECTIONS

Even though the level of stakeholder engagement in the review was more limited than we might have hoped, which limits the completeness of evidence in some areas, the representation and composition of stakeholder groups was, overall, balanced and broad.

This was the 26th country review that we have supported directly.

Global Cyber Security Capacity Centre

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

Cybersecurity Capacity Portal: www.sbs.ox.ac.uk/cybersecurity-capacity