CMAGE

Cyber Security Maturity Assessment Global Ecosystem

Bangladesh Report

Maturity Model Assessment

2021

Report Structure

This report begins with a Highlight Report setting out key observations. That is followed by an introduction to CREST maturity model's structure and an explanation of the assessment methodology used in the research.

Five subsequent chapters contain detailed observations, one relating to each of the five dimensions of the Cyber security Maturity Assessment of the Global Ecosystem (CMAGE).

Each chapter begins with an overall assessment of the maturity of that dimension within the ecosystem, supported by written commentary highlighting significant observations.

A section-by-section assessment of the maturity of each of the indicators within the dimension follows.

Assessment of the maturity level assigned to each indicator is shown in a box immediately below the section heading. The box also contains the relevant maturity model definition (drawn from Appendix B). A short commentary supporting the maturity level assessment is found in the corresponding section.

The report contains six appendices:

Appendix A Glossary
Appendix B Summary of Maturity Level Definitions
Appendix C Professional Certifications & Member Organisations
Appendix D Country Context
Appendix E Bibliography
Appendix F Endnotes

Three standalone extracts of this report are available on request from CREST International:

- A Highlights Report
- A banking sector cyber security risk posture report, and
- A guide to the CREST Maturity Model methodology.

For further information, please contact: info@crest-approved.org

Navigation Key

Move back a page | Move forward a page | Return to contents page | Move back to previously viewed page

Contents

Foreword from Ian Glover, President, CREST International

While organisations and individuals can take steps to maintain and improve their own cyber security, most of us live in a highly connected world. We rely on the actions of others to play their part in sustaining our collective cyber security. Knowingly or unknowingly, we are all part of a complex cyber security ecosystem which reaches far beyond the technology itself.

At the organisational level, the cyber security ecosystem comprises:

- Those who set strategy and policy
- Regulators who set and enforce standards
- Those who buy/consume cyber security services
- Those who provide cyber security services
- Those who facilitate information sharing
- Those who prevent and investigate cyber-crimes
- Those who educate, train and nurture the cyber security workforce

In this Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) we have gathered evidence against twenty indicators across five specific dimensions of Bangladesh's cyber security ecosystem. CREST has made both quantitative and qualitative assessments to arrive at an overall judgment as to its level of cyber security.

This report draws upon the open-source evidence gathered and records assessments made. While it will never be complete, it has been externally validated.

The relational database containing the CMAGE model has helped facilitate consistent application of the assessment, allowing for ease of update and data maintenance, the ability to interrogate the data and to extend the model to include other factors.

Importantly, it enables comparisons over time to understand if investments are providing tangible benefits.

The report is not an end in itself. It is the benchmarked starting point for a journey of collaboration between CREST and national and international stakeholders with a shared interest in improving the overall cyber security posture in Bangladesh.

Unashamedly, the endpoint – at least from a CREST perspective - is that every financial services institution in Bangladesh becomes resilient to cyber-attacks, protecting all stakeholders, particularly the poorest in society.

I would particularly like to thank the Bill & Melinda Gates Foundation for its vision and support in this endeavour. I would also like to thank all those in Bangladesh and the international community who have contributed to this report.

Finally, I want to thank everyone at CREST International for their efforts in producing this report and their commitment to the journey that we are all now undertaking.

Ian Glover
President
CREST International

Highlights Report

Background

CREST International seeks to help build capacity, capability and consistency in Bangladesh's cyber security ecosystem. The underlying aim is that every financial institution in Bangladesh will become more resilient to cyber-attacks to better protect everyone in society.

A comprehensive understanding of the current situation is an essential starting point.

CREST's evaluation methodology, the Cyber security Maturity Assessment of the Global Ecosystem (CMAGE), provides evidence required to build a practical action plan, focused on areas where improvements are most needed.

It is also a benchmark that allows relatively quick and easy re-assessments to establish whether progress is being made.

The CMAGE contains many months of research and assessment, validated by local subject matter experts.

The results are complex. Inevitably, there are areas of good practice and areas where investments of time, effort and money are needed. The ecosystem is interconnected and interdependent. Making improvements in one part of the ecosystem will bring benefits to other areas of the ecosystem as well.

Maturity Model Assessment Summary

Overall Bangladesh Ecosystem

Maturity Level 2

Having gathered and analysed evidence from multiple sources, CREST assesses Bangladesh's cyber security ecosystem to be at Maturity Level 2, a level termed 'Transitional'.

Bangladesh has clearly started a developmental journey towards improving all aspects of its cyber security ecosystem.

With concerted effort, it can progress to Maturity Level 3 by adopting international good practice and utilising IPR-free guidance (being created by CREST International as part of the project's second stage).

Highlights Report

Summary of Observations

The overall maturity assessment for Bangladesh's cyber security ecosystem is based upon the assessed maturity of five constituent Dimensions:

1. National Strategy & Capabilities
2. Information Sharing
3. Services Provision
4. Professional Development
5. Banking Sector Risk Profile

Dimensions and Indicators

Within each **Dimension** are a number of **Indicators**, each of which has been assessed against a series of maturity level definitions following the gathering and analysis of evidence.

Qualitative Assessments — **1-4**

Qualitative Assessments — **5**

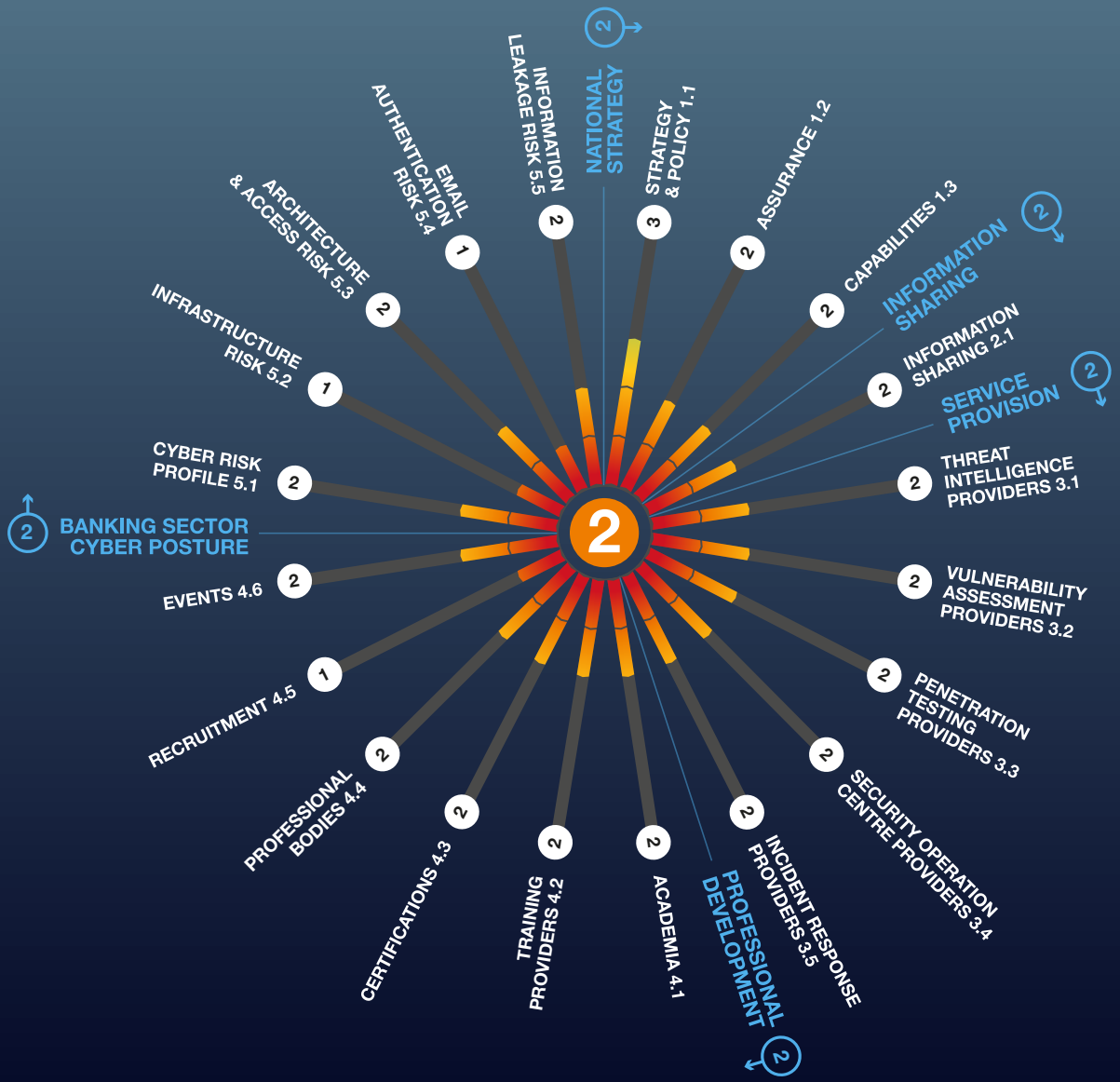
Maturity Scores

A summary of the maturity scores for the five Dimensions and the twenty constituent Indicators are depicted on the following 'starburst' diagram. The length of each radial relates to the assessed maturity of that particular Indicator as confirmed by the number on the white disc at its end. The radials are also colour-coded along their length – as follows:

RED	Level 1
AMBER	Level 2
YELLOW	Level 3
GREEN	Level 4
BLUE	Level 5

Highlights Report

Summary of Observations (continued)



Maturity Levels

1 Emerging
2 Transitional
3 Organised
4 Dynamic
5 Leading

Summary Assessment

Following the 'starburst' diagram is a summary assessment of the key observations for each Dimension and Indicator. More detail is contained in the five Dimension-specific chapters of the main report. This highlight report concludes with a section titled 'Next Steps,' the starting point for a conversation about practical measures to improve Bangladesh's cyber security ecosystem.

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

Formation of a National Cybersecurity Council in 2014 was a key milestone in Bangladesh's journey to improve its cyber security posture.

The 2018 Digital Security Act was another landmark moment which laid the foundations for **establishing a Digital Security Agency, Digital Forensic Lab and a National CERT.** The Act also established extensive legal sanctions to tackle cybercrime.

Bangladesh's government has an ambition to drive a 'Digital Government' and economic growth agenda through ICT capacity building, underpinned by strong cyber security.

Bangladesh Bank is updating its cybersecurity guidelines for financial institutions, which were due to be published in late 2020, but likely delayed by COVID-19, and unavailable at the time of compiling this final report. In 2020, the Executive Director of the Bangladesh Bank, Debdulal Roy, announced plans to launch CERT-Fin, a Computer Emergency Response Team focused on the financial sector. Together, these two initiatives are significant steps in improving financial sector cyber security. Developing an assurance scheme for the financial sector would appear to be the next logical step, which could be readily achieved.

Building upon the 2018 Digital Security Act, tackling cybercrime now appears to be a law enforcement priority.

Streamlined reporting processes for cyber incidents, together with a 24/7 reporting hotline, are reinforcing evidence. **A new Cyber Crime Unit is now operational and there have been recent investments in digital forensics and training,** such as establishing a Cyber Training Centre, Forensics Training Institute and a Detective Training Institute. A significant recent investment in national cyber defence capabilities is also noted.

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 2

Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

Establishing a National Computer Emergency Response Team (N-CERT) was mandated in the 2018 Digital Security Act.

Bangladesh government's **e-Government Computer Incident Response Team (BGD e-GOV CIRT)** is also currently fulfilling the N-CERT role. It is unclear if the two functions will eventually split. **BGD e-GOV CIRT is well-established with strong regional and international links.** A second CERT, Bangladesh CERT (BdCERT), was established in 2007, but may now be inactive - its last website update was in 2017.

BGD e-Gov CIRT is working with Bangladesh Bank to complete the formation of CERT-Fin, the proposed new CERT to support the finance sector, by late 2021.

This should generate a step-change in capability and, when viewed together **with the new N-CERT capability, warrant an upgrade of CREST's assessment to Maturity Level 3.**

Dimension 2

Cyber Security Information Sharing

Maturity Level 2

Highlights Report

Key Observations - Dimension 3 - Cyber Security Service Provision

There appears to be a reasonable mix of local, regional and international providers of cyber security services across most of the five disciplines.

Provision of threat intelligence and security operation centre services are the least developed sectors.

Three CREST International member companies offer one or more services from in-country offices.

Seven locally based companies were identified as also offering services, but their quality could not be assessed.

Several CREST and non-CREST companies also offer cyber security services to clients in Bangladesh from regional offices in nearby countries.

Opportunity

With some stimulus and focussed investment, Bangladesh could develop stronger local capability and potentially generate some export opportunities.

Dimension 3

Cyber Security Service Provision

Maturity Level 2

Highlights Report

Key Observations - Dimension 4 - Cyber Security Professional Development

While several of Bangladesh's universities and colleges offer computer science and ICT courses, very few offer specific cyber security degrees.

Those that do are mainly at postgraduate level. CREST identified a small amount of cyber-related academic research being undertaken.

A first-class cyber security industry needs to be underpinned by an expansion in cyber security education.

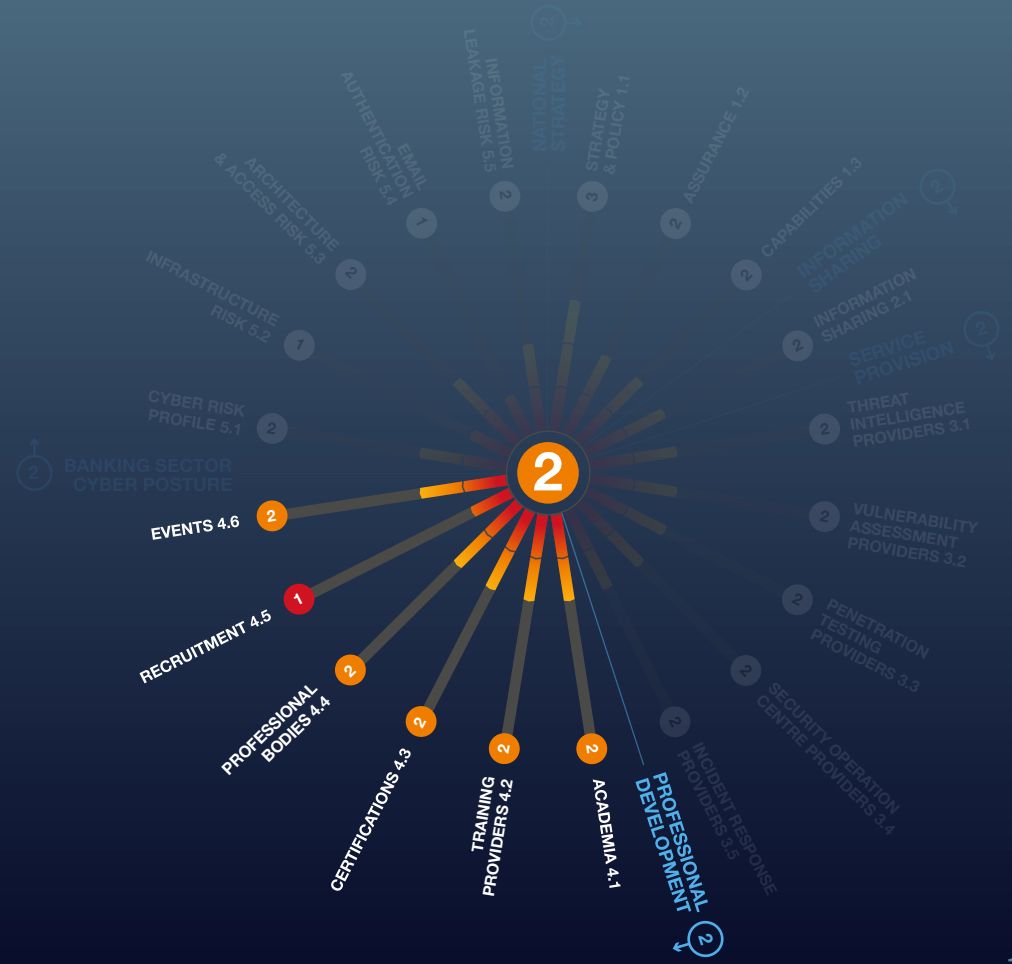
By utilising international good practice, Bangladesh could build upon existing computer science and ICT courses to support creating more specific cyber security courses and qualifications.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 2



Highlights Report

Key Observations - Dimension 4 (continued)

A reasonable mix of online and classroom training is available.

Most providers offer just one or two courses in a wider portfolio of technical and business courses.

It is unclear how many courses lead to recognised certifications.

Examinations for many international professional certifications appear to be accessible in Bangladesh.

The cost of some of these professional certificates are prohibitive to many.

But once individuals and companies see the benefits of professional certifications, cost issues may be overcome.

As part of Stage 2 of the CREST project some “pump priming” may be available to start the process.

While there is evidence of international professional bodies operating in country, this needs to be extended and strengthened to support national aspirations to grow the number of cyber security professionals.

Membership of cyber security focused professional bodies helps galvanise the community and provide forums for professional development and mentoring.

There are occasional cyber-related conferences and exhibitions to support the professional community, but little evidence was found of any in-country cyber security specialist recruitment.

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

CREST's research suggests several financial services organisations appear - at least, from an external view - to be susceptible to cyber-attacks.

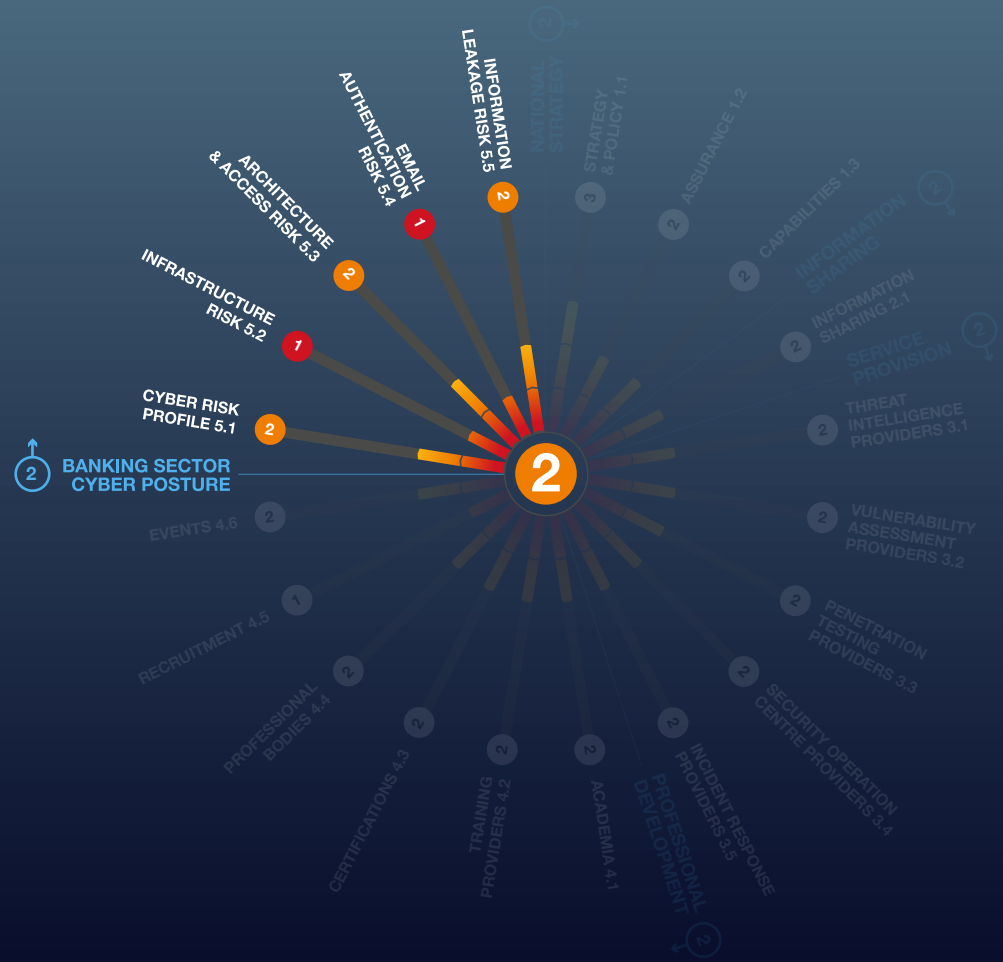
Regulators in Bangladesh can use this assessment to focus attention and highlight areas for review, provide access to the supporting guidance being developed and, where appropriate, encourage take-up of technical security measures to improve cyber resilience.

Continued on next page...

Dimension 5

Banking Sector Cyber Security Posture

Maturity Level 2



Highlights Report

Key Observation - Dimension 5 (continued)

For good cyber defences, organisations need to focus on several key risk areas, including:

- Security architecture
- Access control
- Configuration management
- Vulnerability patching
- Email authentication
- Staff training
- Limiting leakage of information which may be of use to an attacker

Without explicit permission, any external observations undertaken on an organisation are limited by legal and ethical constraints.

While directly assessing many of the key risk areas listed above is not possible, indirect passive (non-intrusive) assessment can be conducted on an organisation's internet-connected infrastructure.

Using this approach, accessible, measurable indicators were used to gain implicit insights into key risk areas.

Overall, passive external assessments were carried out on the public-facing IT infrastructure of a sample of 95 financial institutions. For obvious reasons, all results were anonymised.

Risk is a combination of vulnerability and threat. Vulnerability can be assessed by measurable observations. Threat is primarily a judgement based on intelligence reports.

The general threat to Bangladesh's financial institutions is assessed as lower than that for larger institutions in more advanced economies. Yet some still attract a significant threat score.

54% Overall, **54%** were awarded a cyber risk rating of 'Very High' or 'High', indicating Maturity Level 2 for Risk Profile.

27% Of the sample, **27%** had evidence of critical vulnerabilities on their infrastructure.

33% A further **33%** appeared to be carrying non-critical vulnerabilities, indicating Maturity Level 1 for Infrastructure Vulnerability Risk.

8% In respect of Architecture and Access Risk, **8%** of the sample appeared to have one or more remote access ports open on the public-facing infrastructure.

38% Some **38%** appeared to have one or more database ports open, leading to the award of Maturity Level 2 for this risk category.

57% Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **57%** of the sample.

79% Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **79%** of the sample, indicating Maturity Level 1 for Email Authentication Risk.

56% In **56%** of the sampled institutions, CREST identified that at least some staff data was available online because of third-party data breaches, including Maturity Level 2 for Information Leakage Risk.

There is significant room for improvement in the cyber security posture of many of Bangladesh's banks.

Highlights Report

Next Steps

1. This maturity assessment has not been carried out **as an academic exercise.**

2. Having undertaken the research, CREST International is keen to work with governments, regulators and other stakeholder communities **to drive improvements across Bangladesh's cyber security ecosystem.**

3. CREST is curating a comprehensive **library of IPR-free good practice guides and tools** to assist with ecosystem development.

4. Where there are gaps in the library, CREST will **work with renowned subject matter experts** to develop new guides and tools.

5. The library will be **available throughout 2021** and is shown on the next page.

6. Meanwhile, CREST will be **working with key stakeholders to identify pump-priming activities in Bangladesh**, to help create development pathways.

Highlights Report

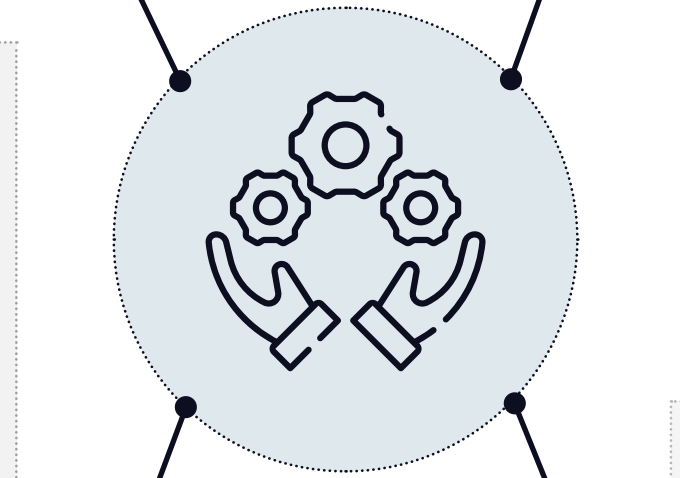
2021 Good Practices Guides and Tools

Goverment Strategy Policy

- Establishing National Cyber Security Strategies
- Introduction to Intervention / Prevention Activities
- Establishing a Cyber Crime Intervention Programme
- Establishing an Effective Cyber Crime Unit

Service Suppliers

- Introduction to Cyber Security Threat Intelligence
- Microfinance and Challenger Bank Threat Intelligence Maturity Model
- Standards of Vulnerability Assessment
- Vulnerability Analysis Maturity Model
- Procurement of Penetration Testing Services
- Penetration Testing Maturity Model for Financial Services, Challenger and Microfinance Organisations
- Critical Function of Security Operations Centres SOCs
- SOC Maturity Assessment Model
- Incident Response Maturity Model for Microfinance and Challenger Banks
- Guide Structure, Development and Deployment of Incident Reponse Teams
- Strategy Reports to Tier 3 (small organisations) Incident Response Services



Training and Academia

- Common University Degree Level Course Syllabus
- CMAGE Maturity Models for professional training providers
- Platform for Career Pathways

Security Postures

- Improving Technical Public Facing Cyber Hygiene
- Metrics for Measuring Improvement in Cyber Hygiene
- Cyber Security for Microfinance and Challenger Banks
- Generic Guide to Simulated Targeted Attack and Response
- Cyber Security Awareness Programme Community Projects

Introduction

Introduction

Background

This report seeks to provide a benchmarked assessment of the maturity of Bangladesh's cyber security ecosystem.

1. Output from this maturity model can be used to help key stakeholders identify areas where emphasis should be placed to help build capacity, capability and consistency within the ecosystem. The library of good practice guides and tools being developed by CREST can then be readily used to support a programme of improvements.
2. Where requested, CREST will seek to work with stakeholders to ensure improvements are delivered to the benefit of all. Periodic re-assessments can be made against this benchmarked starting point to ensure progress is made.
3. **The Bill & Melinda Gates Foundation's Financial Services for the Poor (FSP) programme**[1] seeks to support government and private-sector partners in a shared effort to establish financial services for the world's poorest people. Financial exclusion traps millions of people globally in a cycle of poverty that is difficult to escape. The programme aims to equip them with the means to build more prosperous and secure lives for themselves, their families, and their communities.
4. Financial services must be underpinned by the best possible cyber security to minimise the risk of the most financially vulnerable becoming victims of cybercrime. The best possible cyber security is only delivered when a holistic approach is taken to improve the cyber security ecosystem in which the entity exists.
5. CREST International has considerable experience in taking a holistic approach to addressing the shortcomings of cyber security ecosystems. CREST also has considerable experience of working with financial regulators in Europe, Asia and North America. It is therefore delighted to be actively supporting the Gates Foundation's FSP programme.

CREST International

6. **CREST is an international not-for-profit accreditation and certification body** that represents and supports the technical information security market[2]. It seeks to build cyber security capacity, capability and consistency by providing internationally recognised accreditation for organisations and professional certification for individuals providing cyber security services. It particularly focuses upon **Vulnerability Assessment, Penetration Testing, Cyber Incident Response, Threat Intelligence and Security Operations Centre services**.
7. **In carrying out its mission, CREST International works with a variety of stakeholders across the cyber security ecosystem, in**:
   - *Helping governments set national cyber security strategy and policy*
   - *Helping regulators establish assurance schemes that set and maintain performance standards*
   - *Helping the buying community purchase consistent quality services*
   - *Helping the supplier community deliver benchmarked cyber security services*
   - *Maintaining partnerships with academia and training providers*
   - *Maintaining dialogue with other professional bodies to ensure consistency*
   - *Supporting individuals to improve their knowledge and certify their skills.*

Introduction

Research Methodology

8. **Apart from the section of this report dealing with the banking sector cyber security posture,** all evidence used in preparing it has been gathered using open-source methods, including internet-based research supplemented - for clarity - by email and telephone enquiries. The research has also been presented to audiences of local and international subject matter experts for feedback and validation.

9. In respect of the banking sector cyber security posture, CREST worked with **Orpheus Cyber**[3], a leading cyber threat intelligence service provider, to carry out a passive (non-intrusive) external assessment of the public-facing IT infrastructure from a sample of the country's financial institutions.

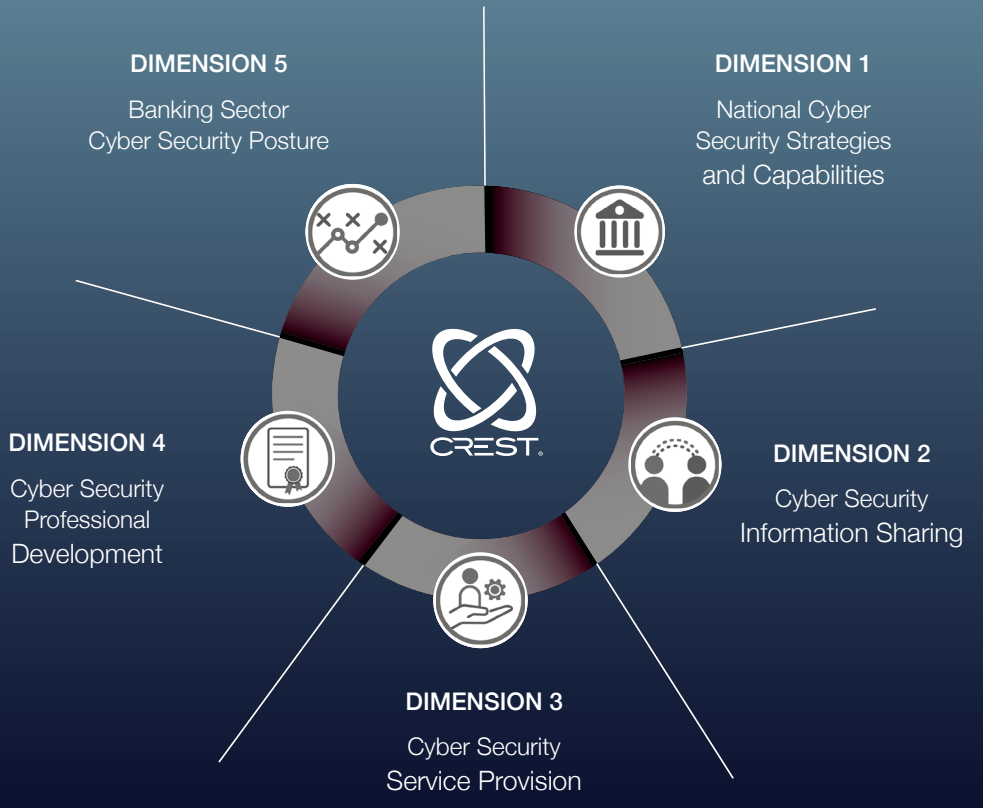
   The assessments were carried out by computer, to common standards, allowing for comparisons, benchmarking and periodic automated reassessments, if required. CREST believes this methodology is a global first - the first time rapid, automated mass assessment has been used as part of cyber security maturity modelling.

10. **Any omissions or corrections that arose during the validation process have now been incorporated into the evidence.** This report represents the baseline upon which improvements to the country's cyber security can be subsequently measured. It will be updated periodically, with stakeholders' support, to assist in reporting progress.

CMAGE Structure

11. The Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) is based on research methodology originally developed by CREST International in 2018. The structure of the CMAGE has matured through its practical application to the conduct of ten country assessments during 2020.

The CMAGE is based upon an assessment of twenty separate Indicators across five Dimensions. The five Dimensions are depicted below.



Introduction

Maturity Level Definitions

12. Each indicator has been assigned **a set of five maturity level definitions** against which evidence can be assessed in a consistent manner. In **Dimensions 1-4 assessment is qualitative. In Dimension 5 evidence is quantitatively assessed against computer-generated metrics.**
13. For simplicity of notation, each dimension has also been allocated its own maturity level, based upon the assessments given to each of its constituent indicators using, where appropriate, qualitative judgement.
14. **In all cases, a generic label has been assigned to each of the five levels of the maturity model, as follows:**

15. A list of the Dimensions and their associated Indicators is shown in the table below. A full listing of the five maturity level definitions for each indicator can be found at **Appendix B.**

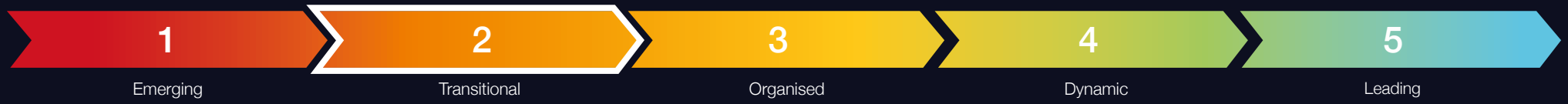
DIMENSION		INDICATOR	
QUALITATIVE ASSESSMENT			
1	**National Cyber Security Strategy & Capabilities**	1.1	Government Strategy & Policy
		1.2	Regulator/Government Operated Assurance Schemes
		1.3	Law Enforcement & Cyber Defence Capabilities
2	**Cyber Security Information Sharing**	2.1	Computer Emergency Response Teams (CERTs)
3	**Cyber Security Service Provision**	3.1	Threat Intelligence Providers
		3.2	Vulnerability Assessment Providers
		3.3	Penetration Testing Providers
		3.4	Security Operations Centre Providers
		3.5	Incident Response Providers
4	**Cyber Security Professional Development**	4.1	Academia & Higher Education
		4.2	Training Providers
		4.3	Professional Certifications
		4.4	Professional Cyber Membership Organisations
		4.5	Specialist Recruitment
		4.6	Events & Exhibitions
QUANTITATIVE ASSESSMENT			
5	**Banking Sector Cyber Security Posture**	5.1	Banking Sector Cyber Risk Profile
		5.2	Infrastructure Vulnerability Risk
		5.3	Architecture & Access Risk
		5.4	Email Authentication Risk
		5.5	Information Leakage Risk

Dimension 1

National Cyber Security
Strategy & Capabilities

National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2*



National strategy is of vital importance.

16. Without a national cyber security strategy, it would be difficult for law enforcement and the judicial system to tackle cybercrime. Academia and professional training providers would struggle to know what courses to provide; potential students would find difficulty in understanding career options. It would also be difficult to justify and target research.

    Without a national strategy, the public and private sectors would have no guidance or framework to base their own cyber security policies on. Ultimately, a lack of national cyber security strategy undermines economic growth. Examining a nation's cyber security strategy provides good insight into its willingness to implement cyber security measures and to tackle cybercrime. A national strategy sets the standards for all other sectors to follow.

17. In conducting the research, CREST sought to identify:

    - Government strategic guidance, policy and legislation published in relation to information/cyber security
    - When it was published
    - How thorough it was
    - Whether it empowered goverment departments and agencies to act, and whether the strategy has been implemented and updated.

18. Bangladesh government published a **"Perspective Plan of Bangladesh 2010-2021 – Making Vision 2021 a Reality[4]."** in 2012. Chapter 7 - **"Towards a Digital Bangladesh by 2021",** outlines the strategic ICT goals that will help move Bangladesh towards a poverty-free middle income prosperous country by 2021[5].

    The second Perspective Plan of Bangladesh 2021-2041, discussed in 2019[6], but published in 2020[7], builds on Vision 2021, with two principal visions:

    a) Bangladesh will be a developed country by 2041, and

    b) Poverty will be a thing of the past in Bangladesh[8].

    Chapter 9 – **"Creating an Innovation Economy for Bangladesh Through Fostering ICT and Scientific Research,"** covers a summary of Bangladesh's current status, what has been achieved so far and discusses national scientific and digital transformation and measures taken to uplift cyber security and improve trust in digitized services[9]. Annex 9 of the report contains tables outlining desired progress in ICT, including research and development, education and use of ICT to enhance the economy[10].

National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2* (continued)

There are several government organisations with cyber security responsibilities.

19. In 2014, the Ministry of Information and Communication Technology was integrated into the Ministry of Posts, Telecommunications and Information Technology (MoPTIT)[11] to become the Information and Communications Technology (ICT) Division[12].

    The ICT Division publishes strategy and policy and has its own Directorate / Department of ICT, established in 2013. The ICT Division sits over the Bangladesh Computer Council (BCC), the governing body for ICT-related activities, including developing ICT policy and strategy[13]. It also oversees the Digital Security Agency, formed in 2019[14], charged with implementing the Digital Security Act 2018[15] and monitor all issues relating to digital security[16]. The ICT Division also presides over Bangladesh Hi-Tech Park Authority and the Office of the Controller of Certifying Authorities (CCA).

20. The National Cyber Security Strategy 2014 mentions future formation of a National Cybersecurity Council, and mandates some of its roles[17]. Chapter IV of the Digital Security Act 2018 authorised establishment of a National Digital Security Council[18].

    The National Digital Security Council (NDSC) is a governmental body with 13 members, including:

    - Bangladesh's Prime Minister as Chair
    - Minister or Deputy of MoPTIT
    - Minister or Deputy of the Ministry of Law Justice and Parliamentary Affairs
    - Governor of the Bangladesh Bank
    - Inspector General of Bangladesh Police
    - Director General of Forces Intelligence
    - Secretary of the ICT Division, and others.

    The 2018 Act also details the powers and meetings of the council. NDSC meetings occur as and when needed. The Digital Security Agency acts as secretary to the council[19].

21. The UNIDIR Cyber Security Policy Portal (2021) on Bangladesh[20] mentions the National Cyber Security Council as being proposed. The Global Cyber Security Centre's Cybersecurity Capacity Review of Bangladesh (2018) discusses the National Cyber Security Strategy 2014 but makes no mention of the National Cyber Security Council[21]. It is assumed this is because the National Digital Security Council is a government body as opposed to a physical organisation.

Overall Assessment:

22. With its role in publishing national policy and strategy, as well as sitting over various organisations such as the Bangladesh Computer Council (BCC) and the Digital Security Agency, formation of the ICT Division[22] was a key milestone in Bangladesh's journey to improve its cyber security posture. The Digital Security Act 2018 was also a pivotal moment, laying the foundations for establishing the National Digital Security Council, the Digital Security Agency, a Digital Forensic Lab, and a National CERT. The act also established extensive legal sanctions to tackle cybercrime[23].

23. The recently published Bangladesh Bank Strategic Plan 2020-2040[24] will undoubtedly improve security and regulation of the financial sector. In March 2020, the Financial Reporting Council Bangladesh[25] mandated compliance to the International Financial Reporting Standards (IFRS) for all banks and financial institutions, another positive step in terms of regulation and security. The government has an ambition to drive a 'Digital Government' and economic growth agenda through ICT capacity building, underpinned by strong cyber security.

Development approach:

24. For Bangladesh's overall assessment score to improve, there needs to be a National CERT in addition to the BGD e-GOV CIRT[26] (which currently acts as National CIRT) along with the Fin-CERT and other sector CIRTS. Continuing development of ICT assurance in the financial sector will also help its maturity level in this Dimension.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy

Assessment – *Maturity Level 3*
Evidence of substantive actions to implement strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

Government strategy must be reviewed and updated regularly to help establish priorities and focus activities.

25. CREST's research sought information on publicly available strategic level policy and legislation relating to national cyber/information security, how up to date it is, and which agencies were empowered to uphold it.
26. **The Bangladesh Computer Council (BCC)**[27] was established in 1990 and sits in the **ICT Division of MoPTIT**[28]. Its roles and activities include:
    - Encouraging and providing support for ICT related activities
    - Formulating national ICT strategy and policy
    - Creating standards and specifications of ICT tools for government organisations
    - Developing human resources in the ICT sector

The BCC is a Certifying Authority. Information on training courses, policies and guidelines is publicly available on its website. Recent, key policies that relate to cyber security which are publicly available, though not all in English, are as follows:

- Digital Security Rules 2020[29] (not in English)
- National Strategy for Robotics, September 2020[30] (English)
- National Blockchain Strategy, March 2020[31] (English)
- National Internet of Things Strategy for Bangladesh, March 2020[32] (English)
- National Strategy for Artificial Intelligence Bangladesh 2020[33] (not in English)
- National ICT Policy 2018[34] (not in English)
- National Cyber Security Strategy 2014[35] (English)
- Guidelines on ICT Security for Banks and non-Bank Financial Institutions (2015)[36] (English version via the BGD e-GOV CIRT website)

27. The BCC provides cyber security services[37] via BGD e-GOV CIRT[38], covered in more detail in Dimension 2.
28. A National Internet of Things Strategy published in March 2020[39] by the ICT Division is one of the latest strategies relating to cyber security. It has a mission *"To transform Bangladesh into a technology-based country by ensuring the use of Internet of Things in every sector as an enabler for growth, as envisioned in Vision 2021, Sustainable Development Goals 2030, and Vision 2041."*[40]
29. The first two goals of the National IoT strategy are:
    - To create a $1bn IoT industry in Bangladesh by 2023
    - To create a 10,000-strong workforce for IoT for domestic and international markets by 2023[41].

    Others include establishing a research and development centre and a training and exhibition centre by 2023 and to create 100 new IoT start-ups by 2025[42].

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy (continued)

Assessment – *Maturity Level 3*

Evidence of substantive actions to implement strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

30. In the **IoT Strategy document's Chapter 3, Strategy 3.3: Skills Enhancement and Human Resource Development**[43]; it details plans to introduce IoT into the curriculum at engineering level and into research activity and doctorates. It details the introduction of IoT trade, certificate, and diploma courses, and training in IoT by inviting international experts to participate in conferences and visit educational institutions[44]. The goals and strategies of the National IoT Strategy 2020 are a positive declaration of intent by the Bangladesh Government.

31. To address the goals of Vision 2021[45], and Vision 2041[46], the ICT Policy 2018[47] (not found in English) was published. Chapter 9 of Vision 2041 gives a quick summary of the 2018 ICT Policy, stating that it was focused on digital security and leveraging new technologies such as IoT, big data, robotics, and AI, as well as ICT in education, ICT skills development, employment, innovation and business promotion with SDG targets to meet by 2030[48].

32. The Digital Security Act 2018[49] is the foundational legislation for implementation of Bangladesh's cyber security strategy and policy. Chapter II authorises creation of the Digital Security Agency with the role of overseeing and enforcing provisions in the Act. Chapter III outlines the role of a National CERT in responding to and mitigating cyber incidents. It also authorises creation of one or more Digital Forensic Labs (the BGD e-GOV CIRT Digital Forensic Lab was established in 2018[50]).

    Chapter IV describes establishing a National Digital Security Council, outlining the makeup of the council, its powers and roles; while Chapter VI of the Act criminalises a wide array of cyber activities, including hacking, identity fraud, and damaging infrastructure, as well as influencing activities such as disseminating propaganda or offensive material[51].

33. The National Cybersecurity Strategy (2014) is the basis for a coordinated national and globally compatible approach to protecting Bangladesh's critical infrastructure against cyber threats. See the next page for more details.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy (continued)

Assessment – *Maturity Level 3*

Evidence of substantive actions to implement strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

The National Cybersecurity Strategy (2014) has three national priorities:[52]

Priority 1: Legal Measures

Priority 2: Technical and Procedural Measures

Priority 3: Organisational Structures

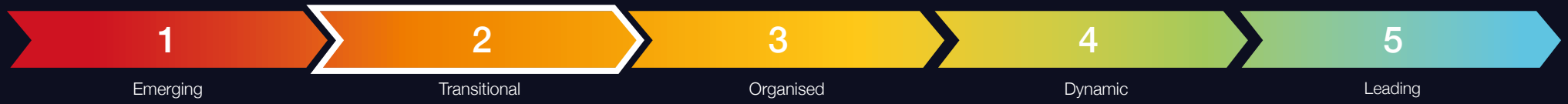
34. Action 1 states Bangladesh's cybercrime laws will be harmonised with global conventions. Action 2 gives government the legal authority to create organisations such as the National Cyber Security Council and defines the legal basis for creating a national CIRT[53].

35. These measures allow for creating a National Cybersecurity Framework with mandatory standards for all stakeholders to abide by, as well as a secure government structure and critical information infrastructure protection[54].

36. This covers the government's cybersecurity role, outlines the role of National Cyber Security Coordinator and details steps to improving the National Incident Management Capacity. One action is to build the Bangladesh Computer Incident Response Team (BD-CIRT) at the National Cybersecurity Council. It discusses cybersecurity skills training, identifying adopting a National CybersecuritySkills Framework as a key activity. Finally, the Digital Security Act 2018 also outlines building a national culture of Cybersecurity by promoting awareness and engaging with civil society and outreach to children[55].

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



Assessment – *Maturity Level 2*
Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.

The central bank or other lead financial authority of any nation is essential in setting ethical standards and operating frameworks for banks and financial institutions.

37. CREST's research looked for publicly available policies and laws which support and uphold financial ethics, integrity, and cyber security.

38. **The Financial Reporting Council (FRC) Bangladesh was established by the Financial Reporting Act 2015** and sits under the Ministry of Finance[56]. It is described as an independent body with the aim of bringing trust, credit worthiness and transparency to audit reports and publicly limited companies. **The 12-member body comprises representatives from government, Bangladesh Bank, Bangladesh Securities Exchange Commission, Federation of Bangladesh Chambers of Commerce and Industries, academia, and professional accounting bodies[57].** The FRC Bangladesh signed a contract with the International Financial Reporting Standards (IFRS) body in June 2020, but prior to that, in March 2020 the FCR Bangladesh mandated IFRS compliance for all banks and financial institutions[58].

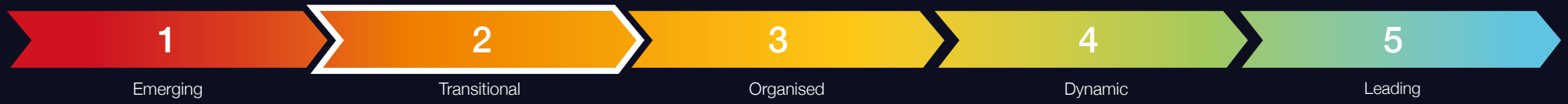
39. The Bangladesh Bank[59] has several publications available in English. **The two most relevant to cyber security are the Guidelines on ICT Security for Banks and Non-Bank Financial Institutions (2015)[60]**, available via the BGD e-GOV CIRT and Bank of Bangladesh website, and the recently published Bangladesh Bank Strategic Plan 2020-2040 - Fostering a Stable Financial System[61].

40. **The Strategic Plan 2020-2040** gives a review of the Strategic Plan (SP) 2015-19. Strategic Goal 9 of SP 2015-19 is ICT-related, with a KPI of preparing and circulating the ICT Security Guidelines (mentioned above) published in 2015[62]. Strategic Goal 11 has a KPI of implementing a risk-based audit approach, though no mention of ICT audit was discovered.

41. **In Strategic Plan 2020-2040, Strategic Goal 8** builds on the ICT development to *'create an IT environment that supports the delivery of accessible, secure, integrated, reliable and client centred programs and services to all stakeholders'*[63]. Objective 8.4 of Goal 8 discusses capacity building for ICT personnel, which includes establishing a research and development (R&D) centre to research new technologies such as blockchain and artificial intelligence. It also aims to establish state-of-the-art best practices by adopting international certifications in cyber security, ICT policy and guidelines, artificial intelligence and audit and inspection, to name a few. The KPIs for these objectives are establishment of the R&D Centre, and formulate frameworks, training, and relevant certifications for at least 50% of staff by December 2024[64].

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes (continued)

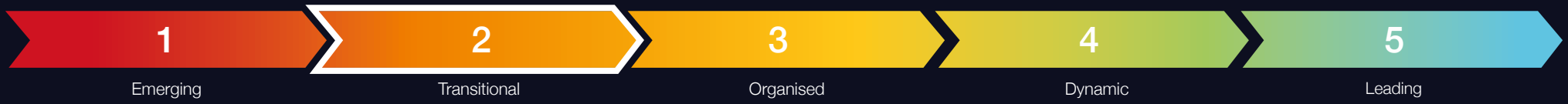


Assessment – *Maturity Level 2*
Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.

42. **Objective 8.6 of Goal 8** is to maintain state-of-the-art ICT infrastructure to ensure functional reliability, security, and business continuity. There are several action points to achieve this, one of which is to formulate cyber threat defence mechanisms and cyber crisis management mechanisms, with the KPI being that both will be established by December 2022[65]. Responsibility for implementing these ICT objectives lies with Bangladesh Bank's Information Systems Development and Support Department (ISDSD).
43. **Strategic Goal 10** is to *"Maintain international standards in accounting and internal controls and build up stronger brand image of BB though effective communication[66]."* This builds on audit and compliance and includes IT. Objective 10.1 it to adopt and maintain national and international standards of financial reporting and audit with a KPI of introducing an Enterprise Risk Management (ERM) unit by December 2020, and another to update all procedures manuals in line with International Internal Audit Standards (IIAD) and International Financial Reporting Standards (IFRS)[67] by December 2021. Objective 10.2 is to strengthen internal controls and compliance, with an action point to implement risk-based audit and IT audit by December 2021[68].
44. Bangladesh Bank's achievement in publishing the Guidelines to ICT Security for Banks and non-Financial Institutions in 2015, and the Strategic Plan 2020-2040 with its numerous KPIs, especially those relating to cyber security, IT audit and compliance, is a great statement of intent to embrace the challenges of the digitised financial world.
45. In an article in Bank Info Security dated May 13, 2020, it reports that Bangladesh Bank was likely to launch a Fin-CERT in 2020, which would report to the BGD-e-GOV CIRT at national level[69]. Launching a financial CERT would meet the KPI of Objective 8.6 in the current strategic plan, to establish a cyber threat defence mechanism and cyber crisis management mechanism.

National Cyber Security Strategy & Capabilities

Indicator 1.3 Law Enforcement & Cyber Defence Capabilities



Assessment – *Maturity Level 2*

Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime. Evidence of some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.

46. **It is important to understand the level of reporting for cybercrime as this is evidence of cybercrime being openly recognised, discussed, and taken seriously as an issue in a public forum.** CREST's research looked for what and where cybercrime was being reported, and what official action was being reported as taken to combat it.

47. Bangladesh Police have cybersecurity/cybercrime capability in both Dhaka Metropolitan Police and within the Criminal Investigation Department.

48. Dhaka Metropolitan Police have a **Counter Terrorism and Transnational Crime (CTTC) Unit**, with responsibility for cybercrime and cyber patrolling[70]. Its website does not give much more information about this unit and its cyber capabilities. A couple of articles from the Click ITTEFAQ dated January 15, 2016[71] and The Asian Age dated February 18, 2016[72], reported the founding of the newly formed CTTC unit. **The articles reveal it was formed, initially with 600 personnel, to combat cybercrimes, terror financing, human trafficking, drug smuggling and mobile bank related crimes[73].** The CCTC's Cyber Crime Investigation Division has an active Facebook page[74], which promotes cybersecurity awareness.

49. The project 'Enhancing the Cyber Crime Investigation Capability of Bangladesh Police' funded by the **Korea International Corporation Agency (KOICA)[75]**; established the **Cyber Police Centre (CPC)[76]** and upgraded the IT Forensic department into a state-of-the-art Forensic Lab. **Both departments sit within the Criminal Investigation Department of Bangladesh Police,** and were inaugurated by the Korean Ambassador to Bangladesh on January 23, 2017[77].

50. The IT Forensic department was originally established in 2012, but since being transformed by this project it now provides forensic support to all investigating agencies concerning cybercrime and digital evidence, giving forensic expert opinion that can be presented as judicial evidence[78].

51. The Cyber Police Centre (CPC) has a mission *'To create highly trained, efficient police officers who can investigate cybercrime efficiently and face the future cyber challenges'*[79]. Training focuses on cybercrime, cybersecurity, social media monitoring and digital forensics, and so far, it has produced a pool of over 600 highly skilled officers[80]. According to its Facebook page, the CPC's objectives include:

    - Preventing and reducing cybercrime
    - Increasing capability to deal with cybercrime
    - Increasing skilled labour in the cybercrime investigation sector[81].

    The CPC's Cybercrime Investigation Centre (CIC) comprises three teams: The Cyber Security Policy Planning Team, the Cybercrime Investigation Team, and the Digital Forensics Team (computer and Mobile)[82].

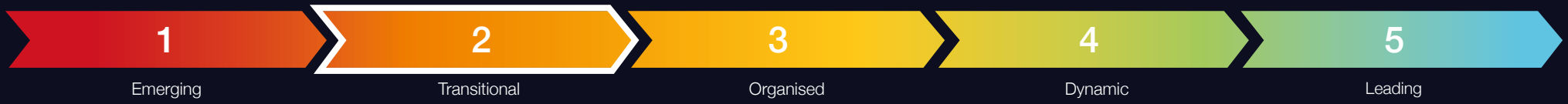
52. The Directorate General of Forces Intelligence of the Bangladesh Armed Forces has multiple intelligence functions which include cyber intelligence[83] and the Director has a seat on the National Digital Security Council[84]. **No evidence of a Military CERT was found during CREST's research.**

Dimension 2

Cyber Security Information Sharing

Cyber Security Information Sharing

Overall Dimension Assessment: *Maturity Level 2*



Information sharing is vital to achieving a common understanding of cyber security risks and vulnerabilities, helping counter cybercriminal threats.

53. Information sharing is vital to achieving a common understanding of cyber security risks and vulnerabilities, helping counter cybercriminal threats. There is no commercial advantage to be gained by not sharing information. Open publication of academic research and sector-specific information exchanges are example mechanisms for sharing information on cyber security risks, threats, and vulnerabilities. There is not much evidence of either of these mechanisms being currently well-established in Bangladesh.

54. Information sharing enables the spread of best practice. The research focused on looking for expert groups such as Computer Emergency Response Teams (CERTs) - teams of information/cyber security experts responsible for protection against, and detection and response to, cyber security incidents.

    They provide cyber security services, as well as running cyber security awareness campaigns or events for organisations and the wider public. Some CERTS operate nationally or within a specific sector and may have links to other regional or international CERTs to enable greater sharing of best practice.

55. The research also looked for evidence of other organisations working as cyber security awareness groups, in specific sectors or wider. With CERTs and information sharing groups, evidence was sought on how many exist and which sectors of society, business, or other stakeholders they provide services to.

Overall Assessment

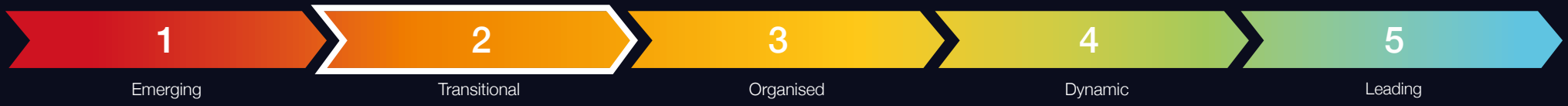
56. The establishment of a National Computer Emergency Response Team (N-CERT) was mandated in the Digital Security Act 2018[85]. Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT)[86] is currently fulfilling the N-CERT role. It is unclear if the two functions will eventually split. BGD e-Gov CIRT is well-established with strong regional and international links. A second CERT, Bangladesh CERT (BdCERT)[87], was established in 2007 but may now be inactive. The possibility of a soon-to-be established and much needed Fin-CIRT is promising.

Development Approach

57. While formation of a Fin-CIRT was publicly announced in 2020, the timeline is uncertain because of the Covid-19 crisis. The Fin-CIRT will collaborate with the BGD e-GOV CIRT[88]. This should generate a step-change in capability. Should a new National-CERT capability be established over and above the existing BGD e-GOV CIRT, then the combination of two new CIRTs will warrant an upgrade of CREST's assessment to Maturity Level 3.

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs) & Information Sharing



Assessment – *Maturity Level 2*
National CERT established. Meets ENISA CERT Maturity Model Tier 1 requirements.

58. **The greater the number of organisations sharing cyber security information and expertise,** the wider the spread of cyber security awareness and knowledge.

> **"Knowledge is like money: to be of value it must circulate, and in circulating it can increase in quantity and, hopefully, in value."**
> - American author Louis L'Amour (1908-1988)

59. The Bangladesh Computer Emergency Response Team (bdCERT) was formed in 2007. It liaises with other CERTS / CIRTS in country and is a member of the Asia Pacific (APCERT)[89] and the Organisation of The Islamic Cooperation Computer Emergency Response Team (OIC-CERT)[90]. The latest update on bdCERT's website was 2017[91], and there is no mention of the bdCERT in the Global Cyber Security Capacity Centre's Cyber Security Capacity Review of Bangladesh (2018)[92], so, it is assumed that it is no longer active.

60. Bangladesh Government's e-Government Computer Incident Response Team (BGD e-GOV CIRT) was established in 2016 and is currently serving as the National CIRT of Bangladesh (N-CERT)[93].

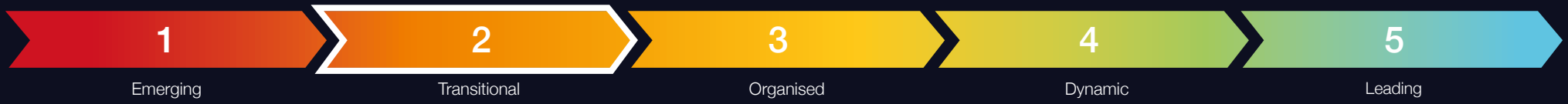
It has several different services, including:

- A Digital Forensics Lab[94]
- A Cyber Sensor Unit
- A 'Cyber Range' simulation platform to educate cyber security students
- Training, and
- Assessing practitioners and testing processes and technologies[95].

It partners with FIRST[96], APCERT[97], OIC-CERT[98], CREST and many other international CERTs[99] and has the responsibilities, including but not limited to, of *'receiving, reviewing, and responding to computer security incidents and activities in territory of Bangladesh as well as keeping close collaboration with international partners to secure the cyberspace of Bangladesh'*[100].

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs) & Information Sharing (continued)



Assessment – *Maturity Level 2*
National CERT established. Meets ENISA CERT Maturity Model Tier 1 requirements.

61. In concurrence with the Digital Security Act 2018, The 2018 Cyber Security Capacity Review of Bangladesh recommends establishing a National CIRT for Incident Response and that CERTS should be established for all critical sectors such as finance, telecommunications, government, military, oil and gas[101].

62. A May 2020 article in Bank Info Security reported the proposed launch of Fin-CERT in 2020, reporting to the BGD e Govt CIRT and Digital Security Agency[102] at national level. A Fin-CERT will be a great asset by boosting cybersecurity expertise within the banking and financial sector, while relieving BGD e-GOV CIRT of some of its current responsibilities. The article says the government proposed other sector CERTs, such as for the chemical sector, commercial facilities sector, emergency services, nuclear and transportation systems sectors[103]. No further information on the proposed Fin-CIRT was found during research.

63. The proposed Fin-CIRT ties in with the Bangladesh Bank Strategic Plan 2020-2040[104]. Objective 8.6 outlines creation of a cyber threat defence and cyber crisis management mechanism by December 2022[105]. The launch of a Fin-CERT would meet this objective.

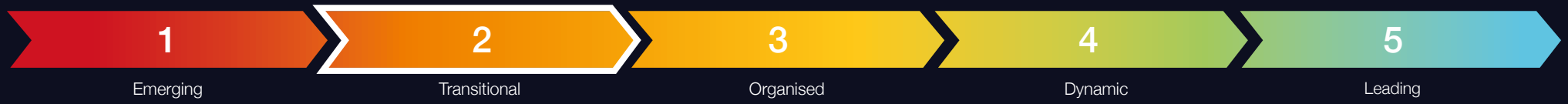
64. On October 22, 2020, BGD e-GOV CIRT organised a cyber drill for financial institutions. The theme was incident handling and 35 teams from 30 banks took part[106]. This is more evidence that BGD e-GOV CIRT was - at that time - still fulfilling the role of a National CIRT and that a Financial Sector CIRT has yet to be established.

Dimension 3

Cyber Security Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 2*



Professional cyber security service provision is essential in any nation to protect individual organisations and, by default, the national economy. Service providers form part of the front line in the fight against cybercrime.

65. Research into how cyber security services are currently provided in Bangladesh involved:
    - Identifying cyber security service providers
    - Examining what services they offer
    - What accreditations they held and
    - Whose accredited services and certifications they provided.
66. Company offices location and customer reach were also recorded. Were they were local companies, registered and only based in Bangladesh? CREST examined if they were regional companies, registered in another Asian country, but with offices and the ability to reach customers in other countries in the region. Or were they large international organisations, with multiple global office locations which may be located in-country? If not, do they have the ability to provide services into Bangladesh without having a permanent physical presence in country or anywhere in the Asian region? When examined together, these factors combined give an idea of the maturity of the cyber security industry.
67. Several of the identified companies provide more than one cyber security service, such as security services, training and events, for example, so appear in more than one indicator. Where possible, ICT companies which provided solutions via purchase of other technology products, such as software, were excluded from the research.

Overall Assessment

68. There appears to be a reasonable mix of local, regional and international providers of cyber security services across most of the five disciplines. Provision of threat intelligence and security operation centre services are the least developed sectors.
69. Three CREST International member companies offer one or more services from in-country offices. A further seven locally based companies were identified as also offering services, but their quality could not be assessed. A number of CREST and non-CREST companies also offer cyber security services to clients in Bangladesh from regional offices in nearby countries.

Development Approach

70. With some stimulus and focussed investment, Bangladesh could develop stronger local capability and potentially generate some export opportunities.

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local/regional providers and a few CREST International members with local offices. Some competition, but with no measure of quality of service for local providers.

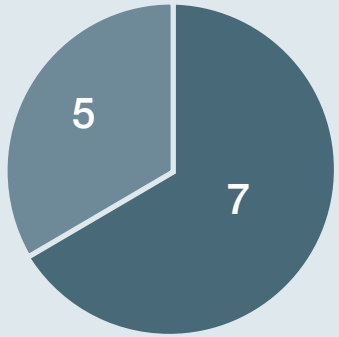
Cyber Threat Intelligence

71. Cyber Threat Intelligence (CTI) is information about current and future cyber threats and actors that adversly affect a nation's or individual organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks[107]. Threat Intelligence includes open source information and intelligence from technical, human, social media and dark web sources.

72. The research looked for companies providing cyber threat intelligence services to organisations in Bangladesh and where they were provided from. For the purposes of a robust cyber security environment, the ideal scenario is a host of Threat Intelligence service providers based in Bangladesh. Evidence of quality, through accreditions or partnerships, was also sought.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	3	7
Regional	0	0	0
International	0	5	5
Total	**4**	**8**	**12**

73.



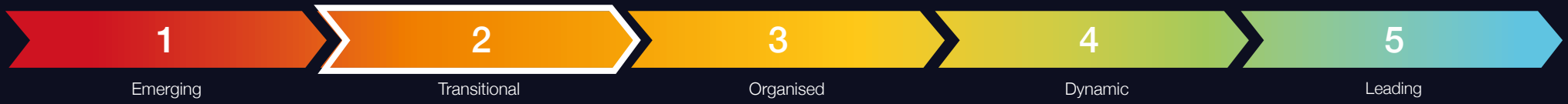
There are **twelve companies providing Cyber Threat Intelligence** services into Bangladesh, though only seven are Bangladesh located.

A majority (seven) are CREST accredited international organisations, three based in Bangladesh and four based elsewhere

It is not immediately clear how frequently cyber threat intelligence services of international organisations are being used. There is room for growth in the number of local Bangladesh companies offering cyber threat intelligence services.

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment Providers



Assessment – *Maturity Level 2*

Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

Vulnerability Assessment (VA)

74. Vulnerability Assessment (VA) is defined by CREST as: *"The examination of an information system or product to determine the adequacy of security measures; the identification of security deficiencies; to predict the effectiveness of the proposed security measures; and to confirm the adequacy of such measures after implementation*[108]*."* As with Threat Intelligence, research focused on looking for companies which provide VA services in Bangladesh, ideally based in Bangladesh.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	5	3	8
Regional	0	0	0
International	1	10	11
Total	**6**	**13**	**19**

75. CREST's research found **19 companies providing Vulnerability Assessment (VA)** services into Bangladesh. **Of the eight based in country, three are CREST accredited international organisations with offices in country.** Of the **11 international organisations offering their services into Bangladesh, it is unknown how often their services are being used.** There is room for growth in the number of local Bangladesh companies offering vulnerability assessment services.

Cyber Security Service Provision

Indicator 3.3 Penetration Testing Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

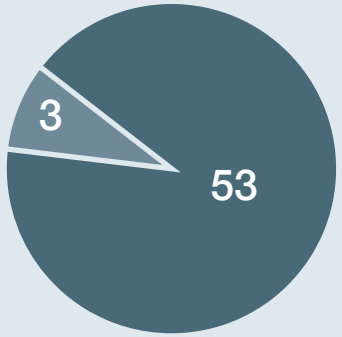
Penetration Testing

76. The UK's National Cyber Security Centre (NCSC) defines penetration testing as: *"A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might. Penetration testing should be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities*[109]*."*

77. CREST's research found significantly more companies providing penetration testing than any other cyber security service. But, as previously mentioned, many service providers deliver more than one cyber security service. In assessing the maturity of the cyber industry, efforts focused on looking for as many service providers based in Bangladesh as could be identified.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	7	3	10
Regional	0	29	29
International	0	24	24
Total	**7**	**56**	**63**

78. The research identified **63 companies providing Penetration Testing services into Bangladesh**. **Only ten were based in Bangladesh,** and **seven of those were Bangladeshi companies.**



Of the **CREST accredited companies, three are based in Bangladesh** and the others split between regional or international offices. **It is not known how often these regional or internationally based companies provide their services** to Bangladeshi clients.

Cyber Security Service Provision

Indicator 3.4 Security Operation Centre Providers

1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

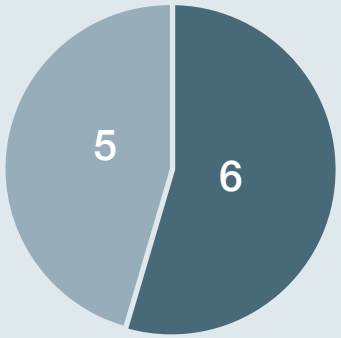
Security Operations Centres

79. **CREST provides a detailed definition of Security Operations Centres:** *"An Information Security Operations Centre (SOC) is a facility where enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. Depending on the nature of the SOC, organisations may offer a variety of services including monitoring, detection, threat hunting, log analysis, incident management, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance. A range of response options may be available, from telephone or email triage through to onsite assistance as required. Where such services are not available within the organisation, the SOC will know where and how to procure appropriate services from third parties[110]."*

80. Security Operations Centres are specialised, so provision of this service is only likely to come from well-established companies, operating in an active cyber security industry market.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	1	5
Regional	0	3	3
International	1	2	3
Total	**5**	**6**	**11**

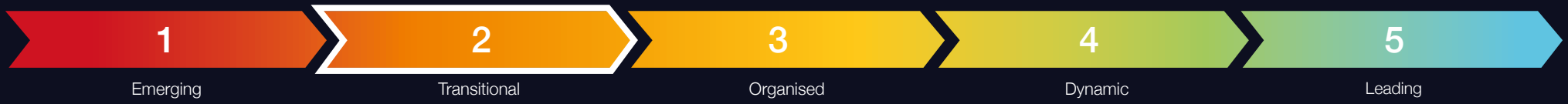
81. **Eleven companies provide SOC services into Bangladesh.** Five are based in country, the rest are regional or internationally based. The majority are CREST accredited international organisations. There is room to see growth in locally based companies in this area.



Of the **total of 11 SOC providers, 6 are CREST accredited companies.**

Cyber Security Service Provision

Indicator 3.5 Incident Response Providers



Assessment – *Maturity Level 2*
Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.

Incident Response Providers

82. **Incident response to a cyber security incident is defined by CREST as:** *"An information (or IT) security incident that could be classified as a cyber security incident, ranges from serious cyber security attacks on critical national infrastructure and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction*[111]*."*

83. Responding to a cyber incident is challenging, as many organisations will not have effective cyber security controls in place. Depending on their size, not all organisations will have a dedicated IT team with cyber security professionals employed in-house. Therefore, companies providing incident response services to clients are a vital component of the cyber industry and the fight against cybercrime. The number of Incident Response service providers based in country is critical to the overall cyber maturity of the cyber industry in that country.

84. Twenty-five companies were identified offering Incident Response services into Bangladesh. Nineteen were CREST accredited organisations, three of which with offices in Bangladesh.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	3	7
Regional	0	5	5
International	2	11	13
Total	**6**	**19**	**25**

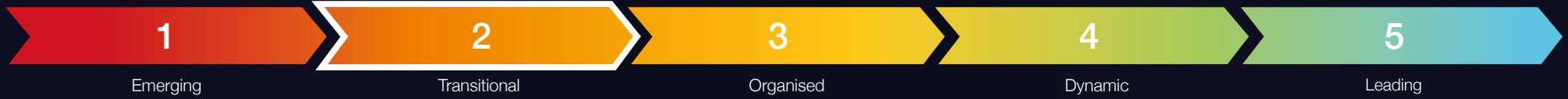
85. Of the four non-accredited IR service suppliers based in country, two are the BGD e-GOV CIRT[112] and the BdCERT[113], suspected to be inactive. One of the international organisations is FIRST[114].

Dimension 4

Cyber Security Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2*



86. Education and professional development are both critical in providing students with the skills and knowledge to thrive in the modern workplace. Without ICT and cyber security being taught in the national education system and then available as professional development, it is difficult to attract young people into the cyber security industry and to train as professionals.

    The continued pace of technological advancement and increased use of the internet generates an increase in threat from cybercriminals. Unprotected digital money is an easy target, and unprotected data is equally valuable. To combat the threat, a country needs a vibrant cyber security industry with well-trained professionals.

87. To determine the health of cyber security professional development, there is a need to identify which higher education establishments and professional training providers offer cyber security qualifications and certifications, and what qualifications and certifications are offered. CREST examined what (if any) professional membership organisations were undertaking in the country to improve the cyber profession. Researchers studied recruitment channels to identify advertised cyber security roles and cyber security freelancers promoting themselves, to ascertain the vibrancy of the cyber security job market.

88. In the recently published "Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041[115]," Chapter 9, 9.2, "The State of Progress Towards Innovation Economy," it provides a summary of Bangladesh's achievements under the previous Perspective Plan 2010-2021. Regarding human resources required for the ICT industry, the government has made progress in **increasing the number of trained IT professionals to 2 million by 2021**[116]. The government has also established 16 labs in universities and 10 IT Training and Incubation Centres at district level. The government also launched other projects and programmes to achieve the target, and [another] 20 specialised labs at universities are in progress[117]. It has also made ICT education at secondary school level compulsory[118].

    Achievements under the 2010-2021 Perspective Plan:

    - 2 — **2 Million** IT professionals by 2021
    - 16 — **16 established** university laboratories
    - 20 — **20 specialised university laboratories** in progress
    - 10 — **10 District level IT Training** and Incubation Centres

89. Vision 2041 also mention a 'a2i Innovation lab', a joint initiative of the Aspire to innovate (a2i) programme, ICT Division, Cabinet division, UNDP and the government's Ministry of Science and Technology. a2i states that it works to solve society's big problems by involving youth through emerging technologies[119]. The lab has been incubating more than 250 projects, and the Teachers Portal has brought together 403,507 teachers, allowing them to access 253,759 quality educational documents and tools. It also provides multimedia classrooms which have been of benefit to the education sector[120].

90. The Ministry of Education[121] has an ICT Master Plan for ICT in Education in Bangladesh (2012-2021) (not in English) and a Master Plan for ICT in Education in Bangladesh (2012-2021) Progress Review Report 2019 (in English)[122]. The Master Plan was written to meet the goals of Vision 2041[123].

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2* (continued)

Overall Assessment

91. While several of Bangladesh's universities and colleges offer computer science and ICT courses, very few offer specific cyber security degrees. Those that do are mainly at postgraduate level. CREST identified a small amount of cyber-related academic research also being undertaken.

92. In terms of professional development, there is a reasonable mix of online and classroom training available, but most providers only offer one or two courses. It is unclear how many courses lead to recognised certifications. This does not match the Government's Vision 2021 as summarised in the Vision 2041 document[124].

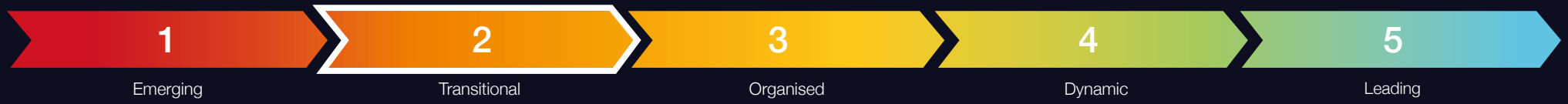
93. There is evidence of a few international professional bodies operating in Bangladesh, but this needs to be extended and strengthened if it is to support national aspirations to grow the number of cyber security professionals. There are occasional cyber-related conferences and exhibitions to support the professional community, but little evidence was found of any in-country cyber security specialist recruitment.

Development Approach

94. A first-class cyber security industry needs to be underpinned by expansion in cyber security education. Utilising international good practice, Bangladesh could build upon the existing computer science and ICT courses to support creation of more specific cyber security courses and qualifications.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education



Assessment – *Maturity Level 2*
In addition to computer science degrees, evidence of some cyber security degrees (BSc, MSc, and PhD) and some research.

Academia and Higher Education

95. Higher education takes place after secondary schooling, usually in further education colleges or universities. It aims to equip people with skills and qualifications needed in their future workplace or careers. Academia is the pursuit of research, higher level education and scholarship.

96. CREST's research sought to identify universities and colleges offering ICT or cyber courses and modules, and the level of these courses – diploma, degree, masters etc. The more students graduating with ICT- or cyber-related degrees, potentially results in more people following an ICT-related career.

97. According to Wikipedia, there are approximately:

104 104 **universities in Bangladesh,** a mix of public and private.

14 Of the public universities, **14 focus on STEM subjects,** there are **four engineering** universities and **one specialising in ICT education.**

5 Of the private universities, **14 focus on STEM or engineering subjects**[125].

This list was used as a guide during research.

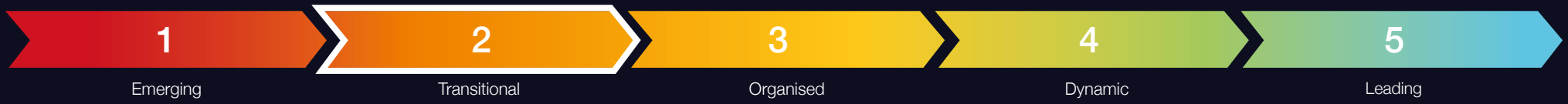
	Cert	Diploma	BA/ BSc	Pg Dip	MSc	PhD	Total
ICT Courses	8	41	2	7	17	9	67
Cyber Cources	3	3	0	2	2	1	9
Total	**11**	**44**	**2**	**9**	**19**	**10**	**76**

98. The table above shows the approximate numbers of courses offered from the **39 universities and colleges used as a sample for CREST's research.** Information on courses provided was taken from the institutions' websites. Where information was offered, it was not all shown in the same level of detail, so numbers are approximate.

99. Of the 39 universities used in research, **seven offered cyber related courses,** the rest were all universities that offered STEM subjects. The most popular level of courses remains at undergraduate level, with the majority offering BSc degrees in an ICT-related subject. It is positive to see so many ICT-related courses being offered and there is plenty of scope for increasing the number of cyber courses available to students.

Cyber Security Professional Development

Indicator 4.2 Training Providers



Assessment – *Maturity Level 2*

Remote (online) delivery of training supplemented with some regional instructor-led provision and a few local providers. No CREST International training provider members with local offices. Some competition but with no measure of quality of service.

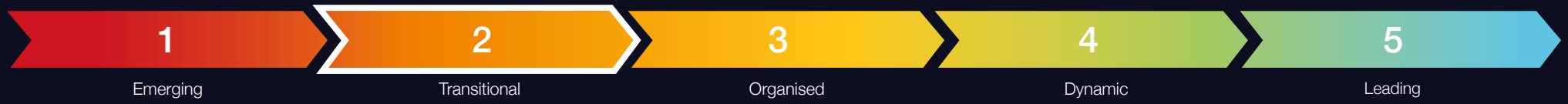
Training Providers

102. Training providers are qualified to provide training via an established course to clients in a particular subject matter area. CREST's research sought to identify the number of training providers in Bangladesh, where they were located and what cyber courses they provide.

103. **Thirteen training providers were found during research.** While the number of training providers is reasonably healthy, most providers are not exclusively focused on cyber security. Only a few offer in-country instructor-led training and it is not immediately clear how many courses lead to recognised certification.

Cyber Security Professional Development

Indicator 4.3 Professional Certifications



Assessment – *Maturity Level 2*
Some International Certification Bodies operate in country but take up is low. Some local institutions and professional associations in operation.

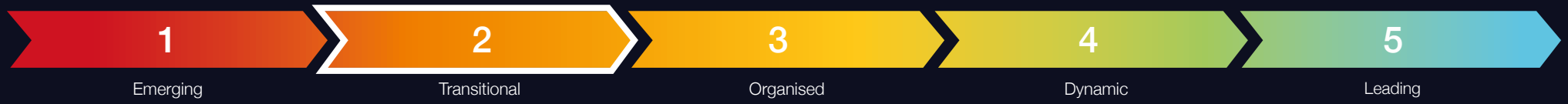
Professional Certifications

102. Professional certifications provide evidence of the holder's skills in that subject at the time of certification. In the cyber security industry, there is a multitude of different cyber certifications, delivered by a growing number of professional training providers. More detail of these training providers and the certifications they provide can be found in **Appendix C.**

103. **Fifteen professional certification bodies were found in Bangladesh during CREST's research.** Most offer certifications with online exams or through Pearson Vue or PSI test centres available in-country. Some certification bodies requiring practical exams offer this element online or through connection to a remote network. Some, (CREST and Cisco, for example) only offer exams at specific testing sites. It seems take-up of certifications is low in Bangladesh from the information gathered.

Cyber Security Professional Development

Indicator 4.4 Professional Cyber Membership Organisations



Assessment – *Maturity Level 2*

Some evidence of international cyber security membership bodies representing individuals and/or companies having local chapters/branches.

Professional Cyber Membership Organisations or Associations

104. Professional membership organisations or associations focus on furthering the profession they represent. They provide membership by subscription. Membership benefits include access to further professional development and training, access to discounted products and events, networking and collaboration with like-minded people, and increasing professional credibility as a result of membership. **These organisations are frequently not-for-profit.**

105. Several international professional membership organisations operate in the cyber security industry, some with chapters based in individual countries and regions. The existence of chapters in a country/region is direct evidence of an appetite for membership of that particular organisation, and indirect evidence of a more general appetite for community and professional ethos. CREST's research sought evidence of any professional cyber membership organisations operating in Bangladesh.

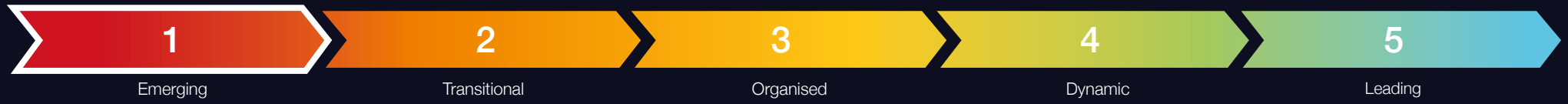
106. Certification body chapter involvement (if offered) is in initial stages, with only one fully fledged chapter in Dhaka (ISACA)[126] with active meetings and engagement, and one under development - the Cloud Security Alliance Bangladesh Chapter[127].

5 Overall, **five professional membership bodies were identified** as operating in Bangladesh.

The lack of cyber security professional membership organisations is in line with the lack of a specialist recruitment market and the apparently poor take-up of professional certifications. It does not match the government's ambitions to develop national cyber security capabilities.

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment



Assessment – *Maturity Level 1*
No evidence of in-country specialist cyber security recruitment.

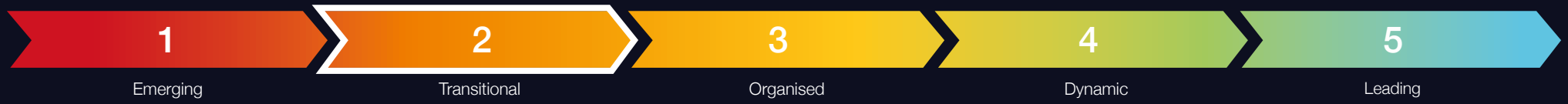
Specialist Cyber Recruitment

107. The presence and activity levels of recruitment companies and platforms provide evidence of how vibrant the job market is in a particular geographical area and/or industry sector. CREST's research looked for companies, online or with a physical in-country presence, that were either recruiting specifically for cyber security roles in Bangladesh, or marketed cyber qualified freelance professionals registered with them.

108. **Only three recruiting companies were found during research and none were specific to cyber-security.** There was little evidence of recruitment activity online, with a few mentions of EC-council and CompTIA certifications in job advertisements.

Cyber Security Professional Development

Indicator 4.6 Events & Exhibitions



Assessment – *Maturity Level 2*

Occasional cyber security events/exhibitions being run in-country, usually organised by an external entity.

Events and exhibitions

109. Events and exhibitions take a great deal of commitment, finances, advanced planning, and organisation to bring to life. There needs to be an appetite from the target audience to pay the ticket price and attend. CREST's research looked for any cyber or information security events held recently in Bangladesh, what level the events were and how frequently they were held. This provides evidence of the appetite for both cyber security knowledge and services in country. The impact of events can be far reaching as they are effective hubs for networking, collaboration, and information sharing, which helps sow seeds of cyber security inspiration.

110. At the time of CREST's research, **only eight public cybersecurity conferences/events were identified** as having taken place in Bangladesh, **all of which were infrequent.**

Dimension 5

Banking Sector Cyber Security Posture

Banking Sector Cyber Security Posture

Overall Dimension Assessment: *Maturity Level 2*

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

111. To assess the current cyber security posture of Bangladesh's banking sector, CREST commissioned a leading cyber threat intelligence service provider, Orpheus Cyber, to undertake passive (non-intrusive) external assessments of the public-facing IT infrastructure from a sample of financial institutions.

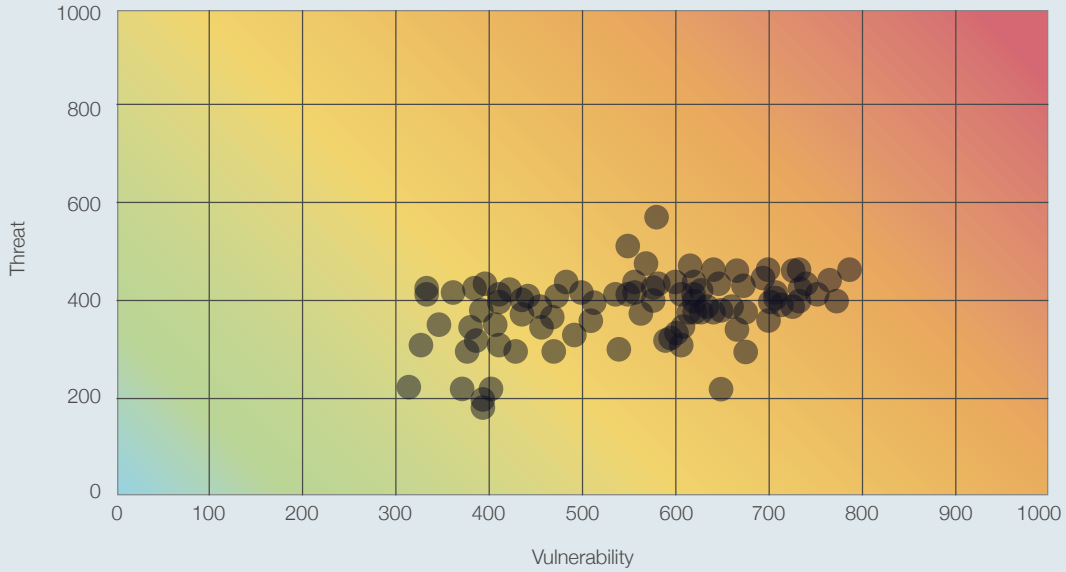
Its brief was to examine the cyber security risk rating of each financial institution against a series of non-intrusive metrics including:

- The presence of vulnerabilities on public-facing IT infrastructure
- The presence of open ports on internet-facing servers
- The adoption of anti-phishing mechanisms
- Availability of breached employee credentials on online forums and marketplaces.

112. Results of research into these four highlighted metrics are explained in more detail in Indicators **Indicators 5.2 to 5.5**. For each institution, results were fed into an Orpheus Cyber proprietary assessment tool to measure vulnerability against threat and determine comparative risk ratings. The anonymised results of the assessments have been plotted on a scatter diagram, right, where very low risk is bottom left and very high risk is top right. These results are covered in more detail in **Indicator 5.1.**

Comparative Risk Rating

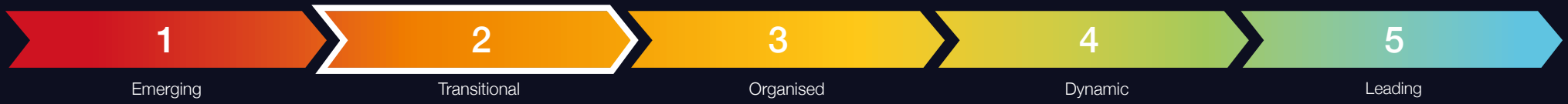
Figures represent CREST's cyber risk rating of each financial institution against a series of non-intrusive metrics



113. In determining the financial institutions to be assessed, the first source was the list of supervised institutions maintained by Bangladesh Bank[128] and the Microfinance Regulatory Authority[129]. This information was cross-checked against the membership list of Bangladesh Bankers Association[130], Wikipedia[131] and the websites of the financial institutions themselves, to generate a representative sample of national and international banks and microfinance institutions operating in Bangladesh. Many micro finance institutions did not appear to have websites. The website addresses and email domains of 95 financial institutions were passed to Orpheus Cyber for initial assessment. The results contained in this report relate to assessments undertaken on these institutions in October 2020. For ethical reasons, all results have been anonymised.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile



Assessment – *Maturity Level 2*
Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

Banking Sector Cyber Risk Profile

114. The totality of the cyber risk faced by individual financial institutions is formed by a complex array of threats and vulnerabilities. No modern-day organisation can be completely immune to cyber risk. The trick is to systematically address risks in terms of severity and impact – starting with highest risks. The same approach applies when taking a sectoral approach.

115. The scale that CREST uses for rating cyber risk ranges **between 0 (very lowest risk)** and **1000 (very highest risk)** and falls into **five different rating bands**:

Very Low	Low	Medium	High	Very High
(0 – 354)	(355 – 408)	(409 – 467)	(468 – 522)	(523 – 1000)

As visible in the scatter diagram on the previous page, assessed financial institutions have been found to have **individual vulnerability scores (X-axis) ranging between 310 and 784**. The **average cyber risk score** for the sample is **464**, which corresponds to a national average risk rating of '**Medium**'.

116. Note that no active (intrusive) assessment was undertaken, nor was any assessment made of IT infrastructure elements that are not internet-facing. If comprehensive assessment were made of entire IT infrastructures, internet-facing and otherwise, results may have differed. However, the levels of access that would have been required for such an undertaking are far beyond the scope of this report.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile (continued)

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

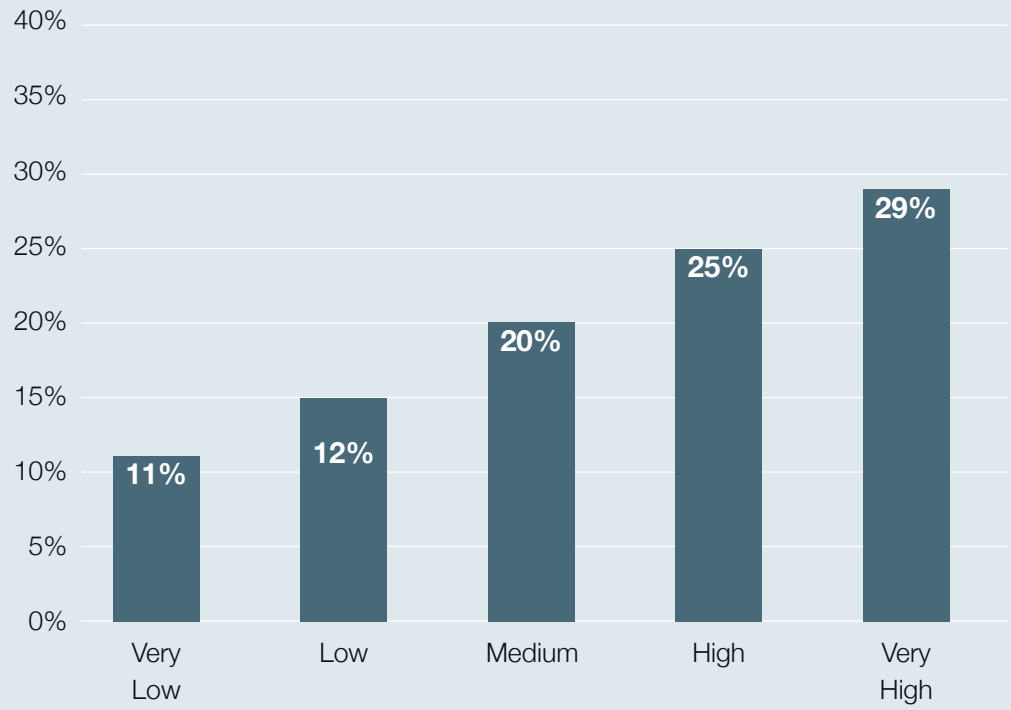
Assessment – *Maturity Level 2*

Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

For research purposes, the cyber risk rating of the public-facing infrastructure is considered sufficient to indicate the general security posture of the whole financial services sector. There appears to be significant room for improvement in the cyber security posture of many of the individual financial institutions, particularly in those with a 'High' or 'Very High' risk rating.

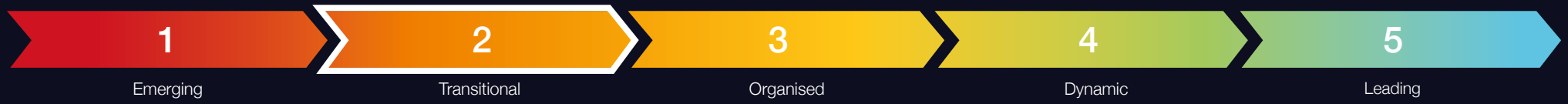
117. A breakdown by category of risk rating of the assessed sample of financial institutions is shown above, and results anonymised. Encouragingly, 23% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'. But 54% of the financial institutions have an overall cyber risk rating of 'Very High' or 'High'. Institutions in these latter two categories are not implementing good cyber hygiene practices and/or operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.

Breakdown of Bangladesh's Financial Institutions by Category of Risk Rating



Banking Sector Cyber Security Posture

Indicator 5.2 Infrastructure Vulnerability Risk



Assessment – *Maturity Level 2*

Infrastructure vulnerability risk is assessed as poor; 20% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 55% or fewer had any known vulnerabilities.

Infrastructure Vulnerability Risk

118. Software patching and other routine housekeeping activities are essential tasks which need to be carried out frequently and methodically to reduce opportunities for attackers. They are a good indicator of an organisation's enduring commitment to security.

    Ethically, research was limited to carrying out non-intrusive examinations of those infrastructure elements directly connected to the internet.

    Formally, the results are similarly constrained, but it is reasonable to assume results are typical of the state of patching across each financial institution's complete IT infrastructure.

119. Vulnerabilities, often referred to as CVEs (Common Vulnerabilities and Exposures)[132], are flaws in software and hardware that cybercriminals seek to exploit when attempting to gain access to the IT infrastructure of a chosen victim. To look for CVEs, they routinely scan portions of the internet. CREST's researchers followed a similar approach, scanning the public-facing IT infrastructure of all 95 of Bangladesh's financial institutions being assessed. By restricting themselves to passive reconnaissance, researchers were unable to confirm if the vulnerabilities they detected actually existed - there is a possibility that in some cases they were false positives.

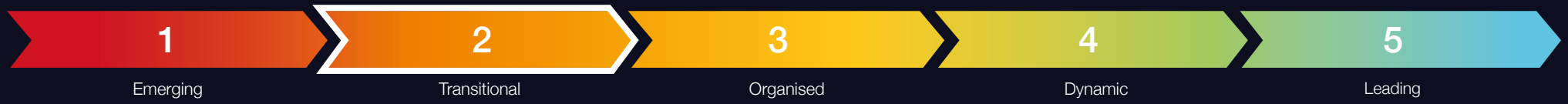
120. **The investigation revealed that 60% of Bangladesh's financial institutions appear to operate an unsecure internet-facing infrastructure, featuring at least one known vulnerability.** The vulnerabilities detected mostly have patches available, so their presence on an internet-facing infrastructure suggests lax patching practices.

121. Each CVE is analysed and assigned a severity score ranging from 0 to 10, with 10 being the most severe; this score is known by the acronym CVSS (Common Vulnerability Scoring System)[133]. Vulnerabilities with a score of 9 or more are classed as critical. Critical vulnerabilities are often prioritised by those with malicious intent because of the ease with which they can be exploited, or the access they provide when successfully exploited.

    CREST's research identified that 27% of Bangladesh's assessed financial institutions were operating internet-facing IT infrastructure with at least one critical vulnerability. In those financial institutions with critical vulnerabilities, these results are indicative of a failure to adopt an 'attacker's eye perspective' and prioritise critical CVEs for remediation.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk



Assessment – *Maturity Level 2*
Architecture & Access risk is poor. 40% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 40% or fewer were identified as having potential database vulnerabilities.

Architecture & Access Risk

122. Security architecture and access management are the most common means by which networks and information are secured. 'Security by design' is the essential foundation upon which all other cyber defences are built. Insufficient segregation between key assets and unguarded routes to gain unauthorised access are examples of gaps that can be exploited by attackers.

    Ethically, the researchers were limited to only examine those assets directly connected to the internet. Therefore, they only focused on the remote access and database ports of internet-facing servers as a simple indicator of the configuration management underpinning the network and, by inference, the likely approach to 'security by design.'

123. In the context of computer infrastructure, ports are gateways through which computers communicate with each other. By design, computer servers have multiple logical communication pathways, tailored to facilitate communications relating to a particular service. When a port is 'open,' the server can receive packets of data related to a particular service, when closed, it cannot. Certain ports need to be configured as 'open' to allow the server to perform its role. Traffic [data] going in and out of these ports can be guarded by mechanisms such as firewalls.

124. If a server is misconfigured and one or more ports are unintentionally left open and unguarded, then cybercriminals can potentially gain access and compromise the computer network. In the same way cybercriminals scan for CVEs (see **Indicator 5.2**), they routinely scan the internet to identify open ports, which they can then target to gain a foothold into the corporate network.

125.

- Cybercriminals frequently look to **scan ports associated with remote access services** – hardware and software that allow authorised users to remotely access a computer or a network from a distinct network connection.
- Cybercriminals favour **targeting remote access services** because, once compromised, they can easily move within a network and gain access to systems containing valuable information they can steal and/or encrypt.
- Certain specialised cybercriminals **target remote access services and gain access to bank networks,** with a view to selling-on this access in online criminal forums and marketplaces.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk (continued)

CREST's research shows just 8% of assessed financial institutions maintain at least one port associated with remote access services open to the internet.

126. In most cases, these ports are configured to accept incoming data packets from the internet for a valid business requirement and will have adequate security measures in place.

    Although banks with open remote access ports on their IT infrastructure remain susceptible to a potential compromise, they are a small subset. Evidence suggests Bangladesh's financial services sector is not highly vulnerable to the threat emanating from ports associated with remote access services.

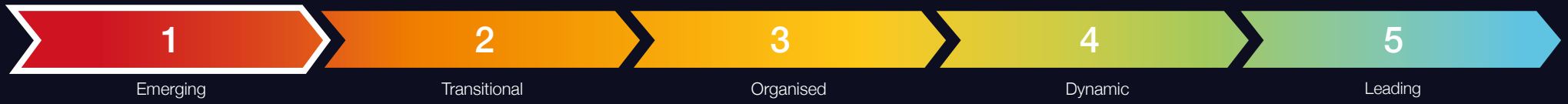
127. Another set of ports cybercriminals target are those used by database services. **CREST's research shows 33% of assessed financial institutions have at least one database-related port open on their public-facing infrastructure.** Although some of these internet-accessible database services are used for valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.

128. While remote access ports left open to the internet can allow cybercriminals to reach a bank's internal network and steal valuable information, exposed databases place customer data and other sensitive information at an even more direct and imminent risk. This is mostly because database services associated with the ports often lack authentication protocols by default, allowing unauthorised third parties to easily access and retrieve their content.

129. Understanding the threat associated with exposed database instances and reducing the possibility of suffering a data leak reduces the risk of committing an offence under the **2006 Technology Act**[134].

Banking Sector Cyber Security Posture

Indicator 5.4 Email Authentication Risk



Assessment – *Maturity Level 1*

Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

Email Authentication Risk

130. **Having an inherent susceptibility to social engineering and phishing campaigns is human nature.** While training and education can help prevent successful attacks, email authentication mechanisms can further reduce the threat. As an outside observer, it has not been possible to comment directly on staff training. But by passively detecting if email authentication mechanisms are in place, an indication of an organisation's commitment to reducing the effectiveness of phishing attacks and similar hazards can be inferred.

131. **Sender Policy Framework (SPF)** and **Domain-based Message Authentication, Reporting & Conformance (DMARC)** are example authentication mechanisms organisations can use to secure email traffic. They work together to ensure email domains are not used fraudulently, preventing the risk of spoofing, and helping block spam messages, malware, and phishing attempts.

132. SPF is regarded as the minimum (basic) standard to safeguard against spoofing and impersonation. DMARC is a more advanced security mechanism that, when correctly enabled, signals a strong cybersecurity posture. While it is still not as commonly implemented as SPF, recent global statistics confirm DMARC implementation rates are growing, with a corresponding decline in domain spoofing[135].

133. Having SPF and DMARC correctly enabled does not entirely negate the threat from phishing. However, it does reduce the chance of falling victim to impersonation attempts and **business email compromise (BEC) scams.** Both are threats that are common within the financial services sector[136].

134. In a BEC scam, cybercriminals target victims with spear-phishing emails devised to impersonate the company's CEO, an employee with the authority to approve money transfers, or a key supplier, for example. This aims to trick recipients into wiring funds to bank accounts under the cybercriminal's control or revealing highly sensitive information that could prove useful in further malicious operations. BEC scams continue proving highly profitable for cybercriminals. In its **2019 Internet Crime Report,** the FBI estimated BEC scams cost global business approximately **USD 1.8 billion**[137]**.**

135.

57%

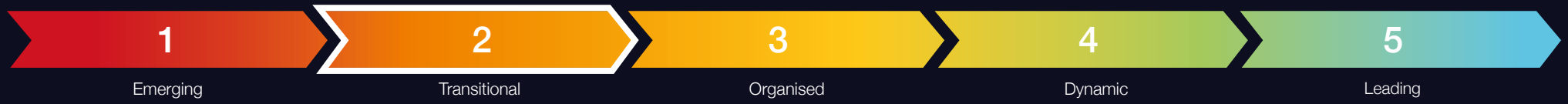
CREST's research revealed **57% of financial institutions sampled had not implemented basic email authentication measures (SPF)**.

79%

79% of the sample had not implemented advanced email authentication measures (DMARC). These results suggest there is still significant room for improving the financial service sector's defences against phishing and similar threats.

Banking Sector Cyber Security Posture

Indicator 5.5 Information Leakage Risk



Assessment – *Maturity Level 2*

Information leakage risk is assessed as poor; more than half of the surveyed financial institutions have had at least some employee credentials compromised in recent years by third-party breaches.

Information Leakage Risk

136. **The more sensitive information about an organisation is publicly available, the greater the risk of successful cyber-attacks.** Employees often expose information via social and professional platforms which may be openly viewed by cybercriminals as a starting point for crafting phishing attacks. Alternatively, cybercriminals often gain access to login credentials via the dark web because of third-party website hacks. While the level of information leakage via employee's use of social and professional platforms is hard to quantify, it is easier to spot instances of login credential exposure, and this is frequently used as a measure of the problem.

137. **Employees often use their work email address to sign-up for third-party websites** – both professional platforms and more leisure-oriented services. However, these platforms and services can expose users' sensitive information in data breaches caused by either malicious external compromise or internal negligence.

> **56%** CREST's research revealed **56% of assessed financial institutions had had at least some of their employees' credentials leaked online** after unconnected attacks on third-party website-based service providers.

138. As a minimum, **work email addresses have been exposed.** In the worst case, plaintext passwords and other log-in information disclosed via third-party breaches have the potential to allow cybercriminals to directly hijack employees' corporate accounts. Alternatively, leaked credentials may allow for more tailored and enhanced brute force attacks, providing adversaries with patterns and common combinations employees might follow when choosing passwords. Third party breaches could also lead to more sophisticated phishing efforts, with cybercriminals using exposed information to craft highly convincing malicious messages, luring recipients into providing access or revealing additional data.

139. It has not been possible to verify how many of the assessed financial institutions follow good hygiene practices and enforce strong password best practices – measures that help mitigate the threat associated with third-party leaked credentials.

However, the high percentage of financial institutions which have fallen victim to a third-party breach suggests the sector remains vulnerable to such threats.

Banking Sector Cyber Security Posture

Mitigation Measures

147. **Ethically, having identified potential vulnerabilities in the financial services sector, it is good practice to outline mitigation measures that, where appropriate and proportional, financial institutions should consider adopting, such as:**

Infrastructure Vulnerability

- Implement an effective patching and software update routine and ensure vulnerabilities of the highest severity and those that cybercriminals actively seek to identify and exploit are prioritised.
- Adopt an attacker's-eye perspective on your organisation to see which vulnerabilities could appear to potential adversaries.

Architecture & Access

- Review open server ports and assess whether there is a business requirement for them to be open. Close those that are not required.
- For those instances required to be internet accessible, ensure appropriate security settings, controls or authentication mechanisms are in place.

Email Authentication

- Create a Sender Policy Framework (SPF) record so it can be determined which IP addresses and hostnames are authorised to send emails from your domain.
- Implement a Domain Message Authentication, Reporting & Conformance (DMARC) policy to monitor and prevent any third parties from attempting to send emails on your behalf.

Information Leakage

- Educate employees on potential threats of using business email accounts on third-party services.
- Establish and enforce a strong password policy to reduce chances of password re-use.
- Implement additional security measures, such as multi-factor authentication.

Appendices

Appendix A

Glossary

Anti-phishing	Mechanisms and processes to defend against phishing attacks: see phishing
BEC	Business Email Compromise: a form of scam in which the cybercriminal seeks to obtain an unauthorised money transfer into an account which they control
CERT	Computer Emergency Response Team
CMAGE	Cyber Security Maturity Assessment for Global Ecosystems
CSIRT	Computer Security Incident Response Team
Dimension	The top-level partitioning of the cyber security ecosystem into five distinct areas of study: covers one or more Indicators to which metrics can be applied
DMARC	Domain-based Message Authentication, Reporting & Conformance: an advanced form of email authentication
Ecosystem	A description of the community of interacting elements which together describe the whole enterprise: in the context of this maturity model it consists of five Dimensions
Ethical Hacking	An alternative name for Penetration Testing: see PenTest
FIRST	Forum of Incident Response & Security Teams: an international association of CERTs/CSIRTs
Indicator	The lower-level partitioning of the cyber security ecosystem into manageable research topics for assessment purposes: one or more indicators build into Dimensions of the ecosystem
Information Exchange	A semi-formal mechanism for experts in different organisations to exchange information on observed cyber security threats, vulnerabilities and incidents
International (service provider)	A cyber security service provider headquartered elsewhere with offices in multiple countries which offers the service remotely or through a visiting employee
IR	Incident Response: a category of cyber security service
Local (service provider)	A cyber security service provider with one or more in-country office(s): company may additionally be classed as international, regional or locally registered
Locally registered (service provider)	A cyber security service provider which is registered and headquartered in the country
Malware	Malicious software intentionally designed to cause damage to a computer or network

Appendix A

Glossary (continued)

Multi-factor authentication	An automated process by which a user is granted access to hardware/software only after successfully presenting two or more pieces of evidence (factors) to an authentication mechanism
PenTest	Penetration Testing: a category of cyber security service in which a security tester carries out an authorised simulated attack on a system to evaluate security
Phishing	A process by which a cybercriminal attempts to obtain sensitive information, such as usernames, passwords and credit card details, by disguising themselves as trustworthy
Port	A physical or virtual connection to a computer server through which different categories of information or instructions are sent and received
Public-facing / Internet-facing	Those elements of a computer system software (and/or hardware) to which there is (paid or free) public access, often via an internet connect: distinct from those elements of a computer system which can only be accessed by authorised internal staff
Regional (service provider)	A cyber security service provider with an office in an adjacent country which offers the service remotely or through a visiting employee
Scam	A deceptive scheme or trick used to cheat an organisation or individual out of something, especially money
SPF	Sender Policy Framework; a basic form of email authentication
SOC	Security Operations Centre: a facility in which a team monitor an organisation's cyber security on an ongoing basis: facility can be in-house outsourced to a cyber security service provider
Spear-Phishing	A highly targeted attempt at phishing in which the cybercriminal often uses known information to add authenticity to a malicious communication
Spoofing	Masking the origin of a malicious email (or other communication) to trick the recipient into believing that it is genuine: used in support of a phishing attack
Third-party breach	Occurs when a cybercriminal uses a third-party system with a trusted connection to your system (typically a supplier) to indirectly gain access to your network or steals your data directly from a (trusted) third-party
TI	(Cyber) Threat Intelligence; a category of cyber security service
VA	Vulnerability Analysis; a category of cyber security service

Appendix B

Summary of Maturity Level Definitions

The comprehensive list of maturity level definitions for each indicator is as follows:

Indicator 1.1
Government Strategy & Policy

Level 5	Level 4	Level 3	Level 2	Level 1
A coordinated cyber security delivery programme underpinned by regular reviews of strategies and policies; across all aspects of the cyber security lifecycle - awareness, education, training, development, standards, risk management, incident response and law enforcement.	Active participation in cyber security implementation and policy development by key Government departments and regulatory bodies, including the Central Bank.	Evidence of substantive actions to implement strategies and policies aimed at improving the country's cyber security posture and/or capabilities.	Some evidence of up-to-date strategies and policies aimed at improving the country's cyber security posture and/or capabilities.	No evidence of up-to-date strategies or policies aimed at improving the country's cyber security posture and/or capabilities.

Indicator 1.2
Regulator/Government Operated Assurance Schemes

Level 5	Level 4	Level 3	Level 2	Level 1
Strong evidence of successful financial services assurance scheme in operation, leading to security improvements. Evidence of best practice also across other sectors.	Evidence of financial services assurance scheme in operation. Strong evidence of regulators operating in other sectors and strategy/policy being developed in respect of assurance schemes.	Strong evidence of good regulation of financial services sector. Evolving strategy/policy in respect of financial services assurance scheme. Some evidence of regulators operating in other sectors.	Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.	No regulator operated assurance schemes identified. Limited financial services regulation by Central Bank. Little evidence of regulators operating in other sectors.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 1.3
Law Enforcement & Cyber Defence Capabilities

Level 5	Level 4	Level 3	Level 2	Level 1
Broad spectrum of coordinated national responses to cybercrime - strategy, legal, reporting, investigation, international collaboration, awareness, education, technical measures. Credible and coordinated cyber defence posture.	National focus for reporting and specialist investigation of cybercrime. Significant investment in law enforcement and cyber defence capabilities. Strong public awareness campaigns. Widespread adoption of technical measures. Some evidence of regional/ international coordination. Strong intervention measures to divert potential cybercriminals into cyber security careers (e.g. Cyber Choices, Cyber First).	Good reporting and investigation of cybercrime. Heathy investment in law enforcement capabilities to counter cybercrime. Awareness of cybercrime within the business community and the public. Some adoption of technical measures. Some investment in cyber defence capabilities. Adoption of some intervention measures to divert potential cybercriminals into cyber security careers (e.g. Cyber Choices).	Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime and some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.	Little evidence of the reporting of cybercrime and its impact. Little evidence of law-enforcement capabilities to tackle cybercrime. Little evidence of public awareness. Little evidence of interest in cyber defence matters.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1
CERTs & Information Sharing

Level 5	Level 4	Level 3	Level 2	Level 1
Fully implemented information exchange arrangements in operation across all sectors. Meets ENISA CERT Maturity Model Tier 3 requirements (more details can be found at **https://www.enisa.europa.eu/publications/study-on-csirt-maturity).**	Evidence of sector-specific CERTs and information exchanges in operation.	Evidence that National CERT has international links (FIRST etc) and is following international standards. Meets ENISA CERT Maturity Model Tier 2 requirements.	National CERT established. Meets ENISA CERT Maturity Model Tier 1 requirements.	Limited evidence of cyber incident reporting or coordinated response.

Indicator 3.1
Threat Intelligence Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally/regionally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2
Vulnerability Assessment Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3
Penetration Testing Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers. Any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4
Security Operation Centre Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally/regionally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local/regional providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers; any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5
Incident Response Service providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (voluntary or self-sustaining) established with a mix of locally-registered members and international members with local offices. Strong local and international benchmarked provision of service with a self-sustaining industry representation.	Some locally-registered CREST member companies (invested or no CREST Chapter). Strong local and international benchmarked provision of service but not yet a self-sustaining industry representation.	No locally-registered CREST member companies, but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Some local providers and a few CREST International members with local offices. Some competition but with no measure of quality of service for local providers.	Virtually no providers; any that exist are likely to be small boutiques with no measure of quality. Market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1
Academia & Higher Education

Level 5	Level 4	Level 3	Level 2	Level 1
Professional bodies and government-influencing academia.	Wider academic engagement and outreach in the cyber security ecosystem.	Academia active in cyber security teaching and research. Significant local choice of cyber security degrees at BSc, MSc, and PhD. Apprenticeship (or similar) programmes available.	In addition to computer science degrees, evidence of some cyber security degrees (BSc, MSc, and PhD) and some research.	Limited evidence of an interest in cyber security within academia (teaching or research). Some computer science degrees available, but with little security content. Apprenticeship programmes not identified.

Indicator 4.2
Training Providers

Level 5	Level 4	Level 3	Level 2	Level 1
CREST Chapter (Voluntary or self-sustaining) established with locally-headquartered and international members. Strong local and international benchmarked provision of services with a self-sustaining industry representation.	Some locally-headquartered CREST member providers (invested or no CREST Chapter). Strong local and international benchmarked provision of services, but not yet a self-sustaining industry representation.	A good balance between online and local instructor-led training. No local/regional CREST training provider member companies, but strong presence from International CREST training provider member companies with local offices. There are in-country providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.	Remote (online) delivery of training supplemented with some regional instructor-led provision and a few local providers. No CREST International training provider members with local offices. Some competition but with no measure of quality of service.	Mainly remote (online) delivery with virtually no instructor-led in-country/regional provision. While there may a small number of providers, they are likely to be small boutiques with no measure of quality. The market is not mature enough for international businesses to be active.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3
Professional Certifications

Level 5	Level 4	Level 3	Level 2	Level 1
All International Certification Bodies operate in-country and take up is strong. Recruitment and access to government and regulated markets demand professional certifications.	All International Certification Bodies operate in-country and take up is strong. Recruitment and access to government and regulated markets does not actively utilise professional certifications.	Most International Certification Bodies (technical, management and audit) operate in-country; take-up is developing but would not be classed as strong.	Some International Certification Bodies operate in-country, but take-up is low. Some local institutions and professional associations in operation.	Virtually no professional certifications available or taken in-country; while there may a small number of certification bodies, take-up of certification is very low. The market may not be mature enough for international businesses to be active.

Indicator 4.4
Professional Cyber Membership Organisations

Level 5	Level 4	Level 3	Level 2	Level 1
Active membership organisation(s) for individuals and companies, setting professional standards and applying enforceable codes of conduct/ethics.	Active membership organisation(s) for individuals and companies, making significant contributions to in-country events and exhibitions.	Some evidence of local cyber security membership organisations for individuals and/or companies.	Some evidence of international cyber security membership bodies representing individuals and/or companies having local chapters/branches.	No evidence of local cyber security membership organisations or local chapters/ branches of international membership bodies.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5
Specialist Recruitment

Level 5	Level 4	Level 3	Level 2	Level 1
Active specialist cyber security recruitment market. Salary and other information made publicly available. CERIS-style association available.	Active general cyber security recruitment market from generic technology recruiters. Role and job description standards encouraged. NIST and CIISEC actively encouraged.	Evidence of organised cyber security recruitment. Evidence of recruitment outreach to academia and schools, talent-spotting initiatives, and growth in the market.	Some evidence of in-country cyber security recruitment.	No evidence of in-country cyber security recruitment.

Indicator 4.6
Events & Exhibitions

Level 5	Level 4	Level 3	Level 2	Level 1
An active programme of cyber security events and exhibitions attracting local and international audiences/speakers/exhibitors.	Regular locally-organised cyber security events and exhibitions being run in-country with mix of local/international speakers/exhibitors.	Evidence of regular locally-organised dedicated cyber security events and exhibitions being run in-country.	Occasional cyber security events and exhibitions being run in-country, usually organised by an external entity.	No evidence of cyber security events and exhibitions being run in-country.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1
Banking Sector Cyber Risk Profile

Level 5	Level 4	Level 3	Level 2	Level 1
Banking sector cyber risk profile is assessed as excellent; no surveyed financial institutions received a cyber risk rating of Very High and 10% or fewer received a rating of High.	Banking sector cyber risk profile is assessed as good. 5% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 25% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as average. 10% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 40% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as poor. 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.	Banking sector cyber risk profile is assessed as very poor. More than 30% of the surveyed financial institutions received a cyber risk rating of Very High and/or more than 55% received a rating of High or Very High.

Indicator 5.2
Infrastructure Vulnerability Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Infrastructure vulnerability risk is assessed as excellent. No surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 10% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as good. 5% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 25% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as average. 10% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 40% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as poor. 20% or fewer of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and 55% or fewer had any known vulnerabilities.	Infrastructure vulnerability risk is assessed as very poor. More than 20% of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and/or more than 55% had any known vulnerabilities.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3
Architecture & Access Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Architecture and Access risk is assessed as excellent. No financial institutions were identified as having potential remote access vulnerabilities and 5% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as good. 5% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 10% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as average. 10% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 20% or fewer were identified as having potential database vulnerabilities.	Architecture and Access risk is assessed as poor. 20% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 40% or fewer were identified as having potential database vulnerabilities.	Remote access and database risk is assessed as very poor. More than 20% of the financial institutions were identified as having potential remote access vulnerabilities and/or more than 40% were identified as having potential database vulnerabilities.

Indicator 5.4
Email Authentication Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Email authentication risk is assessed as excellent. All surveyed financial institutions have correctly enabled basic email authentication measures (SPF) and 10% or fewer had not yet enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as good; 5% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 25% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as average; 10% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 40% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as poor; 15% or fewer of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and 70% or fewer had not correctly enabled advanced email authentication measures (DMARC).	Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5
Information Leakage Risk

Level 5	Level 4	Level 3	Level 2	Level 1
Information leakage risk is assessed as excellent. 15% or fewer of the surveyed financial institutions had been identified as having had some employee credentials compromised in recent years by third-party breaches	Information leakage risk is assessed as good. 30% or fewer of the surveyed financial institutions had been identified as having had some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as average. Between 31% and 50% of the surveyed financial institutions are identified as having had some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as poor. More than half of the surveyed financial institutions have had at least some employee credentials compromised in recent years by third-party breaches.	Information leakage risk is assessed as very poor. More than 80% of the surveyed financial institutions have been identified as having had at least some employee credentials compromised in recent years by third-party breaches.

Appendix C

Professional Certifications and Member Organisations

Background

1. Knowledge, skills, and experience are factors used by companies to help determine who to hire or promote. They are also used by buyers in selecting service providers when award contracts. Experience is a matter of record, often underpinned by endorsements from previous employers or clients. In a mature marketplace, certifications are the common currency used to express an individual's knowledge and skills. Employers can quickly filter potential candidates by their certifications, while buyers can use certifications as a benchmark when looking to award contracts. The availability and use of certifications in both scenarios are a useful indicator of the maturity of a marketplace.

Career progression model

2. For ease of evaluation, cyber security certifications have been categorised into a career progression model using a five-tier hierarchy, denoting approximate skill level equivalence;
    - Foundation (New Entrant)
    - Practitioner (Intermediate)
    - Senior Practitioner (Subject Matter Expert/ Advanced)
    - Principle Advanced (Subject Matter Expert/Senior Management/Chartered)
    - Lead Practitioner (Fellow/Recognised Industry Expert)

    In some career progression models there are two tiers below Foundation (often referred to as the 'Transition Boundary' into the industry).

Certification bodies

3. During CREST's research, fifteen organisations were identified offering one or more certification of relevance to the cyber security profession. Together, they offer 142 different certifications, including 118 with differing degrees of technical content (grouped as 'Technical Certificates of Relevance') and 24 more focused on security management and other skillsets (grouped at 'Other Certificates of Relevance'). In some cases, certification organisations also act as professional membership organisations, holding events and contributing to members' career development.
4. Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres. Some certifications requiring practical exams offer this element online, or through connection to a remote network, although some bodies require physical testing sites, which have limited availability.
5. The certification bodies and individual certifications are shown in the following table by assessed tier level. Exam delivery options are also shown. For brevity, the abbreviation for each certification has been used. The full title of each certification and more details on the exam delivery options are shown on the awarding body's website (shown in the associated endnote in **Appendix F**).

Appendix C

Professional Certifications and Member Organisations (continued)

Certification Body	CERTIFICATION TIER					EXAM DELIVERY				
	Foundation	Practitioner	Senior Practitioner	Principle Advanced	Lead Practitioner	Online	Pearson Vue Centre	PSI Test Centre	Training Classroom	Specialist Test Centre
TECHNICAL CERTIFICATES OF RELEVANCE										
CREST[138]		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council[139]	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA[140]		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2[141]		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS[142]		GSEC GPEN GWAPT GICSP GCIP GCWN GCUX GAWN GPYC GWEB GCIH GCFE GASF GREM GCFA GNFA GSSP-Java GSSP-.Net GICSP GMOB GBFA GCSA	GXPN GCCC GSED GPPA GMON GCIA GRID GCDA GCTI GCED GPPA GDSA GDAT GEVA GNSA		GSE	✓	✓			
CompTIA[143]	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security[144]		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance[145]		CCSK				✓				

Appendix C

Professional Certifications and Member Organisations (continued)

Certification Body	CERTIFICATION TIER					EXAM DELIVERY				
	Foundation	Practitioner	Senior Practitioner	Principle Advanced	Lead Practitioner	Online	Pearson Vue Centre	PSI Test Centre	Training Classroom	Specialist Test Centre
TECHNICAL CERTIFICATES OF RELEVANCE										
PCI[146]		PCIP PCI-DSS QPA	PCI-DSS ISA PCI-DSS AQSA		PCI-DSS QSA PA-QSA PCI-DSS 3DS PCI-DSS P2PE PCI-DSS Secure Software Lifecycle Assessor PCI-DSS Secure Software Assessor PCI-DSS CPSA	✓	✓			
Cisco[147]		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft[148]	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services[149]	AWS Certified Security					✓	✓	✓		
OTHER CERTIFICATES OF RELEVANCE										
EC Council	CNDA CSCU			CCISO		✓	✓		✓	
ISACA		Cybersecurity Audit Scheme COBIT Program	CDPSE			✓		✓		
(ISC)2	Associate of (ISC)2						✓			
SANS	GISF	GLEG GSNA	GISP GCPM	GSLC	GSTRT	✓	✓			
IRCA (ISMS)[150]	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS[151]	CiSMP	BCM CIAA	CIRM				✓		✓	✓
IET[152]	ICTTech									✓

Appendix D

Country Context

Geography

1. Bangladesh is situated in Southeast Asia in the northeast of the Indian Sub-Continent. It is classed as a riverine country, as it lies in the delta region of the Padma (Ganges) and Jamuna (Brahmaputra) rivers. Bangladesh is surrounded by India to the east, north and west, by Myanmar to the southeast and south lies the Bay of Bengal[153].

Natural resources

2. Bangladesh's lack of large mineral resources has been cited as a major obstacle to economic development. Electricity is produced by thermal and hydroelectric processes.[154]

Population

3. In terms of population size, Bangladesh is ranked eighth in the world, with an estimated population of 168,472,00 as at 2020. The population projection for 2030 is 183,691,000. It is one of the most densely populated countries in the world with 1186.9 people per square km (as at 2018)[155].

4. According to the World Population Review, even though population growth has dropped - it now stands at 1% - the reasons for high population growth include low contraception use, high teenage fertility, and child marriage. Birth rate is 17.88 births per 1000 whilst the death rate is 4.8 deaths per 1000[156].

5. Most of the population as of 2018 was rural, with the split being 63.4% rural to 36.6% urban. Life expectancy (calculated in 2016) was male, 70.3 years, and female 72.9 years. The literacy rates of those over 15 was male 75.6%, female 69.9%[157].

Economy

6. According to the World Bank overview on Bangladesh[158], Bangladesh has made great progress in reducing poverty supported by sustained growth. Poverty has been reduced from 43.8% in 1991 to 14.8% in 2016, though there are still 39 million people living below the poverty line. Bangladesh reached lower middle-income country status in 2015 and is likely to graduate from the UN's Least Developed Countries (LDC) by 2024[159].

   Some of the challenges Bangladesh faces include creating better jobs for youth and removing barriers to higher investment, posed by low access to reliable affordable power, transport and infrastructure[160]. This is being addressed, with some of the ICT infrastructure achievements covered by Chapter 9 of Vision 2041[161].

7. In 2017 the GNI of Bangladesh was US$242,754 and per capita US$1,470[162].

Appendix D

Country Context (continued)

Internet connectivity

8. Bangladesh Government's Perspective Plan of Bangladesh 2021-2041, Vision 2041[163], Chapter 9, para 9.2, provides a summary of progress made since the Prospective Plan 2010-2021 was published. Regarding connectivity and internet penetration, Bangladesh has made great improvements, such as initiatives to build ICT infrastructure including a four-tier national data centre; establishing connectivity to rural areas of the country and connecting some of the remotest islands to mainstream digital services. 18,500 government offices have now been brought onto the same network connectivity[164].

9. Under the 'a2i' programme, a national web portal covering 46,500 government offices and 5,875 digital centres has been created, resulting in even the remotest villages receiving some online services. 503 million marginalized citizens received different public and private services from the digital centres. Since 2017, 8,500 post offices have been converted into post-e-centres where IT training is provided[165].

10. Digital payment infrastructure has been deployed nationally with agent banking services being provided through 3,958 digital centres to more than 1 million citizens[166].

11. Mobile penetration is above 84%, with 10% growth per annum. The number of active mobile subscribers in Bangladesh is in the region of 130 million. The number of internet users is nearly 70 million. Bangladesh is one of only 12 countries in the world that has more than 100million active subscribers[167].

Cyber crime

12. A 2015 online article by BDG e-GOV CIRT states that Bangladesh is one of the most vulnerable countries in cyberspace - with 80% of users becoming victims of spam attacks. The article describes several attacks on financial organisations, including the theft of US$81m from Bangladesh Bank by hackers[168].

13. BDG e-GOV CIRT's website shows registered incidents. In 2020, there were 1154 incidents registered and in 2019 there were 910. The most common incidents were malicious code (41.2% of incidents) followed by information gathering at 37.6%[169].

14. A 2019 Dhaka Tribune article states a 3% conviction rate for cybercrime - which translates to just 15 out of 495 cases being proven in court. The absence of successful convictions against cybercriminals is attributed to a lack of skilled lawyers, out of court settlements and the inexperience of law enforcement in handling cybercrimes.

    The article states that in 2018 the lone cyber tribunal (in Dhaka) received 925 cybercrime cases in 2018. In the first two months of 2019, 130 cases had been submitted[170]. This is evidence of cybercrime increasing - or an increase in cybercrimes being reported.

Appendix D

Country Context (continued)

15. A Dhaka Tribune article dated December 7, 2020, reported the global cost of cybercrime as being US$1trillion - a 50% increase since 2018[171]. Another article dated January 3, 2021, reports on a speech by Bangladesh 's Prime Minister, delivered during a police force passing out parade, where she acknowledged cybercrime as a global phenomenon, urging the police to cut cybercrimes and drug abuse. She also called upon the police to gain the confidence, trust, and love of the people - as you can only reduce crime with the help of the people; to serve the people with honesty, dedication, moral values, and discipline, and to learn how to honour[172]. Both articles show cybercrime is very much in focus in Bangladesh, as is a desire to improve the national capability to cope with it.
16. According to the USA's Overseas Security Advisory Council (OSAC), financial scams are one of the major criminal activities in Dhaka, alongside mugging, burglary and petty drugs, although credit card and ATM fraud are low[173].

Cyber Security Professional Development

17. According to the Vision 2041 plan, the government has been making progress in materialising Digital Bangladesh. At the time the report was compiled, the Bangladesh ICT Industry was valued at around $700m USD[174]. The government is developing high tech parks which will become specialised economic zones and a lifeline for the ICT sector. There will also be other parks established within 12 districts.
18. Regarding human resources for the ICT sector, the government states it is making progress in developing trained professionals, with the aim of creating two million trained IT professionals by 2021[175]. The government has made ICT education at secondary level school compulsory and established multiple ICT labs in numerous universities. It supports innovation to ICT start-ups with funding and mentorship. To facilitate this, the government established an Innovation Design and Entrepreneurship Academy (iDEA) under the ICT Division[176].

Other maturity models

19. The Oxford University's Global Cyber Security Capacity Centre (GCSCC) conducted a CMM review of Bangladesh in 2018[177].
20. In the National Cyber Security Index (2020), Bangladesh is 68th on the National Index and 147th on the ICT Development Index[178]. According to their indicators the highest scoring areas are Incident response (83%), the police (78%), and e-identification and trust services (67%). Education and Professional Development scored 44%, while Cyber Security Policy development stood at a figure of 43%[179].

Appendix E

Bibliography

This Bibliography is the list of all articles and the main websites accessed for qualitative research. Some references will also be listed in the endnotes where specific information had been used in writing this report. Details of individual websites of the numerous organisations accessed during the initial stages of quantitative research for each individual dimension and indicator is held seperately, and can be made available upon request to CREST.

AFP (2020). Cybercrime Cost to top $1tn this year. *Dhaka Tribune 7th Dec 2020.* **https://www.dhakatribune.com/world/2020/12/07/cybercrime-costs-to-top-1tn-this-year** (accessed Mar 21)

Asia Pacific Computer Emergency Response Team. (APCERT), (2021). *Members. (online)* **http://www.apcert.org/about/structure/members.html** (accessed Aug 20 and Mar 21)

Bangladesh Computer Council (BCC) (2021). Bangladesh: *ICT Division, MoPTIT, Government of Bangladesh.* **https://bcc.gov.bd/site/page/01cbf22a-b9f5-4a67-829e-55c27ab216f6/Overview** (accessed Aug 20 and Mar 21)

Bangladesh Government e-Government CIRT (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

Bangladesh Government e-Government Computer Incident Response Team (BDG e-GOV CIRT) (2015). Common Vulnerabilities in Cyber Space of Bangladesh. *Author* **https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/** (accessed Mar 21)

Bangladesh e-Government CIRT (BDG e-GOV CIRT) (2021). Incident Reporting Statistics. **https://www.cirt.gov.bd/incident-reporting/statistics/** (accessed Mar 21)

Bangladesh Government e-Government Computer Incident Response Team. (BGD e-GOV CIRT) (2021). Digital Forensics Lab. (online) **https://www.cirt.gov.bd/digital-forensic-lab/** (accessed Mar 21)

Bangladesh Bank, (2021). **https://www.bb.org.bd/en/** (accessed Aug 20 and Mar 21)

Bangladesh Bank. (2015). Guidelines on ICT Security for Banks and Non- Bank Financial Institutions V3 May 2015. Bangladesh: *Author (online)* **https://www.cirt.gov.bd/wp-content/uploads/2019/11/guideline_v3_ict1.pdf** (accessed Aug 20 and Mar 21)

Bangladesh Post (2020). BGD e-GOV CIRT arranging a Cyber Drill for Financial Institutions (22 Oct 2020). Bangladesh: *Author (online)* **https://bangladeshpost.net/posts/bgd-e-gov-cirt-is-arranging-a-cyber-drill-for-financial-institutions-on-22-october-2020-45256** (accessed Mar 21)

Bank of England and CBEST, CBEST Intelligence Led Testing, Understanding Cyber Threat Intelligence Operations, V2, UK, *Bank of England, 2016,* **https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf** (accessed Nov 2020)

Bayers, Abdul (2019). Vision 2041: Institution Matters. Dhaka Bangladesh: *The Financial Express (6th Sep 2019) (Online)* **https://thefinancialexpress.com.bd/views/vision-2041-institution-matters-1567786054** (accessed Mar 21)

BDNewsNet (2018). Directorate General of Forces Intelligence (DGFI). Bangladesh: **https://bdnewsnet.com/wiki/dgfi/** (accessed Mar 21)

BSS (2021). PM Asks Police to Check Cybercrimes, Drug Abuse. *Dhaka Tribune 3rd Jan 2021.* **https://www.dhakatribune.com/bangladesh/2021/01/03/pm-asks-police-to-check-cybercrimes-drug-abuse** (accessed Mar 21)

Appendix E

Bibliography (continued)

Click ITTEFAQ (2016). DMPs Special Counter Terrorism Unit to start functioning in February (15th Jan 2016). Dhaka, Bangladesh: *The Daily ITTEFAQ.* **https://web.archive.org/web/20190812185650/https://www.clickittefaq.com/dmps-special-counter-terrorism-unit-to-start-functioning-in-february/** (accessed Mar 21)

CREST, UK, **https://www.crest-approved.org/** (accessed Nov 2020)

CREST, 'Cyber Security Incident Response Guide V1', 2013, UK, *Author,* **https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf** (accessed Nov 2020)

Criminal Investigation Department (CID) Bangladesh Police. Cyber Crime Centre (CPC). **https://cid.gov.bd/page/ctc** (accessed Mar 21)

Criminal Investigation Department (CID) Bangladesh Police. IT Forensic. **https://cid.gov.bd/page/it-forensic** (accessed Mar 21)

Cyber Crime Investigation Division, Counter Terrorism and Transnational Crime (CTTC), Dhaka Metropolitan Police (DMP), (2021) Facebook Profile Page. Available at **https://www.facebook.com/cyberctdmp/** (accessed Mar 21)

Cyber Police Centre (CPC), Criminal Investigation Department (CID), Bangladesh Police, (2021). Facebook Page. Available at **https://www.facebook.com/pg/cpccidbdpolice/about/** (accessed Mar 21)

Cyber Security Intelligence (2021). National Cyber Security – Bangladesh. UK: *Author. (online)* **https://www.cybersecurityintelligence.com/category/national-cyber-security/location/bangladesh/** (accessed Mar 21)

Dhaka Metropolitan Police. Units; Counter Terrorism; Counter Terrorism and Transnational Crime (CTTC). Bangladesh. **https://dmp.gov.bd/units/** (accessed Aug 20 and Mar 21)

Digital Security Agency, (2020). Bangladesh: ICT Division, MoPTIT, Government of Bangladesh. **https://dsa.gov.bd/** (accessed Mar 21)

European Union Agency for Network and Information Security (ENISA), 'ENISA CSIRT Maturity Assessment Model,' 30 April 2019, *Author.* **https://www.enisa.europa.eu/publications/study-on-csirt-maturity** (Accessed 4 Nov 2020)

Financial Reporting Council (FRC) Bangladesh. **https://www.frcbd.org/** (accessed Mar 21)

Forum of Incident and Security Teams (FIRST). (2020) Members FIRST Teams. (online) **https://www.first.org/members/teams/** (accessed Aug 20 and Mar 21)

General Economics Division (GED), Government of Bangladesh (2012). Perspective Plan of Bangladesh 2010-2021 – Making Vision 2021 a Reality. Dhaka, Bangladesh: *Author (online)* **https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/page/6dca6a2a_9857_4656_bce6_139584b7f160/Perspective-Plan-of-Bangladesh.pdf** (accessed Mar 21)

General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

Global Cyber Security Capacity Centre (2018). Cyber Security Capacity Review of Bangladesh (2018). Oxford: *Author and BGD e-GOV CIRT. (online)* **https://www.cirt.gov.bd/cmm-bangladesh-report/** (accessed Mar 21).

Goswami, Suparna (2020). Bangladesh to Launch CERT-Fin. Bangladesh: *Bank Info Security 13th May 2020 (online).* **https://www.bankinfosecurity.asia/bangladesh-to-launch-cert-fin-a-14272** (accessed Aug 20 and Mar 21)

Appendix E

Bibliography (continued)

Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018.
Bangladesh: *Author (2018).*
https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf
(accessed Aug 20 and Mar 21)

Government of Bangladesh (2020). National Strategy for Artificial Intelligence Bangladesh 2020.
Bangladesh Computer Council (online).
https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-16-17-08-66d778e039591e0aa7302996e47f7216.pdf (accessed Mar 21)

Government of Bangladesh, Information and Communication Technology Division (2020). National Blockchain Strategy, A Pathway to be a Blockchain-enabled Nation March 2020.
Bangladesh: *Author. (online).*
https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf (accessed Mar 21)

Government of Bangladesh, (2020). Digital Security Rules 2020.
Bangladesh: *Bangladesh Computer Council. (online).*
https://bcc.gov.bd/site/page/0723616e-dbb2-41fb-ab2d-49bdac25557f/- (accessed Mar 21)

Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020.
Bangladesh: *Author. (online).*
https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf
(accessed Mar 21)

Government of Bangladesh, Information and Communication Technology Division (2018). National ICT Policy 2018.
Bangladesh: *Author (online)*
https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/31ac714d_80cc_4ba7_9fa2_5030077bafb1//National%20ICT%20Policy-2018.pdf
(accessed Mar 21)

Government of Bangladesh, Information and Communication Technology Division (2020). National Strategy for Robotics September 2020.
Bangladesh: *Author (online)*
https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/588ddd53_acaa_4214_ae01_b1f398687f2f/2020-09-21-16-29-38a296c7a172e5e673860983d18da7e2.pdf
(accessed Mar 21)

Information and Communications Technology Division of MoPTIT, (2021). History and Main Function.
Bangladesh: *Author (online)*
https://ictd.gov.bd/site/page/ab439356-145f-4759-942d-39ea506ff144/History-&-Main-Function
(accessed Aug 20 and Mar 21)

ilab (2020).
Bangladesh: *Aspire to Innovate.*
https://ilab.gov.bd/ (accessed Mar 21)

International Financial Reporting Standards (IFRS). Bangladesh.
UK: *Author (online)*
https://www.ifrs.org/use-around-the-world/use-of-ifrs-standards-by-jurisdiction/view-jurisdiction/bangladesh/ (accessed Mar 21)

ISACA Dhaka Chapter.
https://engage.isaca.org/dhakachapter/home
(accessed Mar 21)

International Financial Reporting Standards (IFRS), (2020). IFRS Application Around the World, Jurisdictional Profile: Bangladesh.
UK: *Author (online) p2-4.*
https://cdn.ifrs.org/-/media/feature/around-the-world/jurisdiction-profiles/bangladesh-ifrs-profile.pdf
(accessed Mar 21)

Kamrul Hasan (2019). Digital Agency Formed.
Bangladesh: *Dhaka Tribune. (online)*
https://www.dhakatribune.com/bangladesh/event/2019/07/11/digital-security-agency-formed
(accessed Mar 21)

Appendix E

Bibliography (continued)

Korea International Cooperation Agency (KOICA). **https://www.koica.go.kr/sites/koica_kr/index.do** (accessed Mar 21)

Ministry of Education, Government of Bangladesh (2020) **https://moedu.gov.bd/** (accessed Mar 21)

Ministry of Education, Government of Bangladesh (2019). Master Plan for ICT in Education in Bangladesh (2012-2021) Progress Review Report 2019. Bangladesh: *Author (online)* **https://moedu.gov.bd/sites/default/files/files/moedu.portal.gov.bd/page/ecea56df_b1bc_4707_bc8d_b99dbc08d8b9/f85661d36608b82ef945518a9ecb3b85.pdf** (accessed Mar 21)

Ministry of Posts Telecommunications & Information Technology (MoPTIT). (2021) Bangladesh: *Government of Bangladesh (online)* **https://ptd.gov.bd/** (accessed Aug and Mar 21)

National Cyber Security Centre (NCSC), *Author,* UK, **https://www.ncsc.gov.uk/** (accessed Nov 2020)

National Cyber Security Index, National Cyber Security Index 2018 - Bangladesh. Estonia, *e-Governance Academy, 2018,* **https://ncsi.ega.ee/country/bd/** (accessed Mar 21)

Organisation of Islamic Cooperation-CERT (OIC-CERT), (2021) Members. (online) **https://www.oic-cert.org/en/allmembers.html#.YDVwYWj7RPY** (accessed Mar 21)

Overseas Security Advisory Council (OSAC) (2020), Bangladesh 2020 Crime and Safety Report. USA: *Author* **https://www.osac.gov/Country/Bangladesh/Content/Detail/Report/a842f414-00f0-43c7-8443-188c64d5b5ef** (accessed Mar 21)

The Asian Age (2016). DMP's Counter- Terrorism Unit headed by Monirul (18th Feb 2016). Dhaka Bangladesh: *Author (online).* **https://dailyasianage.com/news/11220/dmps-counter-terrorism-unit-headed-by-monirul** (accessed Mar 21)

The National Cyber Security Strategy (2014). Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf**

The World Bank, (2020). The World Bank in Bangladesh, Economic Overview. *Author,* 14th October 2020, **https://www.worldbank.org/en/country/bangladesh** (accessed Mar 21)

Tipu, Md Sanaul Islam (2019). 3% Conviction Rate of Cybercrime in Bangladesh. Dhaka Tribune. **https://www.dhakatribune.com/cybersecurity/2019/04/20/3-conviction-rate-of-cybercrime-in-bangladesh** (accessed Aug 20 and Mar 21)

UNIDIR (2021) Cyber Security Policy Portal – Bangladesh. Switzerland: *Author (online)* **https://unidir.org/cpp/en/states/bangladesh** (accessed Mar 21)

Wikipedia, (2021) List of Universities in Bangladesh **https://en.wikipedia.org/wiki/List_of_universities_in_Bangladesh** (accessed Mar 21)

World Population Review, (2021) Bangladesh Population 2021. *Author.* **https://worldpopulationreview.com/countries/bangladesh-population** (accessed Mar 21)

Appendix F

Endnotes

Endnotes have been used to reference specific information instead of footnotes to prevent the sheer quantity of references from interrupting the report flow. If you are reading this electronically, endnotes can be read without flipping to this Appendix. By rolling over the endnote number within the text, the reference will then appear.

1. Further information available on the Bill & Melinda Gates Foundation, Financial Services for the Poor programme website, **https://www.gatesfoundation.org/What-We-Do/Global-Growth-and-Opportunity/Financial-Services-for-the-Poor** (accessed 29 Oct 2020)

2. Further information available on the CREST International website, **https://crest-approved.org/** (accessed 29 Oct 2020)

3. Further information available on the Orpheus Cyber website, **https://orpheus-cyber.com/** (accessed 29 Oct 2020)

4. General Economics Division, Government of Bangladesh (2012). Perspective Plan of Bangladesh 2010-2021 – Making Vision 2021 a Reality. Bangladesh: *Author (online)* Chapter 7 pp54-57 **https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/page/6dca6a2a_9857_4656_bce6_139584b7f160/Perspective-Plan-of-Bangladesh.pdf** (accessed Mar 21)

5. General Economics Division, Government of Bangladesh (2012). Perspective Plan of Bangladesh 2010-2021 – Making Vision 2021 a Reality. Bangladesh: *Author (online)* Chapter 7 pp54-57 **https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/page/6dca6a2a_9857_4656_bce6_139584b7f160/Perspective-Plan-of-Bangladesh.pdf** (accessed Mar 21)

6. Bayers, Abdul (2019). Vision 2041: Institution Matters. Dhaka Bangladesh: *The Financial Express (6th Sep 2019) (Online)* **https://thefinancialexpress.com.bd/views/vision-2041-institution-matters-1567786054** (accessed Mar 21)

7. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

8. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041, Executive Summary. Dhaka, Bangladesh: *Author (online) ppi.* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

9. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, 9.2 pp150. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

10. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Annex 9 pp163-166. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

11. Ministry of Posts Telecommunications & Information Technology (MoPTIT). (2021) Bangladesh: *Government of Bangladesh* (online) **https://ptd.gov.bd/** (accessed Aug and Mar 21)

12. Information and Communications Technology Division of MoPTIT, (2021). History and Main Function. Bangladesh: *Author (online)* **https://ictd.gov.bd/site/page/ab439356-145f-4759-942d-39ea506ff144/History-&-Main-Function** (accessed Aug 20 and Mar 21)

13. Bangladesh Computer Council (BCC) (2021). Bangladesh: *ICT Division, MoPTIT, Government of Bangladesh* **https://bcc.gov.bd/site/page/01cbf22a-b9f5-4a67-829e-55c27ab216f6/Overview** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

14. Kamrul Hasan (2019). Digital Agency Formed. Bangladesh: *Dhaka Tribune. (online)* **https://www.dhakatribune.com/bangladesh/event/2019/07/11/digital-security-agency-formed** (accessed Mar 21)

15. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* Ch IV Paras 12-14. **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

16. Digital Security Agency, (2020). Bangladesh: *ICT Division, MoPTIT, Government of Bangladesh.* **https://dsa.gov.bd/** (accessed Mar 21)

17. The National Cyber Security Strategy (2014). Priority 3: Organisational Structures. Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

18. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* Ch IV Paras 12-14. **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

19. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* Ch IV Paras 12-14. **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

20. UNIDIR (2021) Cyber Security Policy Portal – Bangladesh. Switzerland: *Author (online)* **https://unidir.org/cpp/en/states/bangladesh** (accessed Mar 21)

21. Global Cyber Security Capacity Centre (2018). Cyber Security Capacity Review of Bangladesh (2018). Bangladesh: *Author and BGD e-GOV CIRT. (online).* **https://www.cirt.gov.bd/cmm-bangladesh-report/** (accessed Mar 21)

22. Information and Communications Technology Division of MoPTIT, (2021). History and Main Function. Bangladesh: *Author (online)* **https://ictd.gov.bd/site/page/ab439356-145f-4759-942d-39ea506ff144/History-&-Main-Function** (accessed Aug 20 and Mar 21)

23. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

24. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System. Bangladesh: *Author (online).* **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

25. International Financial Reporting Standards (IFRS), (2020). IFRS Application Around the World, Jurisdictional Profile: Bangladesh. UK: *Author (online)* p2-4. **https://cdn.ifrs.org/-/media/feature/around-the-world/jurisdiction-profiles/bangladesh-ifrs-profile.pdf** (accessed Mar 21)

26. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

27. Bangladesh Computer Council (BCC) (2021). Bangladesh: *ICT Division, MoPTIT, Government of Bangladesh* **https://bcc.gov.bd/site/page/01cbf22a-b9f5-4a67-829e-55c27ab216f6/Overview** (accessed Aug 20 and Mar 21)

28. Ministry of Posts Telecommunications & Information Technology (MoPTIT). (2021) Bangladesh: *Government of Bangladesh (online)* **https://ptd.gov.bd/** (accessed Aug and Mar 21)

Appendix F

Endnotes (continued)

29. Government of Bangladesh, Bangladesh Computer Council (2020). Digital Security Rules 2020. Bangladesh: *Author. (online).* **https://bcc.gov.bd/site/page/0723616e-dbb2-41fb-ab2d-49bdac25557f/-** (accessed Mar 21)

30. Government of Bangladesh, Information and Communication Technology Division (2020). National Strategy for Robotics September 2020 Bangladesh: *Author (online)* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/588ddd53_acaa_4214_ae01_b1f398687f2f/2020-09-21-16-29-38a296c7a172e5e673860983d18da7e2.pdf** (accessed Mar 21)

31. Government of Bangladesh, Information and Communication Technology Division (2020). National Blockchain Strategy, A Pathway to be a Blockchain-enabled Nation March 2020. Bangladesh: *Author. (online).* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-03-391a6d9d1eb062836b440256cee34935.pdf** (accessed Mar 21)

32. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online).* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

33. Government of Bangladesh (2020). National Strategy for Artificial Intelligence Bangladesh 2020. *Bangladesh Computer Council (online).* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-16-17-08-66d778e039591e0aa7302996e47f7216.pdf** (accessed Mar 21)

34. Government of Bangladesh, Information and Communication Technology Division (2018). National ICT Policy 2018. Bangladesh: *Author (online)* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/31ac714d_80cc_4ba7_9fa2_5030077bafb1//National%20ICT%20Policy-2018.pdf** (accessed Mar 21)

35. The National Cyber Security Strategy (2014). Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

36. Bangladesh Bank. (2015). Guidelines on ICT Security for Banks and Non- Bank Financial Institutions V3 May 2015. Bangladesh: *Author (online)* **https://www.cirt.gov.bd/wp-content/uploads/2019/11/guideline_v3_ict1.pdf** (accessed Aug 20 and Mar 21)

37. Bangladesh Computer Council (BCC) (2021). Our Services – Cyber Security Related Service. Bangladesh. *Author* **https://bcc.gov.bd/site/page/01cbf22a-b9f5-4a67-829e-55c27ab216f6/Overview** (accessed Aug 20 and Mar 21)

38. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

39. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online).* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

40. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online)*. **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

41. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online)*. Ch1,1.4 pp5. **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

42. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online).* Ch1,1.4 pp5. **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

43. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online).* Ch3,3.3.1, pp9. **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

44. Government of Bangladesh, Information and Communications Technology Division (2020). National Internet of Things Strategy, Bangladesh March 2020. Bangladesh: *Author. (online).* Ch3,3.3.1, pp9. **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/bdb0a706_e674_4a40_a8a8_7cfccf7e9d9b//2020-10-19-15-04-9807d52e24da56e66f7ec89f7eb540ec.pdf** (accessed Mar 21)

45. General Economics Division, Government of Bangladesh (2012). Perspective Plan of Bangladesh 2010-2021 – Making Vision 2021 a Reality. Bangladesh: *Author (online)* Chapter 7 pp54-57 **https://bangladesh.gov.bd/sites/default/files/files/bangladesh.gov.bd/page/6dca6a2a_9857_4656_bce6_139584b7f160/Perspective-Plan-of-Bangladesh.pdf** (accessed Mar 21)

46. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

47. Government of Bangladesh, Information and Communication Technology Division (2018). National ICT Policy 2018. Bangladesh: *Author (online)* **https://bcc.portal.gov.bd/sites/default/files/files/bcc.portal.gov.bd/page/31ac714d_80cc_4ba7_9fa2_5030077bafb1//National%20ICT%20Policy-2018.pdf** (accessed Mar 21)

48. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9,9.2 pp148. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

49. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

50. BGD e-GOV CIRT (2021). Digital Forensics Lab. Bangladesh: *Author. (online)* **https://www.cirt.gov.bd/digital-forensic-lab/** (accessed Mar 21)

51. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

52. The National Cyber Security Strategy (2014). Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

53. The National Cyber Security Strategy (2014). Priority 1: Legal Measures; Action 2: Government Legal Authority. Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

54. The National Cyber Security Strategy (2014). Priority 2: Technical and Procedural Measures. Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

55. The National Cyber Security Strategy (2014). Priority 3: Organisational Structures. Bangladesh: *The Government of Bangladesh. (online)* **http://www.dpp.gov.bd/upload_file/gazettes/10041_41196.pdf** (accessed Mar 21)

56. Financial Reporting Council (FRC) Bangladesh. **https://www.frcbd.org/** (accessed Mar 21)

57. Financial Reporting Council (FRC) Bangladesh. Background. Bangladesh: *Author (online)* **https://www.frcbd.org/background/** (accessed Mar 21)

58. International Financial Reporting Standards (IFRS), (2020). IFRS Application Around the World, Jurisdictional Profile: Bangladesh. UK: *Author (online)* p2-4. **https://cdn.ifrs.org/-/media/feature/around-the-world/jurisdiction-profiles/bangladesh-ifrs-profile.pdf** (accessed Mar 21)

59. Bangladesh Bank, (2021). **https://www.bb.org.bd/en/** (accessed Aug 20 and Mar 21)

60. Bangladesh Bank. (2015). Guidelines on ICT Security for Banks and Non- Bank Financial Institutions V3 May 2015. Bangladesh: *Author (online)* **https://www.cirt.gov.bd/wp-content/uploads/2019/11/guideline_v3_ict1.pdf** (accessed Aug 20 and Mar 21)

61. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System. Bangladesh: *Author (online).* **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

62. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System; Review of Strategic Pan 2015-19. Bangladesh: *Author (online).* pp xiii-xv. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

63. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System; Strategic Goal 8. Bangladesh: *Author (online)*. pp32. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

64. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System, Strategic Goal 8. Bangladesh: *Author (online).* pp33-34. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

65. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System, Strategic Goal 8. Bangladesh: *Author (online).* pp34. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

66. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System, Strategic Goal 10. Bangladesh: *Author (online).* pp39. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

67. International Financial Reporting Standards (IFRS). Bangladesh. UK: *Author (online)* **https://www.ifrs.org/use-around-the-world/use-of-ifrs-standards-by-jurisdiction/bangladesh/#extent** (accessed Mar 21)

68. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System, Strategic Goal 10, Objective 10.1 and 10.2. Bangladesh: *Author (online)*. pp39. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

69. Goswami, Suparna (2020). Bangladesh to Launch CERT-Fin. Bangladesh: *Bank Info Security 13th May 2020* (online). **https://www.bankinfosecurity.asia/bangladesh-to-launch-cert-fin-a-14272** (accessed Aug 20 and Mar 21)

70. Dhaka Metropolitan Police. Units; Counter Terrorism; Counter Terrorism and Transnational Crime (CTTC). **https://dmp.gov.bd/units/** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

71. Click ITTEFAQ (2016). DMPs Special Counter Terrorism Unit to start functioning in February (15th Jan 2016). Dhaka, Bangladesh: *The Daily ITTEFAQ.* **https://web.archive.org/web/20190812185650/https://www.clickittefaq.com/dmps-special-counter-terrorism-unit-to-start-functioning-in-february/** (accessed Mar 21)

72. The Asian Age (2016). DMP's Counter- Terrorism Unit headed by Monirul (18th Feb 2016). Dhaka Bangladesh: *Author (online).* **https://dailyasianage.com/news/11220/dmps-counter-terrorism-unit-headed-by-monirul** (accessed Mar 21)

73. The Asian Age (2016). DMP's Counter- Terrorism Unit headed by Monirul (18th Feb 2016). Dhaka Bangladesh: *Author (online).* **https://dailyasianage.com/news/11220/dmps-counter-terrorism-unit-headed-by-monirul** (accessed Mar 21)

74. Dhaka Metropolitan Police, Counter Terrorism and Transnational Crime (CTTC), Cyber Crime Investigation Division (2021) Facebook Profile Page. **https://www.facebook.com/cyberctdmp/** (accessed Mar 21)

75. Korea International Cooperation Agency (KOICA). **https://www.koica.go.kr/sites/koica_kr/index.do** (accessed Mar 21)

76. Criminal Investigation Department (CID) Bangladesh Police. Cyber Crime Centre (CPC). **https://cid.gov.bd/page/ctc** (accessed Mar 21)

77. Criminal Investigation Department (CID) Bangladesh Police. IT Forensic. **https://www.cid.gov.bd/cid_it_forensic.php** (accessed Mar 21)

78. Criminal Investigation Department (CID) Bangladesh Police. IT Forensic. **https://www.cid.gov.bd/cid_it_forensic.php** (accessed Mar 21)

79. Criminal Investigation Department (CID) Bangladesh Police. Cyber Crime Centre (CPC). **https://www.cid.gov.bd/cid_cpc.php** (accessed Mar 21)

80. Criminal Investigation Department (CID) Bangladesh Police. Cyber Crime Centre (CPC). **https://www.cid.gov.bd/cid_cpc.php** (accessed Mar 21)

81. Cyber Police Centre (CPC), Criminal Investigation Department, Bangladesh Police, (2021). Facebook Page. Available at **https://www.facebook.com/pg/cpccidbdpolice/about/** (accessed Mar 21)

82. Cyber Police Centre (CPC), Criminal Investigation Department, Bangladesh Police, (2021) Facebook Page. Available at **https://www.facebook.com/pg/cpccidbdpolice/about/** (accessed Mar 21)

83. BDNewsNet (2018). Directorate General of Forces Intelligence (DGFI). Bangladesh: **https://bdnewsnet.com/wiki/dgfi/** (accessed Mar 21)

84. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* Ch IV Paras 12-14. **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

85. Government of Bangladesh (2018). Digital Security Act 2018, Act No. XLVI of 2018. Bangladesh: *Author (2018).* **https://www.cirt.gov.bd/wp-content/uploads/2020/02/Digital-Security-Act-2020.pdf** (accessed Aug 20 and Mar 21)

86. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

87. Bangladesh Computer Emergency Response Team (bdCERT), (2014). Bangladesh. **http://www.bdcert.org/about_bdcert.html** (accessed Mar 21)

88. Goswami, Suparna (2020). Bangladesh to Launch CERT-Fin. Bangladesh: *Bank Info Security 13th May 2020 (online).* **https://www.bankinfosecurity.asia/bangladesh-to-launch-cert-fin-a-14272** (accessed Aug 20 and Mar 21)

89. Asia Pacific Computer Emergency Response Team. (APCERT), (2021). Members. (online) **http://www.apcert.org/about/structure/members.html** (accessed Aug 20 and Mar 21)

Appendix F

Endnotes (continued)

90. Organisation of Islamic Cooperation-CERT (OIC-CERT), (2021) Members. (online) **https://www.oic-cert.org/en/allmembers.html#.YDVwYWj7RPY** (accessed Aug 20 and Mar 21)

91. Bangladesh Computer Emergency Response Team (bdCERT), (2014). Bangladesh. **http://www.bdcert.org/about_bdcert.html** (accessed Mar 21)

92. Global Cyber Security Capacity Centre (2018). Cyber Security Capacity Review of Bangladesh (2018). Oxford: *Author and BGD e-GOV CIRT. (online)* **https://www.cirt.gov.bd/cmm-bangladesh-report/** (accessed Mar 21)

93. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

94. BGD e-GOV CIRT (2021). Digital Forensics Lab. Bangladesh: *Author. (online)* **https://www.cirt.gov.bd/digital-forensic-lab/** (accessed Mar 21)

95. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

96. Forum of Incident and Security Teams (FIRST). (2020) Members FIRST Teams. (online) **https://www.first.org/members/teams/** (accessed Aug 20 and Mar 21)

97. Asia Pacific Computer Emergency Response Team. (APCERT), (2021). Members. (online) **http://www.apcert.org/about/structure/members.html** (accessed Aug 20 and Mar 21)

98. Organisation of Islamic Cooperation-CERT (OIC-CERT), (2021) Members. (online) **https://www.oic-cert.org/en/allmembers.html#.YDVwYWj7RPY** (accessed Aug 20 and Mar 21)

99. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). Partners. **https://www.cirt.gov.bd/partners/** (accessed Aug 20 and Mar 21).

100. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

101. Global Cyber Security Capacity Centre (2018). Cyber Security Capacity Review of Bangladesh (2018). Bangladesh: *Author and BGD e-GOV CIRT.* (online) pp30 R1.7. **https://www.cirt.gov.bd/cmm-bangladesh-report/** (accessed Mar 21)

102. Goswami, Suparna (2020). Bangladesh to Launch CERT-Fin. Bangladesh: *Bank Info Security 13th May 2020 (online).* **https://www.bankinfosecurity.asia/bangladesh-to-launch-cert-fin-a-14272** (accessed Aug 20 and Mar 21)

103. Goswami, Suparna (2020). Bangladesh to Launch CERT-Fin. Bangladesh: *Bank Info Security 13th May 2020 (online).* **https://www.bankinfosecurity.asia/bangladesh-to-launch-cert-fin-a-14272** (accessed Aug 20 and Mar 21)

104. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System. Bangladesh: *Author (online).* **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

105. Bangladesh Bank. Strategic Plan 2020-2024 – Fostering a Stable Financial System, Strategic Goal 8. Bangladesh: *Author (online)*. pp34. **https://www.bb.org.bd/en/index.php/about/strategic_plan** (accessed Mar 21)

106. Bangladesh Post (2020). BGD e-GOV CIRT arranging a Cyber Drill for Financial Institutions (22 Oct 2020). Bangladesh: *Author (online)* **https://bangladeshpost.net/posts/bgd-e-gov-cirt-is-arranging-a-cyber-drill-for-financial-institutions-on-22-october-2020-45256** (accessed Mar 21)

107. Bank of England and CBEST, CBEST Intelligence Led Testing, Understanding Cyber Threat Intelligence Operations, V2, UK, *Bank of England,* 2016, Para2.2.2 p 9, **https://www.bankofengland.co.uk/-/media/boe/files/financial-stability/financial-sector-continuity/understanding-cyber-threat-intelligence-operations.pdf** (accessed Nov 2020)

Appendix F

Endnotes (continued)

108. CREST, 'Accredited Companies Providing Vulnerability Assessment Services', 2020, **https://service-selection-platform.crest-approved.org/accredited_companies/vulnerability_assessment/** (accessed Nov 2020)

109. National Cyber Security Centre (NCSC), "Penetration Testing", UK, *Author,* 8 Aug 2017, **https://www.ncsc.gov.uk/guidance/penetration-testing** (accessed Nov 2020)

110. CREST, 'Accredited Companies providing Security Operations Centres (SOC)' 2020, *Author*, **https://service-selection-platform.crest-approved.org/accredited_companies/soc/** (accessed Nov 2020)

111. CREST, 'Cyber Security Incident Response Guide V1', 2013, UK, *Author,* Part 2, p11, **https://www.crest-approved.org/wp-content/uploads/2014/11/CSIR-Procurement-Guide.pdf** (accessed Nov 2020)

112. Bangladesh Government e-Government Computer Incident Response Team (BGD e-GOV CIRT). (2021). **https://www.cirt.gov.bd/** (accessed Aug 20 and Mar 21).

113. Bangladesh Computer Emergency Response Team (bdCERT), (2014). Bangladesh. **http://www.bdcert.org/about_bdcert.html** (accessed Mar 21)

114. Forum of Incident and Security Teams (FIRST). (2020) Members FIRST Teams. (online) **https://www.first.org/members/teams/** (accessed Aug 20 and Mar 21)

115. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

116. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9 pp151 **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

117. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9 pp151 **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

118. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: Author (online) Ch9 pp151 **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

119. ilab (2020). Bangladesh: *Aspire to Innovate.* **https://ilab.gov.bd/** (accessed Mar 21)

120. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9,9.2, pp147 **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

121. Ministry of Education, Government of Bangladesh (2020) **https://moedu.gov.bd/** (accessed Mar 21)

122. Ministry of Education, Government of Bangladesh (2019). Master Plan for ICT in Education in Bangladesh (2012-2021) Progress Review Report 2019. Bangladesh: *Author (online)* **https://moedu.gov.bd/sites/default/files/files/moedu.portal.gov.bd/page/ecea56df_b1bc_4707_bc8d_b99dbc08d8b9/f85661d36608b82ef945518a9ecb3b85.pdf** (accessed Mar 21)

123. Ministry of Education, Government of Bangladesh (2019). Master Plan for ICT in Education in Bangladesh (2012-2021) Progress Review Report 2019. Bangladesh: *Author (online)* **https://moedu.gov.bd/sites/default/files/files/moedu.portal.gov.bd/page/ecea56df_b1bc_4707_bc8d_b99dbc08d8b9/f85661d36608b82ef945518a9ecb3b85.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

124. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9 pp151 **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

125. Wikipedia, (2021) List of Universities in Bangladesh **https://en.wikipedia.org/wiki/List_of_universities_in_Bangladesh** (accessed Mar 21)

126. ISACA Dhaka Chapter. **https://engage.isaca.org/dhakachapter/home** (accessed Mar 21)

127. Cloud Security Alliance Bangladesh Chapter. **https://cloudsecurityalliance.org/chapters/global/** (accessed Mar 21)

128. Bangladesh Bank, Supervised Institutions, **https://www.bb.org.bd/fnansys/bankfi.php** (accessed 26 May 2020)

129. Bangladesh Microfinance Regulatory Authority, Licensed MFIs, **http://www.mra.gov.bd/images/Licensed_NGO_MFIs/lic08012020en.pdf** (Accessed 26 May 2020.

130. Bangladesh Association of Banks, **http://www.bab-bd.com/member_banks/** (accessed 26 May 2020)

131. Wikipedia, List of Banks in Bangladesh, **https://en.wikipedia.org/wiki/List_of_banks_in_bangladesh** (accessed 26 May 2020)

132. Common Vulnerabilities & Exposures (CVE) is a publicly available list of disclosed flaws, each is assigned a unique identification number, **https://cve.mitre.org** (accessed 29 Oct 2020)

133. Further information on CVSS available on Wikipedia, **https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System** (accessed on 29 Oct 2020)

134. Bangladesh Data Protection Overview, **https://www.dataguidance.com/notes/bangladesh-data-protection-overview** (accessed 23 Dec 20)

135. Valimail report on DMARC, 2019, **https://www.valimail.com/resources/domain-spoofing-declines-as-protective-measures-grow/** (accessed 30 Oct 2020)

136. Finance Digest Report, 2019, **https://www.financedigest.com/rise-sophisticated-bec-scams-finance-industry** (accessed 30 Oct 2020)

137. FBI Internet Crime Report, 2019, **https://www.ic3.gov/Media/Y2019/PSA190910** (accessed 31 Oct 2020)

138. CREST International, **https://www.crest-approved.org/** (accessed Aug 20)

139. EC Council, **https://www.eccouncil.org/** (accessed Aug 20)

140. ISACA, **https://www.isaca.org/** (accessed Aug 20)

141. (ISC)2, **https://www.isc2.org/** (accessed Aug 20)

142. SANS, **https://www.sans.org/** (accessed Aug 20)

143. CompTIA, **https://www.comptia.org/** (accessed Aug 20)

144. Offensive Security, **https://www.offensive-security.com/** (accessed Aug 20)

145. Cloud Security Alliance, **https://cloudsecurityalliance.org/education/** (accessed Aug 20)

146. PCI, **https://www.pcisecuritystandards.org/program_training_and_qualification/** (accessed Aug 20)

147. Cisco, **https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html** (accessed Aug 20)

148. Microsoft, **https://www.microsoft.com/en-us/learning/browse-all-certifications.aspx** (accessed Aug 20)

149. Amazon Web Services, **https://aws.amazon.com/training/path-security/?nc2=sb_lp_se** (accessed Aug 20)

150. IRCA(ISMS), **https://www.quality.org/** (accessed Aug 20)

151. BCS, **https://www.bcs.org/get-qualified/certifications-for-professionals/information-security-and-ccp-scheme-certifications/** (accessed Aug 20)

Appendix F

Endnotes (continued)

152. IET, **https://www.theiet.org/career/professional-registration/ict-technician/** (accessed Aug 20)

153. Husain, Syed Sajjad and Tinker, Hugh Russell, (2021). Bangladesh, Introduction and Quick Facts. USA: *Encyclopaedia Britannica,* **https://www.britannica.com/place/Bangladesh.** (Accessed 26 March 2021).

154. Husain, Syed Sajjad and Tinker, Hugh Russell, (2021). Bangladesh, Resources and Power. USA: *Encyclopaedia Britannica,* **https://www.britannica.com/place/Bangladesh** (Accessed 26 March 2021).

Husain, Syed Sajjad and Tinker, Hugh Russell, (2021). Bangladesh, Introduction and Quick Facts. USA: *Encyclopaedia Britannica,* **https://www.britannica.com/place/Bangladesh** (Accessed 26 March 2021).

155. World Population Review, (2021) Bangladesh Population 2021. *Author.* **https://worldpopulationreview.com/countries/bangladesh-population** (accessed Mar 21)

Husain, Syed Sajjad and Tinker, Hugh Russell, (2021). Bangladesh, Introduction and Quick Facts. USA: *Encyclopaedia Britannica,* **https://www.britannica.com/place/Bangladesh** (Accessed 26 March 2021).

156. The World Bank, (2020). The World Bank in Bangladesh, Economic Overview. *Author,* 14th October 2020, **https://www.worldbank.org/en/country/bangladesh/overview** (accessed Mar 21)

157. The World Bank, (2020). The World Bank in Bangladesh, Economic Overview. *Author,* 14th October 2020, **https://www.worldbank.org/en/country/bangladesh/overview** (accessed Mar 21)

158. The World Bank, (2020). The World Bank in Bangladesh, Economic Overview. *Author,* 14th October 2020, **https://www.worldbank.org/en/country/bangladesh/overview** (accessed Mar 21)

159. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

Husain, Syed Sajjad and Tinker, Hugh Russell, (2021). Bangladesh, Introduction and Quick Facts. USA: *Encyclopaedia Britannica,* **https://www.britannica.com/place/Bangladesh** (Accessed 26 March 2021).

160. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

161. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp148. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

162. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp149. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

163. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp149. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

Appendix F

Endnotes (continued)

164. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp150. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

165. BDG e-GOV CIRT (2015). Common Vulnerabilities in Cyber Space of Bangladesh. *Author* **https://www.cirt.gov.bd/common-vulnerabilities-in-cyber-space-of-bangladesh/** (accessed Mar 21)

166. Bangladesh e-Government CIRT (BDG e-GOV CIRT) (2021). Incident Reporting Statistics. **https://www.cirt.gov.bd/incident-reporting/statistics/** (accessed Mar 21)

167. Tipu, Md Sanaul Islam (2019). 3% Conviction Rate of Cybercrime in Bangladesh. *Dhaka Tribune.* **https://www.dhakatribune.com/cybersecurity/2019/04/20/3-conviction-rate-of-cybercrime-in-bangladesh** (accessed Aug 20 and Mar 21)

168. AFP (2020). Cybercrime Cost to top $1tn this year. *Dhaka Tribune* 7th Dec 2020. **https://www.dhakatribune.com/world/2020/12/07/cybercrime-costs-to-top-1tn-this-year** (accessed Mar 21)

169. BSS (2021). PM Asks Police to Check Cybercrimes, Drug Abuse. *Dhaka Tribune* 3rd Jan 2021. **https://www.dhakatribune.com/bangladesh/2021/01/03/pm-asks-police-to-check-cybercrimes-drug-abuse** (accessed Mar 21)

170. Overseas Security Advisory Council (OSAC) (2020), Bangladesh 2020 Crime and Safety Report. USA: *Author* **https://www.osac.gov/Country/Bangladesh/Content/Detail/Report/a842f414-00f0-43c7-8443-188c64d5b5ef** (accessed Mar 21)

171. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp150. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

172. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp151. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

173. General Economics Division (GED), Government of Bangladesh (2020). Making Vision 2041 a Reality - Perspective Plan of Bangladesh 2021-2041. Dhaka, Bangladesh: *Author (online)* Ch9, Para9.2, pp151. **http://oldweb.lged.gov.bd/UploadedDocument/UnitPublication/1/1049/vision%202021-2041.pdf** (accessed Mar 21)

174. Global Cyber Security Capacity Centre (2018). Cyber Security Capacity Review of Bangladesh (2018). Oxford: *Author and BGD e-GOV CIRT.* (online) **https://www.cirt.gov.bd/cmm-bangladesh-report/** (accessed Mar 21).

175. National Cyber Security Index, National Cyber Security Index 2018 - Bangladesh. Estonia, *e-Governance Academy,* 2018, **https://ncsi.ega.ee/country/bd/** (accessed Mar 21)

176. National Cyber Security Index, National Cyber Security Index 2018 - Bangladesh. Estonia, *e-Governance Academy,* 2018, **https://ncsi.ega.ee/country/bd/** (accessed Mar 21)