



Pakistan



**CMAGE**  
Cyber Security Maturity Assessment Global Ecosystem

# Pakistan Report

Maturity Model Assessment

2021

# Report Structure

**This document begins with a Highlight Report outlining key observations, followed by an introduction to the CREST maturity model structure, and an explanation of assessment methodology used in the research.**

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

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

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

The assessment of the maturity level assigned to each indicator is shown in the box immediately below the section heading. The box also contains the relevant maturity model definition (drawn from Appendix B).

A short commentary to support the maturity level assessment is also 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](mailto:info@crest-approved.org)**



## Navigation Key



Move back  
a page



Move forward  
a page

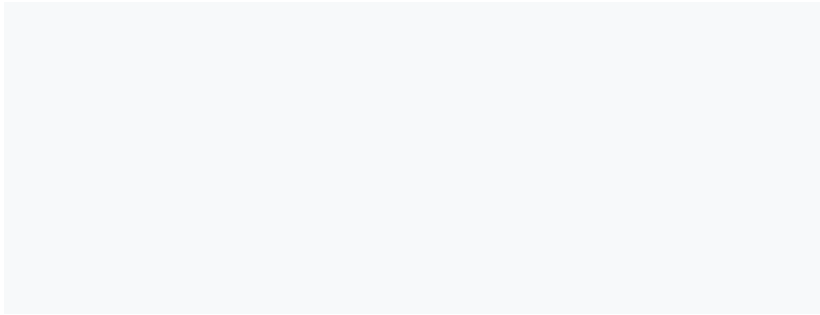
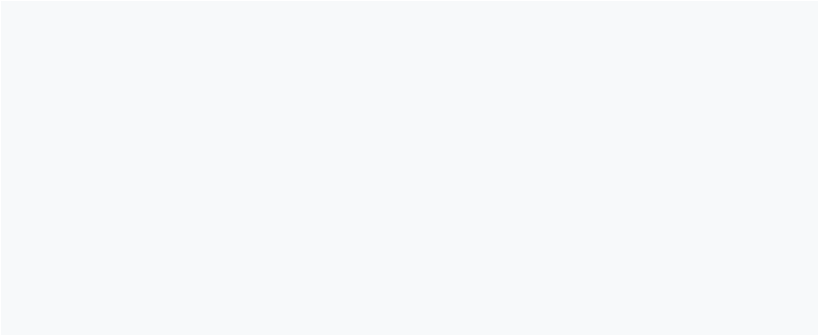
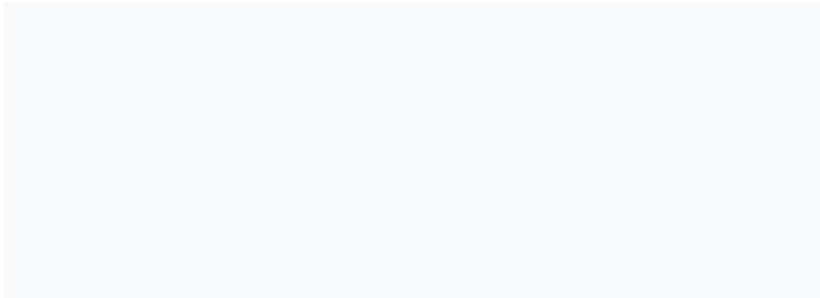


Return to  
contents page



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 Pakistan's cyber security Ecosystem.

CREST has made both quantitative and qualitative assessments to arrive at an overall judgment regarding its level of cyber security.

This report draws upon open-source evidence we have gathered, and records assessments we have made.

While it will never be a complete assessment, it has been externally validated.

The relational database containing the CMAGE model has helped facilitate consistent application of the assessment and allows for ease of update and maintenance of the data, the ability to interrogate the data and the ability 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 which have a shared interest in improving Pakistan's overall cyber security posture.

Unashamedly, the endpoint from a CREST perspective is that every financial services institution in Pakistan 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 Pakistan and the international community who have contributed to this report.

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



**Ian Glover**

President  
CREST International





# Highlights Report

## Background

**CREST International seeks to help build capacity, capability and consistency in Pakistan's cyber security ecosystem. The underlying aim is that every financial institution in Pakistan 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 the 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 brings benefits to other areas of the ecosystem as well.

### Maturity Model Assessment Summary

#### Overall Pakistan Ecosystem

##### *Maturity Level 2*

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

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

With concerted effort it should be possible to progress to 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 Pakistan's cyber security ecosystem is based upon the assessed maturity of five constituent Dimensions:

### 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**

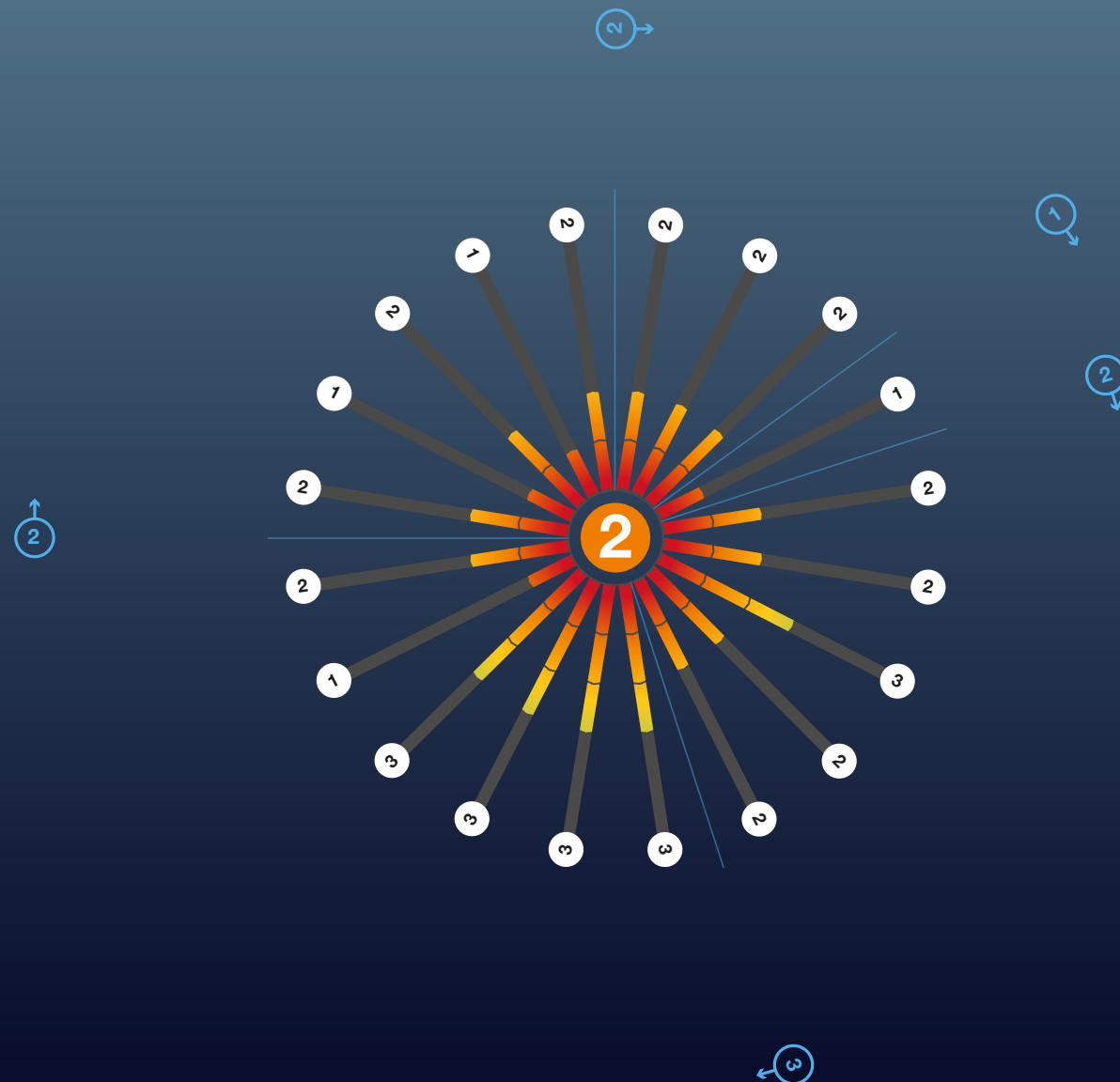
### Maturity Scores

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:

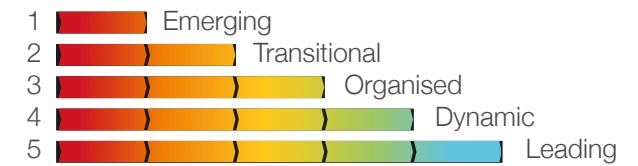
|        |         |
|--------|---------|
| RED    | Level 1 |
| AMBER  | Level 2 |
| YELLOW | Level 3 |
| GREEN  | Level 4 |
| BLUE   | Level 5 |

# Highlights Report

## Summary of Observations (continued)



### Maturity Levels



### 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 highlights report concludes with a section titled 'next steps'; the starting point for a conversation about practical measures to improve Pakistan's cyber security ecosystem.

# Highlights Report

## Key Observations - Dimension 1 - National Cyber Security & Capabilities

By its actions, the government of Pakistan is clearly signalling its intent to tackle cybercrime and to make government, business and society more secure. However, there was no immediate evidence of a publicly available, comprehensive, national cyber security strategy.

Establishing the **National Response Centre for Cyber Crime (NR3C)** is a significant step forward in addressing cybercrime issues. It is beginning to make tangible progress in many areas. NR3C's Cyber Scouts initiative has real promise. Cyber criminals often lure young people to work for them with promises of wealth and kudos. Without effective programmes to counter this view, the young are vulnerable to grooming.

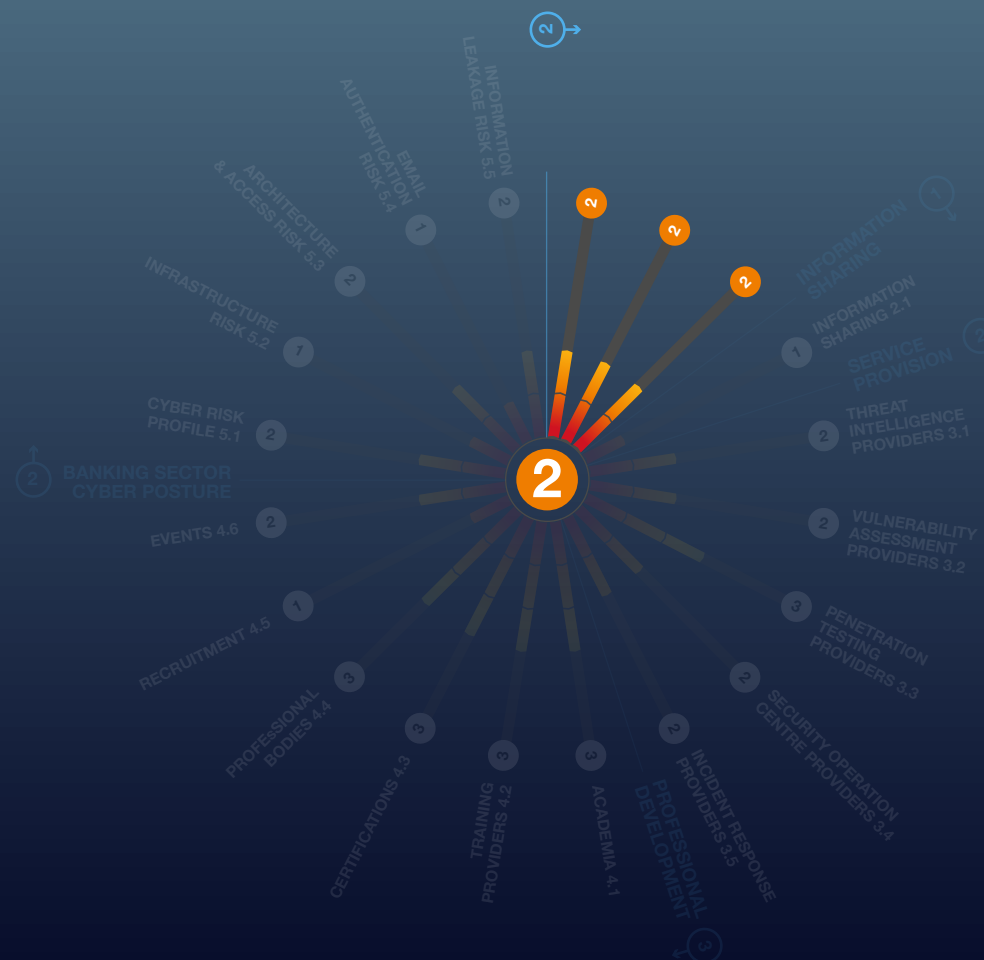
There is strong evidence that key government ministries and agencies, such as the **State Bank of Pakistan (SBP)**, the **Securities & Exchange Commission (SEC)**, the **Pakistan Telecommunications Authority** and the **Ministry of Social Protection & Poverty Alleviation** are paying attention to addressing cyber security issues within their own sphere of influence.

While no formal cyber security assurance schemes could be identified, the SBP and SEC have recently published relevant frameworks.

## Dimension 1

### National Cyber Security Strategy & Capabilities

*Maturity Level 2*



# Highlights Report

## Key Observations - Dimension 2 - Cyber Security Information Sharing

**A formal national CERT could not be identified during the research.**

However, **Pakistan Information Security Association (PISA)** runs its own **CERT** and is a temporary full member of the **Organisation of Islamic Cooperation (OIC) CERT**. PISA also represents Pakistan at the annual Asia-Pacific CERT exercise.

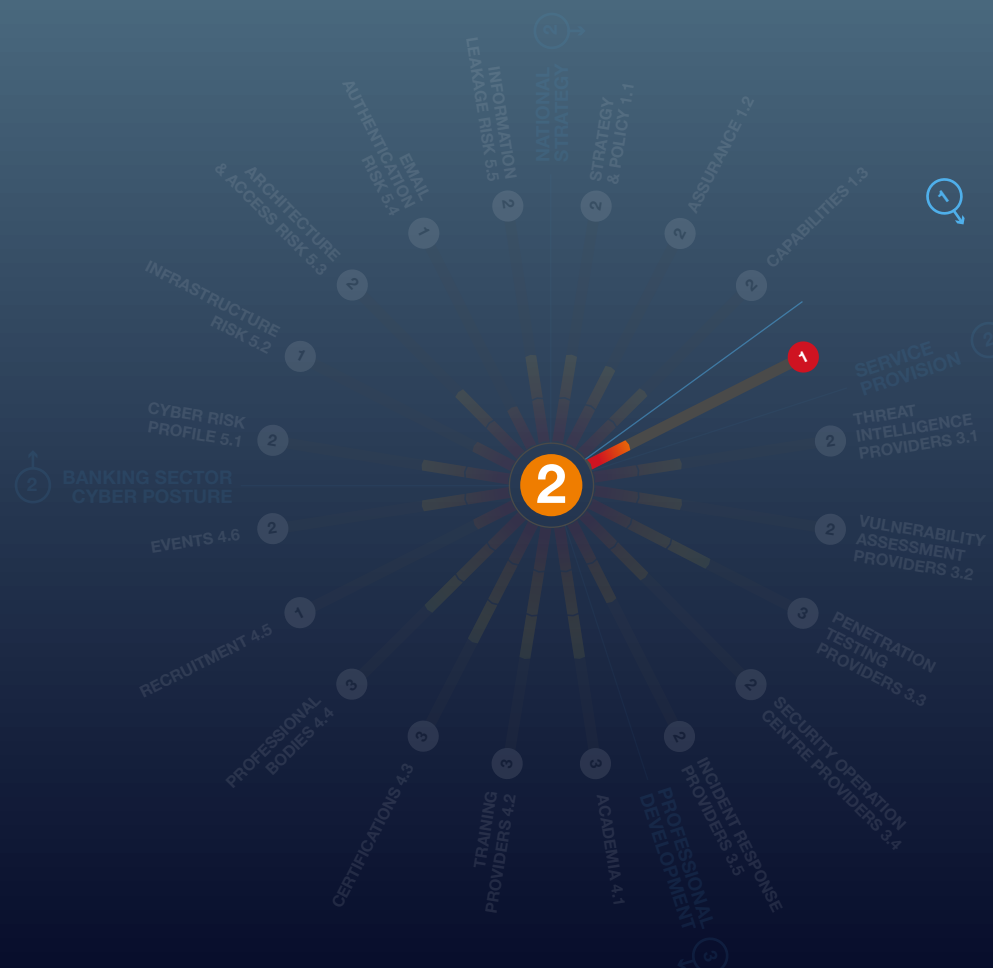
**Two further companies were identified as offering Computer Emergency Response Team (CERT) services.** These companies, **Pakcert and Onsite**, principally provide commercial cyber security and training services. Neither company appeared to be affiliated to international information sharing associations, such as FIRST or AP CERT.

**Pakistan is on the cusp of Maturity Level 2.**

## Dimension 2

Cyber Security Information Sharing

*Maturity Level 1*





# Highlights Report

## Key Observations - Dimension 3 - Cyber Security Service Provision



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



Research identified a further twelve local companies that also offer such services, but their quality could not be assessed.



A number of CREST and non-CREST companies offer cyber security services to clients in Pakistan from regional offices in nearby countries.

### Overall

A good mix of local, regional and international providers of cyber security services exist across the five disciplines examined.

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

## Dimension 3

### Cyber Security Service Provision

*Maturity Level 2*



# Highlights Report

## Key Observations - Dimension 4 - Cyber Security Professional Development

**A first-class cyber security industry needs to be underpinned by a comparable offering of cyber security education.**

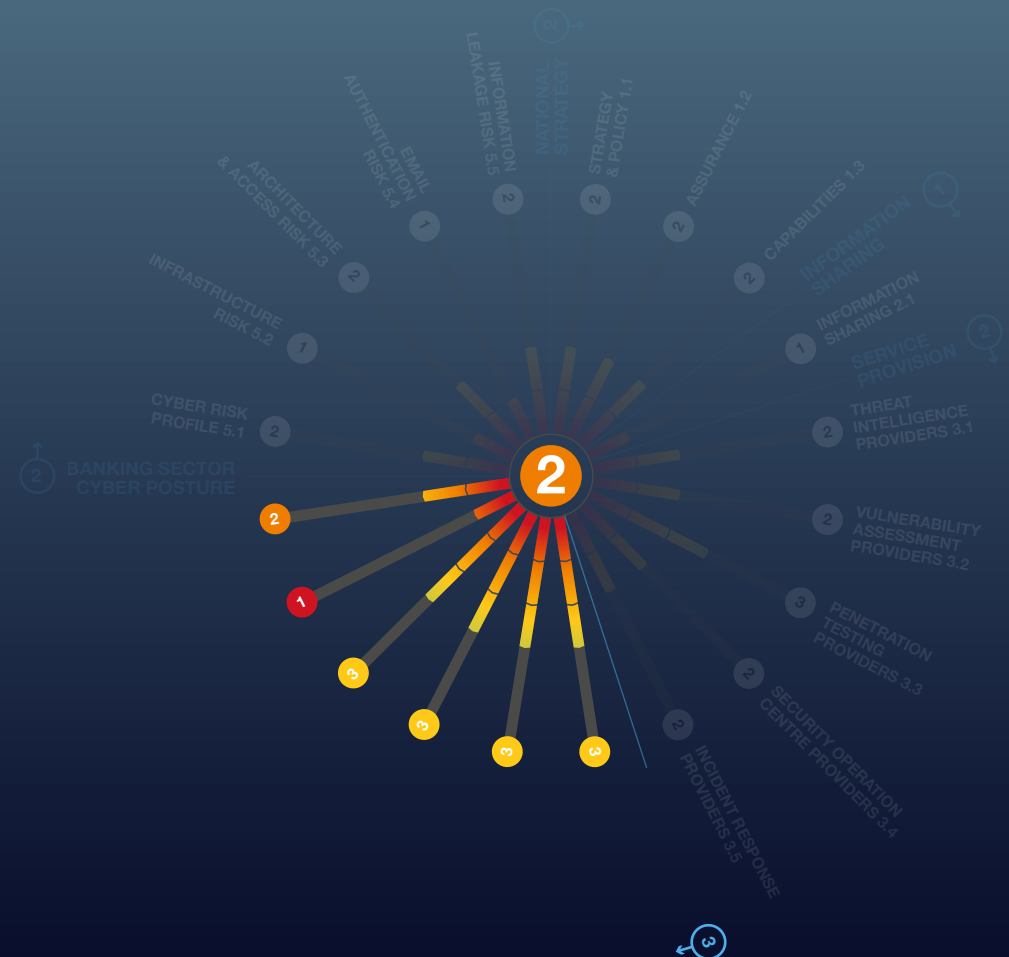
The formation of a National Centre for Cyber Security (NCSS), and its focus on developing R&D laboratories in selected universities, is a promising initiative that will strengthen national response to cyber challenges by adding capacity and depth of knowledge.

Continued on next page...

## Dimension 4

### Cyber Security Professional Development

*Maturity Level 3*



# Highlights Report

## Key Observations - Dimension 4 (continued)



There is a good blend of in-country and international cyber security training. Although the National Cyber Training Program (NCTP) was only launched in 2020, it could quickly become a significant addition to the mix.



Examinations for many international professional certifications are readily accessible in Pakistan. There is some evidence that take-up in certifications is improving and likely to expand further with the advent of the NCTP.



Costs of some professional certificates are currently prohibitive. It is possible that once individuals and companies see the benefits of professional certifications the cost issue may be overcome.



As part of the project's Stage 2, some 'pump priming' funds may be available to start the process.



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



There is evidence of some international professional bodies operating in Pakistan, but this needs to be extended and strengthened to better support national aspirations to grow the number of cyber security professionals.



Alongside the international professional bodies, two Pakistan-focused professional bodies, PISA and Global Information Security Society for Professionals of Pakistan (GISPP), have been established. Both are active, with their own international reach.

# Highlights Report

## Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

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

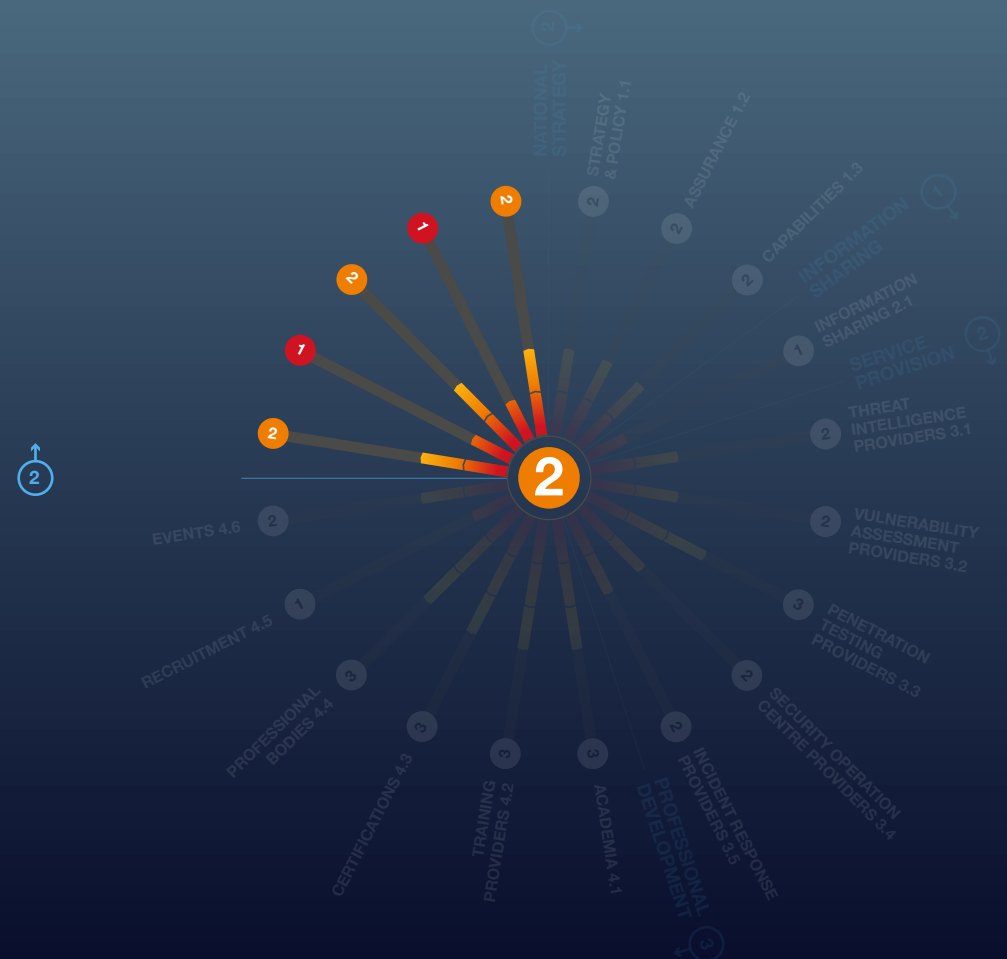
Pakistan's regulators can utilise this assessment to focus attention and highlight areas for review, provide access to the supporting guidance being developed and, where appropriate, encourage take up of technical security measures to improve cyber resilience.

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:

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

Directly assessing many of the key risk areas listed above is not possible. However, 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 many key risk areas.

Passive external assessments were carried out on the public-facing IT infrastructure of a sample of 73 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.

CREST assessed the general threat to Pakistan's financial institutions is lower than for larger institutions in more advanced economies.

Yet some of Pakistan's financial institutions still attract a significant threat score.

46%

Overall, **46%** were awarded a risk rating of 'Very High' or 'High', indicating Maturity Level 2 for Risk Profile.

24%

**24%** of the sample had evidence of critical vulnerabilities within their infrastructure.

30%

A further **30%** appeared to be carrying non-critical vulnerabilities. This indicates 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.

30%

Some **30%** appeared to have one or more database ports open, leading to the award of Maturity Level 2 for this risk category.

72%

Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **72%** 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. Our research indicates Maturity Level 1 for Email Authentication Risk.

79%

In **79%** of sampled institutions, at least some staff data was available online as a result of third-party data breaches, indicating Maturity Level 2 for Information Leakage Risk.

**There is significant room for improvement in the cyber security posture of many of Pakistan'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 Pakistan's cyber security ecosystem.**

3

CREST is in the process of 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

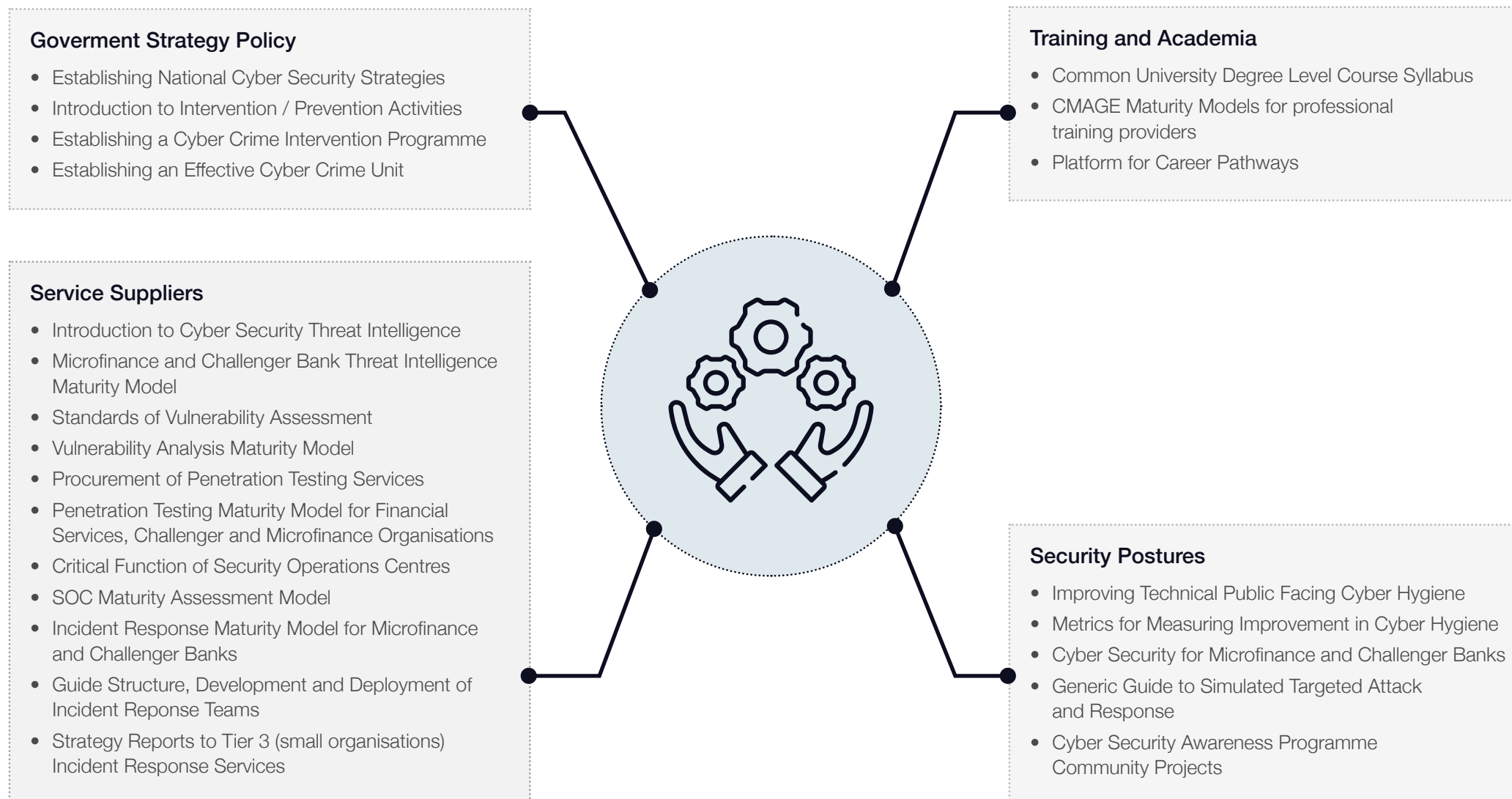
The library will be **available throughout 2021** and is shown on the next page.

6

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

# Highlights Report

## 2021 Good Practices Guides and Tools





Introduction

# Introduction

## Background

**This report seeks to provide a benchmarked assessment of the maturity of Pakistan'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.
2. The library of good practice guides and tools being developed by CREST can then be readily used to support a programme of improvements.
3. Where requested, CREST will subsequently 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 being made.
4. **The Bill & Melinda Gates Foundation's Financial Services for the Poor (FSP) programme<sup>1</sup>** 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 people with the means to build more prosperous and secure lives for themselves, their families, and their communities.
5. Financial services must be underpinned by the best possible cyber security measures if they are to minimise the risk of the most financially vulnerable people 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.

6. 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

7. **CREST is an international not-for-profit accreditation and certification body** that represents and supports the technical information security market<sup>2</sup>. 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.**

8. **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

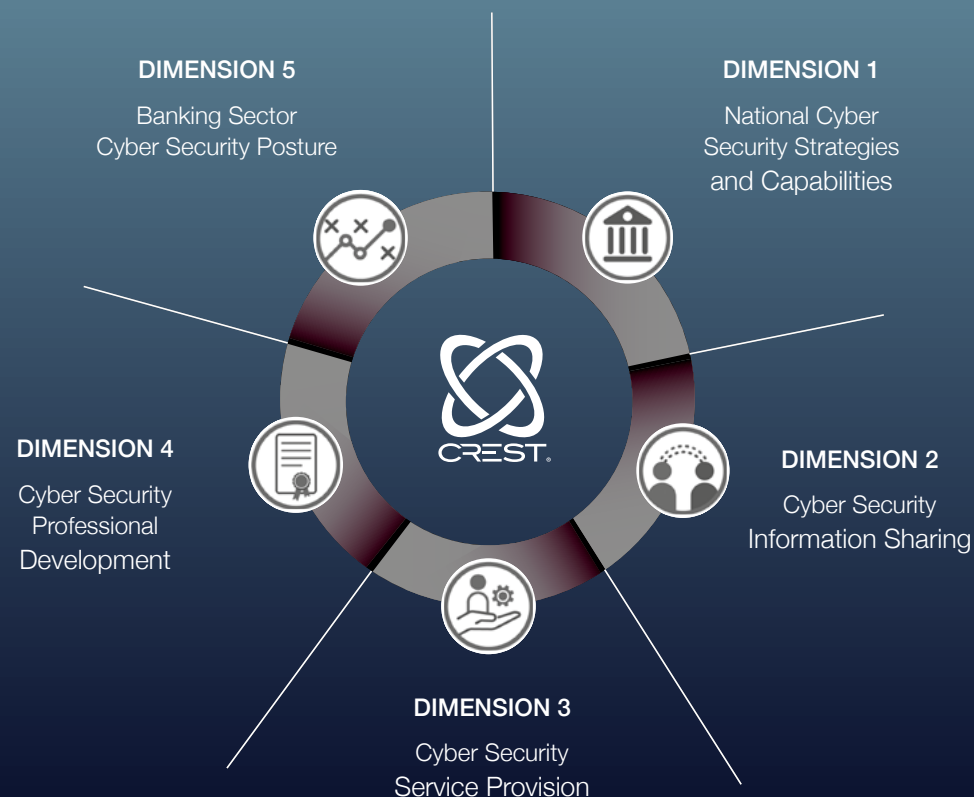
## Research Methodology

9. **Except for the section of this report dealing with the banking sector cyber security posture,** all evidence used in preparing this report has been gathered using open-source methods, including internet-based research supplemented - where needed for clarity - by email and telephone enquiries. The research has subsequently been presented to audiences of local and international subject matter experts for feedback and validation.
10. In terms of banking sector cyber security posture, CREST worked with **Orpheus Cyber<sup>3</sup>**, 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 that rapid, automated mass assessment has been used as part of cyber security maturity modelling.
11. **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 is envisaged the report will be updated periodically with stakeholder support to assist in reporting progress.

## CMAGE Structure

12. This Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) is based on a 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 on assessment of twenty separate Indicators across five Dimensions. The five Dimensions are depicted diagrammatically in the image below.





# Introduction

## Maturity Level Definitions

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



16. The complete listing of the Dimensions and their associated Indicators is shown in the table, right. 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                        |

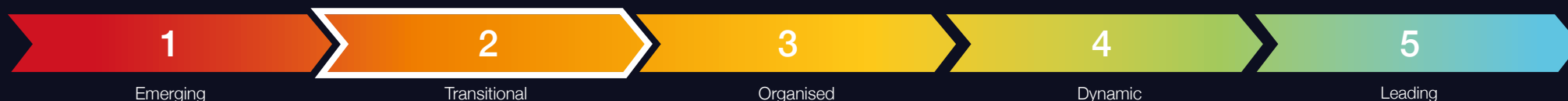


## **Dimension 1**

National Cyber Security  
Strategy & Capabilities

# National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2*



**National strategy is of vital importance.**

**Without a national strategy for cyber security, it would be difficult for law enforcement and the judicial system to tackle cybercrime.**

17. 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. The public and private sectors would have no guidance or framework to base their cyber security policies on. Ultimately, a lack of national cyber security strategy would undermine economic growth.

Examining the **National Cyber Security Strategy** provides good insight into a nation's willingness to implement cyber security measures and to tackle cybercrime. In short, a national cyber security strategy sets the standards for all other sectors to follow.

18. In conducting its research, CREST was looking for:



Government strategic guidance, policy and legislation published in relation to information/cyber security



When it was published



How thorough it was



Whether it empowered government departments and agencies to act, and if the strategy has been implemented and updated

# National Cyber Security Strategy & Capabilities

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

19. The **Global Cyber Strategies Index 2020** assesses countries on their **existing laws and strategies** for the following criteria:

According to the Index, Pakistan is only listed as having draft privacy legislation and e-commerce and cybercrime legislation dated 2012 and 2016 respectively<sup>4</sup>.

### Overall Assessment

20. Whilst Pakistan is currently at Level 2, the national ambition for progress is very clear. **The National Centre for Cyber Security<sup>5</sup> and the National Cyber Training Programme<sup>6</sup>** are evidence of a commitment to improve Pakistan's Cyber Security capabilities – nationally, organisationally and individually.

21. **The National Centre for Cyber Security (NCCS)** was established in 2018<sup>7</sup> as a joint initiative of the Higher Education Commission and Planning Commission. NCCS's mission is to build national capabilities and capacities in cyber security to produce indigenous professionals and solutions in the sector<sup>8</sup>.

22. The **National Cyber Training Program's (NCTP)** mission is 'to train the youth of Pakistan in advanced cyber skillsets to shape technical work force for emerging technologies with industry leaders which will contribute to Pakistan's defence, knowledge economy and global progress. NCTP is a 100% online training programme where our youth will get a hands-on advanced security education with practical tools, which will help them to become a functional cybersecurity professional from day one'<sup>9</sup>.

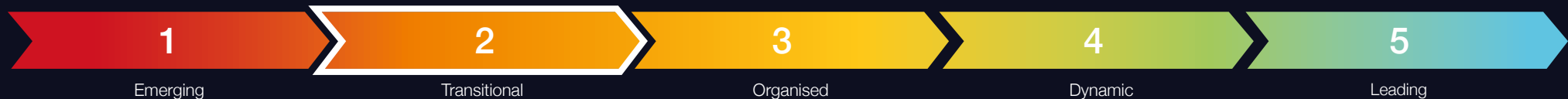
23. A review of cybercrime can be found in **Appendix D** of this report.

### Development approach

24. The key to fulfilling improvements in Pakistan's cyber-security is to follow through on the aspirations of current programmes. Mandating minimum standards across the public and financial sectors would be a strong addition to the portfolio.

# National Cyber Security Strategy & Capabilities

## Indicator 1.1 National Strategy & Policy



### Assessment – Maturity Level 2

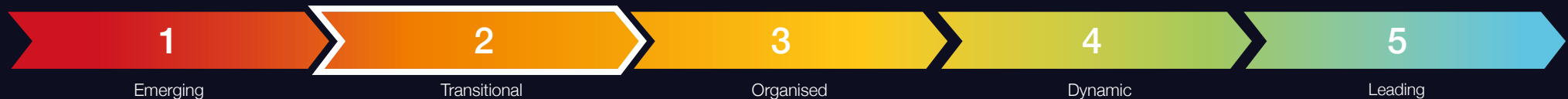
Some evidence of up-to-date strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

25. **Government strategy must be reviewed and updated regularly to help to establish priorities and focus activities.** The 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 Prevention of Electronic Crimes Act (PECA) 2016<sup>10</sup> lays out the groundwork for good cyber security though it now nearly five years old. Chapter II and V cover offences and punishments. Chapter III, covering the establishment of an investigative agency<sup>11</sup>, states government may establish an investigative agency. In Chapter IV, International Cooperation, it states the Government may [...] extend such cooperation to a foreign Government<sup>12</sup>. And in Chapter VI, Preventative Measures, it states that federal government may constitute one or more CERTs to respond to cyber threats on Pakistan<sup>13</sup>.
27. The PECA 2016 has since been augmented by the Prevention of Electronic Crimes Investigation Rules 2018<sup>14</sup>, which gives authority for an investigative agency and international cooperation. According to the Pakistan Telecommunications Authority Annual Report 2018-2019, it has submitted a framework for a telecommunications CERT to the government<sup>15</sup>.
28. The consultation draft of the Data Protection Bill 2020, still to be published, is a vast improvement on the 2018 draft which did not make it into law. This one is much more comprehensive and includes more detail on:
  - Data security
  - Data integrity
  - Breach reporting
  - Data access control, and
  - Processing sensitive personal data guidelines.
29. Importantly, it details establishing a new authority, the Personal Data Protection Authority of Pakistan, which must be created within six months of the Bill going live. It must comprise seven members:
  - Three IT experts
  - One legal expert
  - A representative from civil society
  - A financial expert and
  - An ex-officio member / or representative from either the Ministry of IT and Telecom, Ministry of Defence or Ministry of Interior<sup>16</sup>.



# National Cyber Security Strategy & Capabilities

## Indicator 1.2 Regulator/Government Operated Assurance Schemes



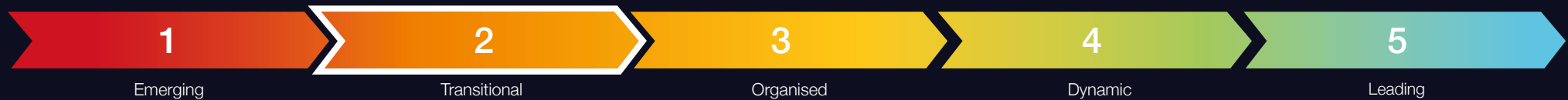
### Assessment – Maturity Level 2

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.

30. The central bank or other lead financial authority of any nation is essential in setting the ethical standards and operating frameworks for banks and financial institutions operating within the country. The research focused on looking for any publicly available policies and laws which support and uphold financial ethics, integrity and cyber security.
31. The State Bank of Pakistan has no one overarching cyber security policy for the banking and financial sector. Instead, it has issued various guidelines and circulars which cover different aspects of cyber and information security. The main ones found during research include:
  - a. “Guidelines on Information Technology security”, issued in 2004<sup>17</sup>.
  - b. “Prevention Against Cyber Attack - BPRD Circular No. 07 of 2016” which all financial institutions had to implement by December 31, 2016<sup>18</sup>.
  - c. “The Enterprise Technology Governance & Risk Management Framework for Financial Institutions - BPRD Circular no 5 of 2017”, which all financial institutions had to implement by June 30, 2018<sup>19</sup>.
  - d. “Security of Digital Payments - PSD Circular no 9 of 2018” - lists 17 action points to be implemented by all financial institutions. These points included specified security protocols and producing assessment plans for the implementation of Payment Card Industry Data Security Standards (PCI DSS) and Payment Application Data Security Standard (PA DSS) to be achieved by January 31, 2019<sup>20</sup>.
  - e. The circulars in points (c) and (d) were mentioned and adherence to them re-emphasised in “Measures to Enhance Cyber Resilience amid Covid-19 Threat - PSD - Circular no 3 of 2020”, issued on March 26, 2020. It gave banks, microfinance banks and payment system operators further guidelines to follow, including a direction to immediately establish dedicated Cyber Threat Intelligence Units (CTI-Us), Emergency Response Teams (ERTs) and submit the name of their CTI focal person to the State Bank by March 31, 2020<sup>21</sup>.
32. The Securities & Exchange Commission of Pakistan published “Guidelines on Cybersecurity Frameworks for the Insurance Sector” which came into effect on July 1, 2020. The guidelines encourage insurers to follow the NIST Cybersecurity Framework<sup>22</sup>, ISACA's COBIT<sup>23</sup> and ISO 27000 Series<sup>24</sup>, as an example of standards and best practices to follow. The guidelines also directed insurers to appoint a Chief Information Security Officer (CISO) and conduct cyber risk assessments, among other recommendations<sup>25</sup>.

# 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.

33. It is important to understand the level of reporting for cybercrime, as it is evidence of cybercrime being openly recognised, discussed and taken seriously as an issue in a public forum. The research looked for what and where cybercrime was being reported, and what official action was being reported to combat it.
34. PECA 2016<sup>26</sup> Chapter II, which covers offences and punishment, is very clear with definite language regarding the consequences of committing any of the listed electronic offences. Chapter V, covering prosecution and trial of offences, is similarly decisive.
35. The Prevention of Electronic Crimes Investigation Rules 2018 were brought into force to enable the government to reinforce PECA 2016. Para 3(1) of the rules gives the Federal Investigation Agency (FIA)<sup>27</sup> the authority to investigate cybercrimes through its Cybercrime wing. In paragraphs 18 and 18(2), the FIA and its Cybercrime wing are the designated agencies with authority to seek or extend cooperation to any foreign government<sup>28</sup>.
36. The National Response Centre for Cyber Crime (NR3C), also known as the FIA's Cybercrime wing, is headquartered in Islamabad and has 15 offices in other cities. It is the nation's cybercrime reporting centre. It also hosts Cyber Scouts, a superb initiative which engages with youth, educating and training them in cyber security and cybercrime awareness, with the aim that they also positively influence friends and family<sup>29</sup>.

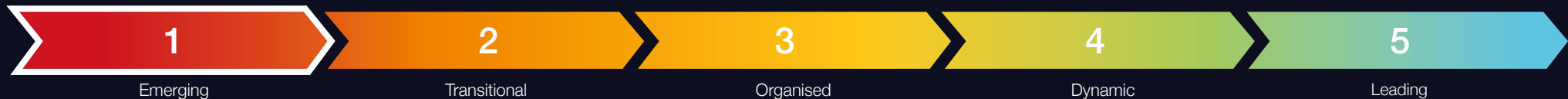


## **Dimension 2**

Cyber Security  
Information Sharing

# Cyber Security Information Sharing

## Overall Dimension Assessment: *Maturity Level 1*



38. Information sharing is vital to achieving common understanding of cyber security risks and vulnerabilities, helping counter the threats posed by cybercriminals. There is no commercial advantage to be gained by not sharing information. Open publication of academic research and sector-specific information exchanges are two 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 Pakistan.
39. Information sharing also enables the spread of best practice. The research focused on looking for expert groups such as **Computer Emergency Response Teams (CERTs)**, which, as information/cyber security experts, are responsible for protection against, detection and response to cyber security incidents.
- They provide cyber security services, as well as running cyber security awareness campaigns and events for other organisations and the 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.
40. The research also looked for evidence of other organisations working as cyber security awareness groups, either for a specific sector or wider. With both CERTs and the various 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

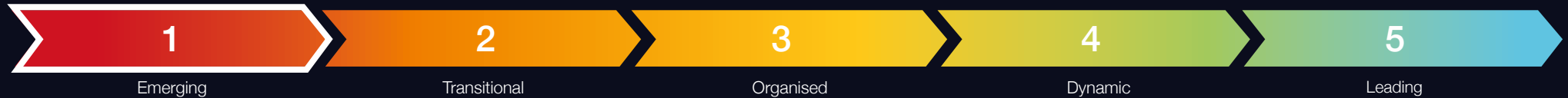
41. Pakistan has three CERTs. Two of which, PakCERT<sup>30</sup> and Onsite<sup>31</sup> are not members of any regional or international forum such as the Forum of Incident Response Teams (FIRST)<sup>32</sup> or AP CERT<sup>33</sup>. Both operate more as commercial service providers than as organisations for public benefit.
- Pakistan International Security Authority (PISA)**<sup>34</sup> which provides PISA-CERT, is a member of the international **Organisation of the Islamic Cooperation CERT (OIC-CERT)**<sup>35</sup>, and liaises with, but is not a member of, APCERT. None of the three CERTs are officially classed as the national CERT.
42. The paper **Cyber Security: Where Does Pakistan Stand? (SDPI 2019 p9)** discusses the creation of a National CERT and the Prevention of Electronic Crimes Act 2016 (chapter VI para 48-49)<sup>36</sup> proposes a CERT. In the SDPI (2019) paper it discussed this CERT as being within the **Pakistan Telecommunications Authority (PTA)**, as part of the PTA's CERT-Pakistan Telecom Sector Implementation Plan<sup>37</sup>.
43. In PTA's 2019 annual report, Chapter 4 – Cyberspace Management, it states that the baseline framework for establishing a telecommunications sector CERT has been prepared by PTA and submitted to the government of Pakistan, with an expected operational date of the CERT being sometime in 2020<sup>38</sup>. No evidence of the PTA CERT's establishment was found at the time of research.

## Development Approach

44. As a priority, Pakistan needs to establish a national CERT with formal links and a mandated role in coordinating national responses to cyber incidents. Nationally and internationally, the CERT should be regarded as a source of freely available information and advice.

# Cyber Security Information Sharing

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



### Assessment – Maturity Level 1

Limited evidence of cyber incident reporting or coordinated response.

45. 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)

46. **PakCERT was established in 2000, as one of the first information security providers in Pakistan.** It provides a variety of cyber security services and solutions to the public, but is not yet affiliated with, or a member of, any regional or international CERT Forums<sup>39</sup>. **Onsite is a cyber security service provider which has a CERT, but similarly to PakCERT,** is not affiliated with, or a member of any regional or international CERT forum<sup>40</sup>.

47. **PISA-CERT has been in operation since 2012,** with international links via its membership of OIC-CERT and regional links via its liaison with APCERT. PISA-CERT took part in the 2020 APCERT exercise as an external team<sup>41</sup>. PISA as an organisation also runs training, conferences and has chapters.



## **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. Cyber security service providers form part of the front line in the fight against cybercrime.**

48. Research into how cyber security services are currently provided in Pakistan quantified cyber security service providers, examined what services they offered, what accreditations they held and what accredited services and certifications they provided.
49. The location of company offices and customer reach were also recorded. CREST examined if they were local companies, registered and only based in Pakistan. Are they regional, registered in another Asian country, but with offices and the ability to reach regional customers? Or are they a large international organisation, with multiple global office locations which may be located in-country? If not, can they provide services into Pakistan without having a permanent physical presence there, or anywhere in the Asian region? When examined together, all of these factors combined give an idea of the maturity of the cyber security industry.

50. Several companies provided more than one cyber security service such as security, training and events, for example - so appear in more than one indicator. Where possible, ICT companies providing solutions via the purchase of other technology products, such as software, were excluded from the research.

## Overall Assessment

51. Pakistan is assessed as being at Level 2 across four of the five service provision disciplines. The exception is Penetration Testing, which is at Level 3. Good progress is being made towards Level 3 goals across the remaining disciplines. There are no local CREST member companies, but two CREST International Members have locally-based offices. There are a small number of local service providers across most disciplines.

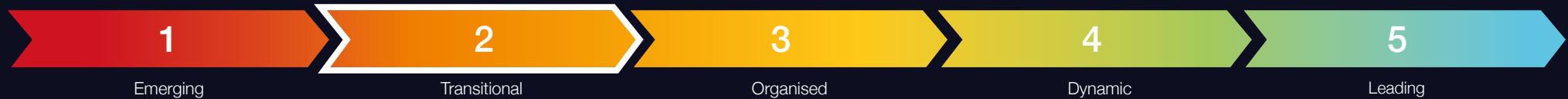
## Development Approach

52. Demand-led growth in the number of service providers should encourage investment. Encouragement from government and regulators should lead to adoption of benchmarked standards.



# Cyber Security Service Provision

## Indicator 3.1 Threat Intelligence Providers



### 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

53. Cyber Threat Intelligence is information about current and future cyber threats and actors that adversely affect a nation's or individual organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks<sup>42</sup>. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark-side sources.
54. The research looked for companies providing cyber threat intelligence services to organisations in Pakistan and where these services were delivered from. For the purposes of a robust cyber security environment, the ideal scenario is a host of Threat Intelligence service providers based in Pakistan. Evidence of quality, through accreditations or partnerships these companies may have, was also sought.

| Office Location | Non-CREST Accredited | CREST Accredited | Total |
|-----------------|----------------------|------------------|-------|
| In-country      | 5                    | 2                | 7     |
| Regional        | 0                    | 0                | 0     |
| International   | 1                    | 5                | 6     |
| Total           | 6                    | 7                | 13    |

55. There are **13 companies offering threat intelligence services in Pakistan. Seven are based in Pakistan, two are CREST Accredited International companies**, with one based in Karachi and the other with offices in Islamabad, Karachi and Lahore.

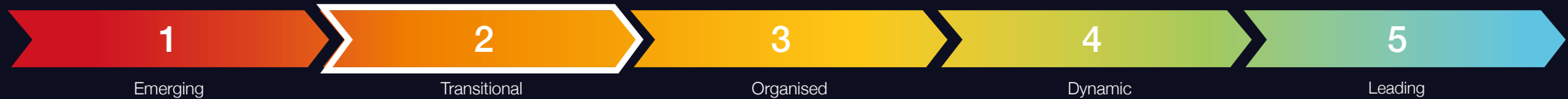
56.





# 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)

57. 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<sup>43</sup>.”

As with threat intelligence, research focused on looking for companies which provide VA services, ideally based in Pakistan.

58. CREST’s research found **20 companies providing Vulnerability Assessment (VA) services into Pakistan**. Some **eight companies operate in-country**, two of which **are CREST accredited**.

| Office Location | Non-CREST Accredited | CREST Accredited | Total |
|-----------------|----------------------|------------------|-------|
| In-country      | 6                    | 2                | 8     |
| Regional        | 0                    | 0                | 0     |
| International   | 2                    | 10               | 12    |
| Total           | 8                    | 12               | 20    |



# Cyber Security Service Provision

## Indicator 3.3 Penetration Testing Providers



### Assessment – Maturity Level 3

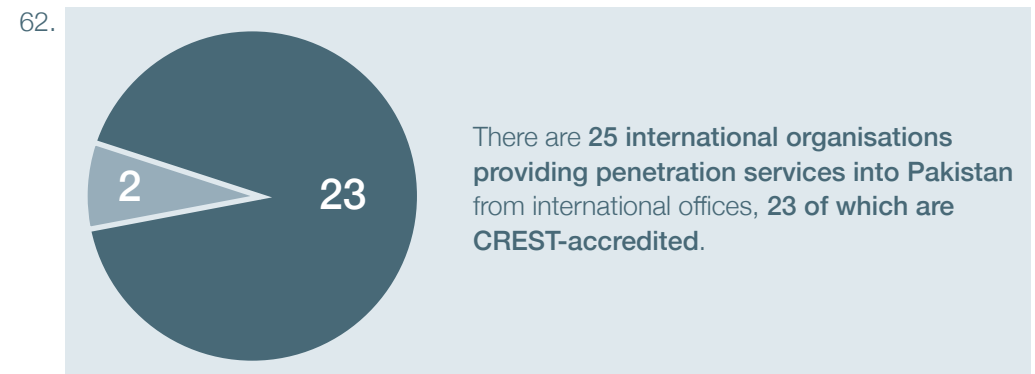
No locally-registered CREST member companies but a strong presence from international CREST members with local offices. There are some locally registered providers, but these are not benchmarked against international standards. There is competition and international providers view the market as being mature enough for investment.

### Penetration Testing

59. 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<sup>44</sup>."
60. CREST's research found significantly more companies providing penetration testing than any other cyber security service. Although, 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 Pakistan as could be identified.

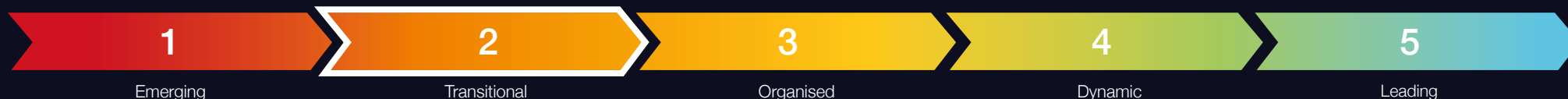
| Office Location | Non-CREST Accredited | CREST Accredited | Total |
|-----------------|----------------------|------------------|-------|
| In-country      | 12                   | 3                | 15    |
| Regional        | 0                    | 29               | 29    |
| International   | 2                    | 23               | 25    |
| Total           | 14                   | 55               | 69    |

61. In total, **69 companies** were found providing Penetration Testing services into Pakistan. Of those, **15 companies** operate in country; three are CREST-accredited. Regionally, there are **29 companies** providing services into Pakistan, all of which are CREST-accredited.



# Cyber Security Service Provision

## Indicator 3.4 Security Operation Centre Providers



### 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

#### 63. 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<sup>45</sup>.”

64. 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      | 6                    | 1                | 7     |
| Regional        | 0                    | 3                | 3     |
| International   | 0                    | 1                | 1     |
| Total           | 6                    | 5                | 11    |

65. **There are 11 companies capable of providing Security Operation Centre services into Pakistan. Seven operate in country**, one of which is a CREST-accredited international company, based in Karachi. **There are three regionally-based companies and one international company**, all of which are all CREST-accredited companies with the capability to offer their services into Pakistan at clients' request.

# 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

66. 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<sup>46</sup>.”
67. Responding to a cyber incident is challenging, as many organisations will not have effective cyber security controls in place. Depending on size, not all organisations will have a dedicated IT team with cyber security professionals employed in-house. 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.
68. There are **25 companies providing Incident Response Services into Pakistan**. Of the **eight companies operating in-country**, one is the **Pakistan Computer Emergency Response Team (PakCERT)**<sup>47</sup> and another **three are CREST-accredited**. There are **five regionally-based organisations**.

| Office Location | Non-CREST Accredited | CREST Accredited | Total |
|-----------------|----------------------|------------------|-------|
| In-country      | 5                    | 3                | 8     |
| Regional        | 0                    | 5                | 5     |
| International   | 1                    | 11               | 12    |
| Total           | 6                    | 19               | 25    |

69.





## **Dimension 4**

Cyber Security  
Professional Development

# Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 3*



70. **Education and professional development are both critical in providing students, from school age to adulthood, 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 them 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 for them, and unprotected data is equally valuable. To combat the threat, a country needs a vibrant cyber security industry with well-trained professionals.

71. To determine the health of cyber security professional development, there is a need to identify higher education establishments and professional training providers that offer cyber security qualifications and certifications, and exactly what is offered.

CREST examined what professional membership organisations were doing in Pakistan 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.

## Overall Assessment

72. Four of the six Professional Development Indicators are already at Level 3. The remaining two - specialist recruitment, and events and exhibitions - are at Levels 1 and 2 respectively. Considerable effort will be required for these indicators to reach level 3.

## Development Approach

73. Building the cyber security 'community' will take time and effort but will also make a real difference. A vibrant programme of events and exhibitions will be a big step forward, as will a healthy recruitment market connecting academia, employers, professional standards bodies and the National Cyber Training Program.

# Cyber Security Professional Development

## Indicator 4.1 Academia & Higher Education



### Assessment – Maturity Level 3

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.

### Academia and Higher Education

74. Higher education, taking place after secondary school in further education colleges or universities, aims to equip people with the skills and qualifications needed in workplaces or careers. Academia is the pursuit of research, higher level education and scholarship.
75. CREST's research sought to identify universities and colleges offering ICT or cyber courses and modules to students, and what level these courses were at – diploma, degree, masters etc. The more students graduating with ICT- or cyber-related degrees, potentially results in more people following an ICT-related career.
76. The table on the right shows approximate numbers of courses offered from the 23 universities and colleges CREST researched. Information on courses provided was taken from the institutions' websites, which was not all shown at the same level of detail, hence numbers are approximate. There is plenty of scope for increasing the number of cyber courses available to students.

|               | Unknown Level       | M Tech | BA/ BSc | Pg Dip | MSc | PhD | Total            |
|---------------|---------------------|--------|---------|--------|-----|-----|------------------|
| ICT Courses   | 4                   | 0      | 8       | 0      | 1   | 0   | 13 <sup>48</sup> |
| Cyber Courses | 1<br>(Cyber Scouts) | 1      | 8       | 0      | 6   | 0   | 16               |
| Total         | 5                   | 1      | 16      | 0      | 7   | 0   | 29               |

77. To address the lack of skilled cyber security professionals, the National Centre for Cyber Security is driving higher education in cyber security with several universities as academic partners, establishing cyber security labs in 11 of the universities, as well as new PhD and MS degrees (128 PhDs, and 96 MS Degrees)<sup>49</sup>.
78. The National Response Centre for Cyber Crime (NRC3)<sup>50</sup> runs Cyber Scouts<sup>51</sup>, a programme for school children to learn about cyber security, who then share their knowledge with friends and family, raising general awareness.

# Cyber Security Professional Development

## Indicator 4.2 Training Providers



### Assessment – Maturity Level 3

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.

### Training Providers

79. 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, where they were located and what cyber courses they were providing.
80. 23 cyber security training providers were found during CREST's research, which is encouraging, including:



**One CREST member company** offering instructor-led courses



Both CERTs and at least **two other providers also offer instructor-led training**



A few of the training providers **have extensive training portfolios**

Whilst evidence is limited, it appears that a few companies offer 'boot-camps' to encourage skills development.

81. In respect of online training, the most impressive initiative is the one-year courses offered by the government-backed National Cyber Training Program (NCTP)<sup>52</sup>. Established in June 2020, the NCTP is a free training programme for young people, delivering a one-year course in various cyber security areas such as penetration testing, coding or ethical hacking. Its vision is to reduce unemployment, create awareness of the cyber world and drive economic growth by encouraging the influx of foreign currency<sup>53</sup>. This positive initiative shows a drive to improve cyber security knowledge and promote the profession from the ground up.



# Cyber Security Professional Development

## Indicator 4.3 Professional Certifications



### Assessment – Maturity Level 3

Most International Certification Bodies (technical, management and audit) operate in-country take-up is developing but would not be classed as strong.

### Professional Certifications

82. Professional certifications provide evidence of the holder's skills in that subject area at the time of certification. In the cyber security industry, there is a multitude of different certifications, provided 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**.

83. 15 certification bodies were found during CREST's research.



Most offer certifications with online exams or through Pearson Vue or PSI test centres available in-country.



Some certifications requiring practical exams offer this element online or through connection to a remote network.

Some, such as CREST and Cisco, only offer exams at specific testing sites, with these bodies offering multiple sites across Asia. It is difficult to assess the actual take up of certifications, but there is a good mix available.

84. There are three active chapters (ISACA, CSA) based in Pakistan, with regular events involving members' meetings, university seminars and partnering with cyber security conferences. Several certification bodies organise training in Pakistan, either themselves or with accredited training partners.

# Cyber Security Professional Development

## Indicator 4.4 Professional Cyber Membership Organisations



### Assessment – Maturity Level 3

Some evidence of local cyber security membership organisations for individuals and/or companies.

### Professional Cyber Membership Organisations or Associations

85. Professional membership organisations or associations are usually focused on furthering the profession they represent. They provide membership by subscription. Membership benefits include gaining access to further professional development and training, access to discounted products and events, networking and collaboration with like-minded people and increasing professional credibility because of membership. These organisations can frequently be not-for-profit organisations.
86. 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 has sought evidence of any professional cyber membership organisations operating in Pakistan.

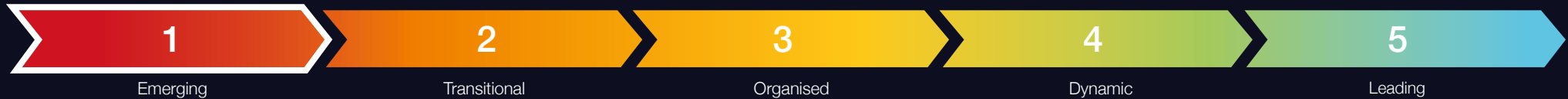
87.

There were **five professional cyber membership organisations identified in Pakistan**. Two local organisations, **Pakistan International Security Authority (PISA)**<sup>54</sup> and the **Global Information Security Society for Professionals of Pakistan (GISPP)**<sup>55</sup>, also have international expat membership.



# 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

88. The presence and activity 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 Pakistan or marketed cyber-qualified freelance professionals.

89.

**7** **Seven recruitment companies** were identified as operating within Pakistan. All were generic organisations recruiting for a variety of sectors. One was a regional company and all the rest were international organisations.

# Cyber Security Professional Development

## Indicator 4.6 Events & Exhibitions



### Assessment – Maturity Level 3

Evidence of regular locally-organised dedicated cyber security events/exhibitions being run in-country

## Events and exhibitions

90. **Events and exhibitions take a great deal of commitment, finances, advanced planning and organisation to bring to life, and 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 recently held in Pakistan, what level of event they were and how frequently they were held. This provides evidence of an appetite for cyber security knowledge and services. The impact of these events can be far reaching - as they are effective hubs for networking, collaboration and information sharing, which helps sow seeds of cyber security inspiration in their audiences.

91.

7

CREST's research found **seven events organised in recent years**. Some were purely for an in-country audience, while others attracted a regional or international audience. It is positive to see some international events run by organisations within Pakistan, such as PISA, and not just large international organisations.

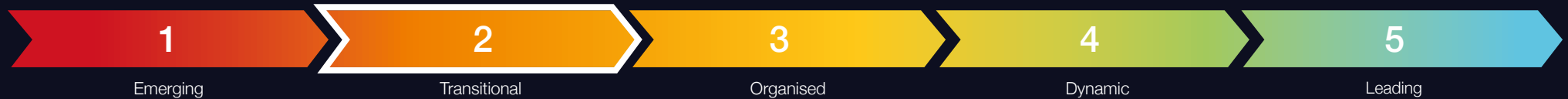


## **Dimension 5**

Banking Sector Cyber  
Security Posture

# Banking Sector Cyber Security Posture

## Overall Dimension Assessment: *Maturity Level 2*



93. As a means of assessing the current cyber security posture of Pakistan'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:

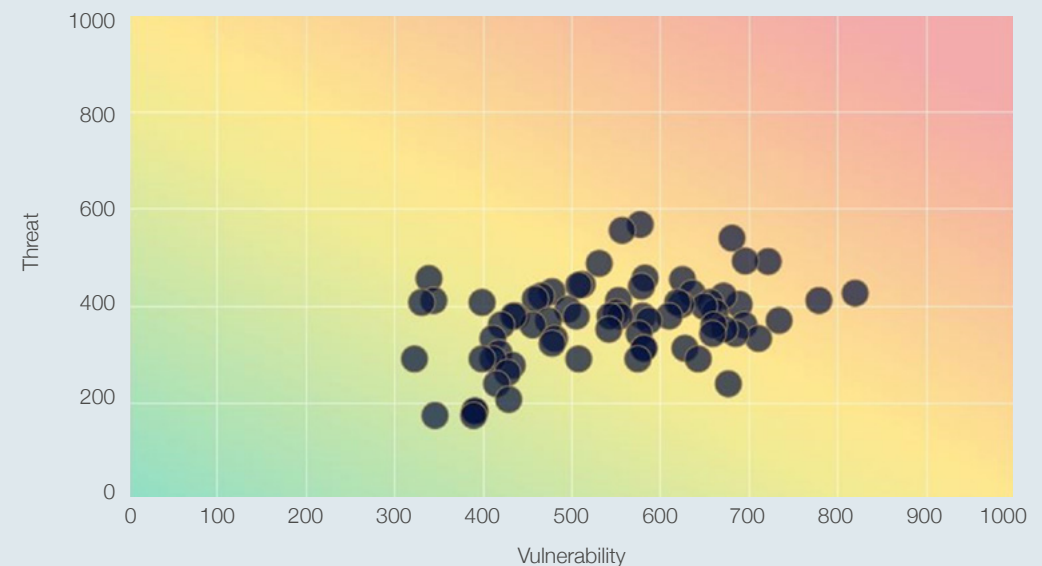
- The presence of vulnerabilities on public-facing IT infrastructure
- The presence of open ports on internet-facing servers
- The adoption of anti-phishing mechanisms, and
- Availability of breached employee credentials on online forums and marketplaces.

94. The results of the research into these four highlighted metrics are explained in more details in **Indicators 5.2 to 5.5**. For each institution, the 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**.

95. In determining the financial institutions to be assessed, the first source was the list of supervised institutions maintained by the State Bank of Pakistan<sup>56</sup>. This information was cross-checked against the membership list of Pakistan Banks' Association<sup>57</sup>, Wikipedia<sup>58</sup> and the websites of the financial institutions themselves to generate a representative sample of national and international banks and microfinance institutions operating in Pakistan.

### Comparative Risk Rating

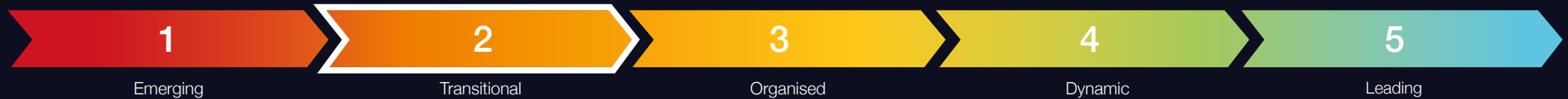
Figures represent CREST's cyber risk rating of each financial institution against a series of non-intrusive metrics



The website addresses and email domains of 73 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

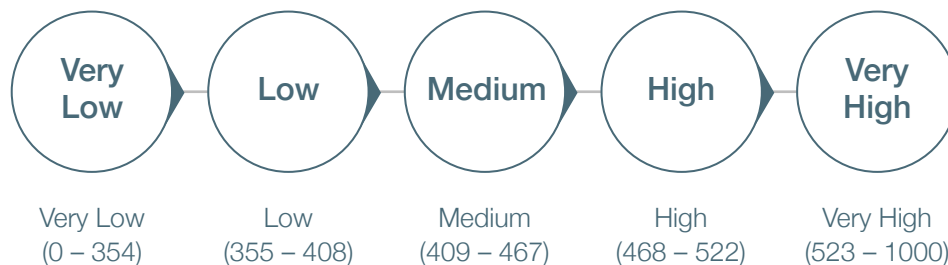
Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

### Banking Sector Cyber Risk Profile

96. The totality of 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.

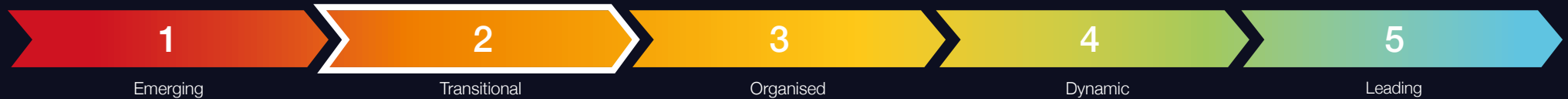
97. The scale CREST uses for rating cyber risk ranges between 0 (very lowest risk) and 1000 (very highest risk) and falls into five different rating bands:

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 322 and 820**. The **average cyber risk score** for the sample is **455**, which corresponds to a national average risk rating of **‘Medium’**.



# Banking Sector Cyber Security Posture

## Indicator 5.1 Banking Sector Cyber Risk Profile (continued)



### Assessment – Maturity Level 2

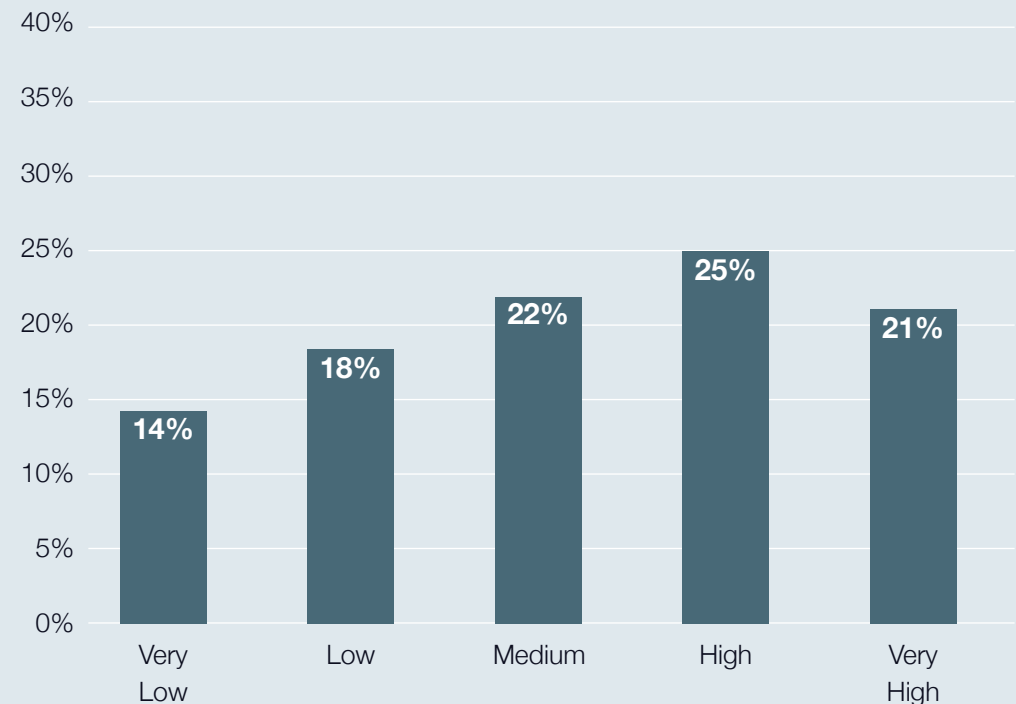
Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

98. Note that no active (intrusive) assessment was undertaken, nor was any assessment made of IT infrastructure elements that are not internet-facing. It may well be that if a comprehensive assessment were made of entire IT infrastructures, internet-facing and otherwise, that results may have differed. However, the levels of access required for such a task are far beyond the scope of this report.

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 individual financial institutions, particularly in those with a **'High'** or **'Very High'** risk rating.

99. A breakdown by category of risk rating of the assessed sample of financial institutions is shown above, and the results anonymised. Encouragingly, **32%** of the financial institutions have an overall cyber risk rating of **'Very Low'** or **'Low'**. Yet **46%** of the financial institutions have an overall cyber risk rating of **'Very High'** or **'High'**. Institutions in these latter two categories appear not to be implementing good cyber hygiene practices and/or operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.

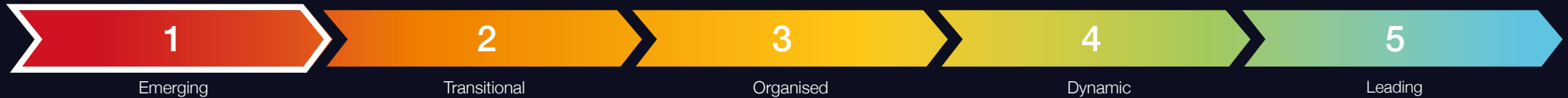
**Breakdown of Pakistan's Financial Institutions by Category of Risk Rating**





# Banking Sector Cyber Security Posture

## Indicator 5.2 Infrastructure Vulnerability Risk



### Assessment – Maturity Level 1

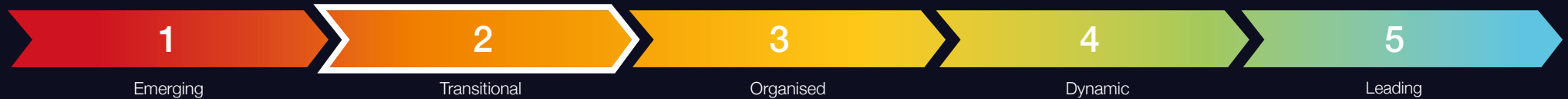
Infrastructure vulnerability risk is assessed as very poor; more than 20% of the surveyed financial institutions had critical known vulnerabilities on their IT infrastructure and/or more than 55% had any known vulnerabilities.

### Infrastructure Vulnerability Risk

100. 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 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.
101. Vulnerabilities, often referred to as CVEs<sup>59</sup>, (Common Vulnerabilities and Exposures) are flaws in software and hardware that cybercriminals constantly 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 73 of Pakistan's financial institutions being assessed. By restricting themselves to passive reconnaissance only, researchers were unable to confirm if the vulnerabilities they detected existed. There is a possibility that in some cases they were false positives.
102. **The investigation revealed that 54% of Pakistan's financial institutions appear to operate an unsecure internet-facing infrastructure that features at least one known vulnerability.** The vulnerabilities detected mostly have patches available. Their presence on an internet-facing infrastructure suggests lax patching practices.
103. 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<sup>60</sup> (Common Vulnerability Scoring System). 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 by which they can be exploited, or the access they provide when successfully exploited. **CREST's research identified that 24% of Pakistan's assessed financial institutions were found to be operating internet-facing IT infrastructure that contained 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; 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.

### Architecture & Access Risk

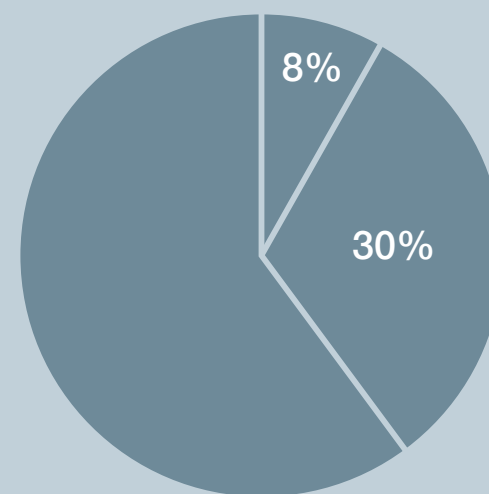
104. Security architecture and access management are the most common means of securing networks and information. “Security by design” is the essential foundation upon which all other cyber defences are built. Insufficient segregation between key assets and unguarded routes to gain unauthorised access are examples of gap that can be exploited by an attacker. Ethically, researchers were limited to only examine those assets directly connected to the internet. They therefore 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 taken to security by design.
105. 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. Traffic [data] going in and out of these ports can be guarded by mechanisms such as firewalls.
106. 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 that cybercriminals scan for CVEs (see **Indicator 5.2**), they routinely scan the internet to identify open ports which they can target to gain a foothold into the corporate network.
- 107.
-  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 also look to 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)

108. **CREST's research showed that 8% of the assessed financial institutions maintain at least one port associated with remote access services open to the internet.** In most cases these ports will have been configured to accept incoming data packets from the internet for valid business requirements and will have adequate security measures in place. Although those banks that have open remote access ports on their IT infrastructure remain susceptible to a potential compromise, they are a small subset. Evidence suggests Pakistan's financial services sector is not highly vulnerable to the threat emanating from ports associated with remote access services.
109. Another set of ports on computer servers that cybercriminals often deliberately target are those used by database services. **CREST's research showed that 30% of the assessed financial institutions have at least one database-related port open on their public-facing infrastructure.** As above, although some of these internet-accessible database services are in place to meet valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.
110. 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 even more direct and imminent risk. This is mostly because the database services associated with the ports often lack authentication protocols by default, allowing unauthorised third parties to easily access and retrieve content.
111. Understanding the threat associated with exposed database instances - and reducing the possibility of suffering a data leak - also reduces the risk of fines under Pakistan's Personal Data Protection Bill 2020<sup>61</sup>, once it becomes law and takes effect.

Pakistan's financial institution Access risk - open ports



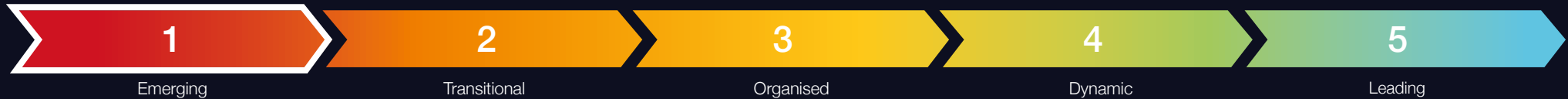
### Key

8% - have remote access services open to the internet

30% - have at least one database-related port open to the internet

# Banking Sector Cyber Security Posture

## Indicator 5.4 Email Authentication Risk



### Assessment – Maturity Level 1

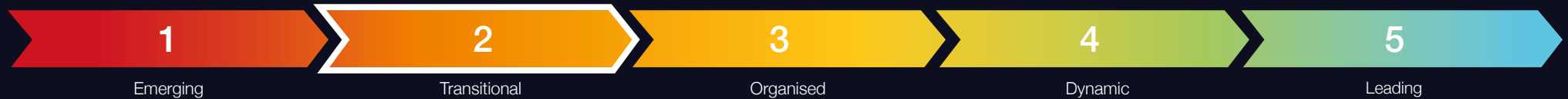
Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

### Email Authentication Risk

112. **Having an inherent susceptibility to social engineering and phishing campaigns is human nature.** While training and education can help prevent successful attacks, the use of 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 gained.
113. **Sender Policy Framework (SPF) and Domain-based Message Authentication, Reporting & Conformance (DMARC)** are authentication mechanisms organisations can use to secure email traffic. They work together to ensure email domains are not used fraudulently, preventing spoofing risk and helping block spam messages, malware and phishing attempts.
114. 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<sup>62</sup>.
115. Having SPF and DMARC correctly enabled does not entirely negate the threat of phishing. But it does reduce the chance of falling victim to impersonation attempts and business email compromise (BEC) scams. Both are common threats in the financial services sector<sup>63</sup>.
116. In a BEC scam, cybercriminals target victims with spear-phishing emails devised to impersonate the company's CEO, an employee with authority to approve money transfers, or a key supplier, for example. The aim is to trick recipients into wiring funds to bank accounts under the cybercriminal's control or revealing sensitive information that could prove useful in further malicious operations. BEC scams are highly profitable for cybercriminals. **In its 2019 Internet Crime Report, the FBI estimated that globally BEC scams cost businesses approximately US\$1.8 billion**<sup>64</sup>.
117. **72%** CREST's research revealed that **72% of the sample of financial institutions 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

118. **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 as a result 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's easier to spot instances of login credential exposure and this is often used as a measure of the problem.
119. **Employees often use their work email address to sign-up for third-party websites** – not only professional platforms but also leisure-oriented services. However, these platforms and services can expose users' sensitive information in data breaches caused by either a malicious external compromise or internal negligence.

79%

CREST's research revealed that **79% of the assessed financial institutions had had at least some employees' credentials leaked online** after unconnected attacks on third-party website-based service providers.

120. 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 may also lead to more sophisticated phishing efforts, with cybercriminals using the exposed information to craft highly convincing malicious messages luring recipients into providing access or revealing additional data.
121. It has not been possible to verify how many assessed financial institutions follow good hygiene practices and enforce strong password best practices. These measures may help mitigate the threat associated with third-party leaked credentials.

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

# Banking Sector Cyber Security Posture

## Mitigation Measures

122. 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, including:

### Infrastructure Vulnerability

- Implement effective patching and software updating routines and ensure the vulnerabilities of highest severity and those 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 not required.
- For internet-accessible instances, 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 the 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 associated with using business email accounts on third-party services.
- Establish and enforce a strong password policy to reduce password re-use.
- Implement additional security measures, such as multi-factor authentication.



Appendices



# Appendix A

## Glossary

|                        |   |  |   |
|------------------------|---|--|---|
| <b>Anti-phishing</b>   | Mechanisms and processes to defend against phishing attacks: see phishing   | <b>FIRST</b>                                 | Forum of Incident Response & Security Teams: an international association of CERTs/CSIRTs   |
| <b>BEC</b>             | Business Email Compromise: a form of scam in which the cybercriminal seeks to obtain an unauthorised money transfer into an account which they control                    | <b>Indicator</b>                             | 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 |
| <b>CERT</b>            | Computer Emergency Response Team  | <b>Information Exchange</b>                  | A semi-formal mechanism for experts in different organisations to exchange information on observed cyber security threats, vulnerabilities and incidents                            |
| <b>CMAGE</b>           | Cyber Security Maturity Assessment for Global Ecosystems  | <b>International (service provider)</b>      | A cyber security service provider headquartered elsewhere with offices in multiple countries which offers the service remotely or through a visiting employee                       |
| <b>CSIRT</b>           | Computer Security Incident Response Team  | <b>IR</b>                                    | Incident Response: a category of cyber security service   |
| <b>Dimension</b>       | 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               | <b>Local (service provider)</b>              | A cyber security service provider with one or more in-country office(s): company may additionally be classed as international, regional or locally registered                       |
| <b>DMARC</b>           | Domain-based Message Authentication, Reporting & Conformance: an advanced form of email authentication  | <b>Locally registered (service provider)</b> | A cyber security service provider which is registered and headquartered in the country  |
| <b>Ecosystem</b>       | 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 | <b>Malware</b>                               | Malicious software intentionally designed to cause damage to a computer or network  |
| <b>Ethical Hacking</b> | An alternative name for Penetration Testing: see PenTest  |  |   |



# Appendix A

## Glossary (continued)

|  |  |
|--|--|
| <b>Multi-factor authentication</b>     | 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   |
| <b>PenTest</b>                         | 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   |
| <b>Phishing</b>                        | A process by which a cybercriminal attempts to obtain sensitive information, such as usernames, passwords and credit card details, by disguising themselves as trustworthy   |
| <b>Port</b>                            | A physical or virtual connection to a computer server through which different categories of information or instructions are sent and received  |
| <b>Public-facing / Internet-facing</b> | Those elements of a computer system software (and/or hardware) to which there is (paid or free) public access, often via an internet connection: distinct from those elements of a computer system which can only be accessed by authorised internal staff |
| <b>Regional (service provider)</b>     | A cyber security service provider with an office in an adjacent country which offers the service remotely or through a visiting employee   |
| <b>Scam</b>                            | A deceptive scheme or trick used to cheat an organisation or individual out of something, especially money   |
| <b>SFP</b>                             | Sender Policy Framework; a basic form of email authentication  |
| <b>SOC</b>                             | Security Operations Centre: a facility in which a team monitors an organisation's cyber security on an ongoing basis: facility can be in-house, or outsourced to a cyber security service provider   |
| <b>Spear-Phishing</b>                  | A highly targeted attempt at phishing in which the cybercriminal often uses known information to add authenticity to a malicious communication   |
| <b>Spoofing</b>                        | 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  |
| <b>Third-party breach</b>              | 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                                  |
| <b>TI</b>                              | (Cyber) Threat Intelligence; a category of cyber security service  |
| <b>VA</b>                              | 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. Healthy 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 <a href="https://www.enisa.europa.eu/publications/study-on-csirt-maturity">https://www.enisa.europa.eu/publications/study-on-csirt-maturity</a> ). | 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

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

##### Level 4

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.

##### Level 3

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.

##### 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.

##### Level 1

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 when determining who to hire or promote. They are also used by buyers when selecting service providers. Experience is a matter of record that can be 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 the certifications they hold. Buyers can also use certifications as a benchmark when looking to award a contract. The availability and use of certifications in both scenarios is a useful indicator of the maturity of a marketplace.

### Career progression model

2. For ease of evaluation, various 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 as 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 as 'Other Certificates of Relevance'). In some cases, certification organisations also act as professional membership organisations, holding events and contributing to through-career development of members.
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 a physical testing site for which there is limited availability in Pakistan.
5. 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 (also 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 <sup>65</sup>                   |                       | CPSA<br>CPIA<br>CPTIA   | CRT<br>CRTIA<br>CRTSA<br>CRIA<br>CC NIA<br>CCHIA<br>CCMRE   | CCSAS<br>CCSAM<br>CCTIM, CCIM<br>CCT Inf<br>CCT App<br>CCWS | Fellow                           |               | ✓                  |                 |                    | ✓                      |
| EC Council <sup>66</sup>              | CEH<br>CND<br>ECSS    | ECSA<br>ECIH<br>EDRP<br>CASE-Java<br>CASE-.Net<br>ECES<br>CTIA  | APT<br>LPT<br>CHFI<br>CAST<br>CEH(Master)<br>CSA  | ECDA<br>ECTI  |                                  | ✓             | ✓                  |                 | ✓                  |                        |
| ISACA <sup>67</sup>                   |                       | CSX-P   | CISA<br>CRISC<br>CISM   |   | CGEIT                            | ✓             |                    | ✓               |                    |                        |
| (ISC)2 <sup>68</sup>                  |                       | HCISPP<br>SSCP<br>CAP   | CISSP<br>CCSP<br>CSSLP  |   | CISSP-AP<br>CISSP-EP<br>CISSP-MP |               | ✓                  |                 |                    |                        |
| SANS <sup>69</sup>                    |                       | GSEC<br>GWAPT<br>GCIP<br>GCUX<br>GPYC<br>GCIH<br>GASF<br>GCFA<br>GSSP-Java<br>GSSP-.Net<br>GICSP<br>GBFA<br>GCSA<br>GPEN<br>GICSP<br>GCWN<br>GAWN<br>GWEB<br>GCFE<br>GREM<br>GNFA<br>GMOB<br>GCSA | GXPB<br>GCCB<br>GSED<br>GPPA<br>GMON<br>GCI<br>GCTI<br>GDS<br>GDAT<br>GNSA<br>GCCC<br>GPPA<br>GCI<br>GCDA<br>GCED<br>GDSA<br>GEVA |   | GSE                              | ✓             | ✓                  |                 |                    |                        |
| CompTIA <sup>70</sup>                 | Pentest+<br>Security+ | CySA+   | CASP+   |   |                                  | ✓             | ✓                  |                 |                    |                        |
| Offensive Security <sup>71</sup>      |                       | OSCP<br>OSWP  | OSCE<br>OSWE  | OSEE  |                                  | ✓             |                    |                 |                    |                        |
| Cloud Security Alliance <sup>72</sup> |                       | 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 <sup>73</sup>                    |                               | PCIP<br>PCI-DSS QPA  | PCI-DSS ISA<br>PCI-DSS AQSA                  |                    | PCI-DSS QSA<br>PA-QSA<br>PCI-DSS 3DS<br>PCI-DSS P2PE<br>PCI-DSS Secure<br>Software Lifecycle<br>Assessor<br>PCI-DSS Secure<br>Software Assessor<br>PCI-DSS CPSA | ✓             | ✓                  |                 |                    |                        |
| Cisco <sup>74</sup>                  |                               | CCNA<br>CC CyberOps<br>Associate   | CCNP Security<br>CC CyberOps<br>Professional | CCIE Security      |   |               | ✓                  |                 |                    | ✓                      |
| Microsoft <sup>75</sup>              | MTA: Security<br>Fundamentals | Azure Security<br>Engineer Associate<br>Microsoft 365<br>Security Administrator<br>Associate |  |                    |   | ✓             | ✓                  |                 |                    |                        |
| Amazon Web<br>Services <sup>76</sup> | AWS Certified<br>Security     |  |  |                    |   | ✓             | ✓                  | ✓               |                    |                        |
| OTHER CERTIFICATES OF RELEVANCE      |                               |  |  |                    |   |               |                    |                 |                    |                        |
| EC Council                           | CNDA<br>CSCU                  |  |  | CCISO              |   | ✓             | ✓                  |                 | ✓                  |                        |
| ISACA                                |                               | Cybersecurity Audit<br>Scheme<br>COBIT Program   | CDPSE  |                    |   | ✓             |                    | ✓               |                    |                        |
| (ISC)2                               | Associate of (ISC)2           |  |  |                    |   |               | ✓                  |                 |                    |                        |
| SANS                                 | GISF                          | GLEG<br>GSNA   | GISP<br>GCPM                                 | GSLC               | GSTRT   | ✓             | ✓                  |                 |                    |                        |
| IRCA (ISMS) <sup>77</sup>            | Associate Auditor             | Internal Auditor   | Auditor                                      | Lead Auditor       | Principle Auditor   |               |                    |                 | ✓                  |                        |
| BCS <sup>78</sup>                    | CSMP                          | BCM<br>CIAA  | CIRM   |                    |   |               | ✓                  |                 | ✓                  | ✓                      |
| IET <sup>79</sup>                    | ICTTech                       |  |  |                    |   |               |                    |                 |                    | ✓                      |

# Appendix D

## Country Context

### Geography

1. Pakistan sits to the north east of India. It achieved independence in 1947. Iran sits to Pakistan's west, Afghanistan to the northwest and north, China to the northeast. The coast of the Arabian Sea forms Pakistan's southern border<sup>80</sup>.
2. Pakistan has a diverse geography of mountain ranges. The famous Himalayas and Khartoum ranges lie on the north boundary and the Western and Safid Mountain range are to the west, bordering Afghanistan. Valleys, plateaus and a large flat flood plain around the Indus River make up the rest of the country's terrain. Around 3/5ths of the country is rough mountainous terrain and 2/5ths is level plain<sup>81</sup>.
3. The capital is Islamabad, which sits in the very north of the country. Karachi, in the south, is Pakistan's most populous city, with a population of 16,093,786. Other major cities include Lahore, Faisalabad, Rawalpindi, Gujranwala, Peshawar, Multan, Hyderabad and then Islamabad which has an estimated population of 1,129,198 as at 2020<sup>82</sup>.



4. Map showing Pakistan's key geographical features and major conurbations.

### Natural resources

5. Pakistan has several natural resources, including iron ore, copper, enormous quantities of limestone (used in the cement industry) oil, natural gas, coal (poor quality), and other minerals which are exported. Most seem to be under exploited resources.<sup>83</sup>

### Population

6. The population of Pakistan was estimated in 2019 to be 219,382,000 and in 2020, 222,862,646<sup>84</sup>. Pakistan's population is growing rapidly and is expected to surpass the population of Indonesia by 2048. It is currently ranked the fifth largest population in the world<sup>85</sup>, with two thirds of the population under 30 years old; 32.5% under 15; 28.2% aged between 15 and 19yrs, and 21.6% aged between 30 and 44<sup>86</sup>. In 2016, the population split between urban and rural living was 44.3% urban and 55.7% rural<sup>87</sup>.
7. Education is not compulsory in Pakistan and after primary school there are considerably less girls in education<sup>88</sup>. In 2015, literacy rates were 72.2% male and 47.3% female<sup>89</sup>. There are many languages spoken. Urdu is the official language. English is spoken widely<sup>90</sup>.

### Economy

8. Pakistan has a mixed economy. Agriculture used to hold the biggest share of GDP but is now only approximately one-fifth of GDP. Manufacturing is approximately one-sixth of GDP. Trade and services combined constitute the largest component of the economy<sup>91</sup>.

# Appendix D

## Country Context (continued)

9. According to Macrotrends, in 2017 Pakistan's Gross National Income (GNI) was US\$311.26bn and US\$1,500 per capita. In 2018, GNI was US\$377.07bn and US\$1590 per capita, representing an increase of 8.29% on 2017 and a growth rate of 5.69%. In 2019, GNI was US\$331.62bn and US\$1530 per capita, a decline of 1.62% on 2018 but still a growth rate of 2.32%<sup>92</sup>. GDP for 2019 was 0.99%, a 4.85% decline from 2018<sup>93</sup>.
10. The World Bank's overview on Pakistan states that real GDP growth is estimated to have declined 1.9% in 2019 to -1.5% in 2020. This reflects the effects of the COVID-19 pandemic and restrictions which have disrupted supply and demand. While domestic economic activity will recover as COVID-19 restrictions ease, Pakistan's economic prospects will remain subdued. Economic growth is projected to be below potential, averaging 1.3% for Financial Year 2021-22<sup>94</sup>.
11. The banking sector in Pakistan has suffered some serious cyber security breaches in the past few years. In 2018, US\$6 million was lost in cyberattacks, as online security measures failed to prevent security breaches in which overseas hackers stole customer's data<sup>95</sup>.

### Internet connectivity

12. In the article **"Pakistan's Great Digital Divide"** published in The Diplomat in July 2020, it was stated that around 35% of Pakistan lacks intranet infrastructure, partly due to the rural - urban divide, geography, and a lack of electricity and telecommunications infrastructure in large parts of the country. In some regions, internet access is purposefully cut off or restricted due to security concerns. Only 78 million people have access to broadband, and 76 million have access to mobile connectivity (3 and 4G)<sup>96</sup>. According to the Inclusive Internet Index 2020, Pakistan ranks 76th of 100 countries and 24th of the 26th Asian Countries, with low levels of digital literacy and poor quality of networks being major impediments<sup>97</sup>.

### Cyber crime

13. According to a 2018 article in Pakistan Today, in 2018 the FIA's Cybercrime wing conducted 2,295 inquiries, registered 255 cases and arrested 209 people, an increase on 2017 statistics and the highest figures since the Prevention of Electronic Crime Act was passed in 2016. Pakistan established 15 new cybercrime reporting centres in the same year, to assist in the reporting and handling of cybercrime<sup>98</sup>.
14. An article in ProPakistani cited a recent report that ranked Pakistan as the seventh worst of 60 countries in 2018 regarding cybersecurity<sup>99</sup>. The report quoted is by Comparitech, since updated in 2020, which now ranks Pakistan as the eighth worst country, which shows an improvement<sup>100</sup>.
15. A 2020 article "The Cyber Threat Facing Pakistan" states Pakistan is one of the top targets for foreign espionage. It suggests Pakistan needs to invest in more resources, develop a strong cybersecurity framework and update its legislation. The most recent legislation linked to cybersecurity is the 2016 Prevention of Electronic Crimes Act. While Pakistan has a National Response Centre for Cyber Crime (NRC3), this body lacks the capacity to effectively deal with and protect the nation from cybercrime due to insufficient resources<sup>101</sup>.
16. A 2018 Threat Intelligence Analysis report from PakCERT analysed incidents in October 2018 where data stolen from approximately 19,864 customer's debit cards of 22 Pakistani banks was being sold on the dark web for US\$100-160 per card<sup>102</sup>. An article in 2018 by Cybersecurity Insiders states that after receiving thousands of complaints, Bank Islami launched a probe into the same incident and discovered that US\$3m worth of transactions had been made by the international fraudsters using the stolen card details<sup>103</sup>.

# Appendix D

## Country Context (continued)

17. In May 2020, more than 115 million mobile subscriber's details (including full name, home address, mobile number and Computerised National Identity Card (CNIC) number) were stolen. Cybercriminals tried to sell the package for 300 bitcoins - the equivalent of US\$2.1 million. At the time of the CPO magazine article exposing the breach, (cited below), investigations were ongoing and none of the affected mobile data operators had admitted the data breach or provided any directives to affected users. The data stolen was dated 2013. Initial thoughts are that the data was possibly derived from a breach of an old back up file<sup>104</sup>.
18. In an **Express Tribune article dated January 2021**, it noted that cybercrime quintupled during the pandemic in 2020 compared to previous years. The article states: "According to the data published by the FIA Cybercrime Wing, as many as 94,227 complaints of web-based crime including fraud...and access to unauthorized accounts were received in 2020 which was 5% higher than the previous year."
19. In 2019 the Federal Investigation Agency (FIA) received 56,000 cybercrime complaints. In comparison, reports in 2020 revealed a 50% decrease during lockdown. Before lockdown, in March 2020, a total of 923 complaints (154 banking, 130 website fraud, 497 mobile banking, 141 media) were received. During the 2020 lockdown, a total of 488 complaints (89 online banking, 70 website, 273 mobile banking, 50 social media) were received<sup>105</sup>.

### Cyber Security Professional Development

20. No online articles were found during CREST's research regarding the state of Pakistan's Cyber Security Professional Development.

### Other maturity models

21. Other cyber security maturity models or indexes that were looked at during the research are as follows:
22. The Global Cybersecurity Index 2018, published in 2019 by the International Telecommunication Union (ITU), rates Pakistan for Cyber Security as 18th out of 38 countries in the Asia Pacific Region and 94th of 175 countries globally<sup>106</sup>. It also classes Pakistan as a country with a medium commitment to cybersecurity, defined as: "Countries that have developed complex commitments and engage in cybersecurity programmes and initiatives"<sup>107</sup>.
23. As of 23 March 2020, The National Cyber Security Index (NCSI) by the e-Government Academy Foundation ranks Pakistan as 65th of 160 in its world ranking. Rankings are decided against performance of four general cyber security indicators, four baseline cyber security indicators and four incident response and crisis management indicators<sup>108</sup>.

24. The Inclusive Internet Index 2020 ranks a country's internet provision by: availability (quality and breadth of infrastructure); affordability (cost of access relevant to income); relevance (extent of local language content) and readiness (capacity to access the internet). Pakistan is ranked 77th of 100 countries<sup>109</sup>.
25. There is currently no published CMM Cyber Maturity Model (CMM) by the Global Cyber Security Capacity Centre on Pakistan<sup>110</sup>.

# 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 separately, and can be made available upon request to CREST.

Ahmed, Qazi Mohammad Misbahaddin, (2018). Analysis of the Recent Attack on Pakistan Banks. *PakCERT Threat Intelligence Report PCTI-2018-0111* (online) <https://www.pakcert.org/img/PakCERT%20Threat%20Intelligence%20Report%20-%20web.pdf> (accessed 30 Dec 20)

APCERT Cyber Drill 2020, (2020). Press Release, Bankers Doubles Down on Miner. Asia-Pacific Region: *Author*. [https://www.apcert.org/documents/pdf/APCERT\\_Drill2020\\_Press%20Release.pdf](https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf) (accessed Dec 20)

Asia Pacific CERT (APCERT). <https://www.apcert.org> (accessed July and Dec 20)

Baloch Shah Meer, Musyani Zafar (8 July 2020). Pakistan's Great Digital Divide. Washington USA: *The Diplomat*. <https://thediplomat.com/2020/07/pakistans-great-digital-divide/> (accessed Dec 20)

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

Bischoff Mark (3 Mar 2020). Which Countries have the worst (and best) Cyber Security? UK: *Comparitech*. <https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/> (accessed 27 Dec 20)

Centre for Strategic and International Studies, (2020). Global Cyber Strategies Index. Washington USA: *Author*. <https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/global-cyber-strategies-index> (accessed 27 Dec 20)

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

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

European Union Agency for Network and Information Security (ENISA), (2019). ENISA CSIRT Maturity Assessment Model. Greece: *Author*. <https://www.enisa.europa.eu/publications/study-on-csirt-maturity> (Accessed 23 Dec 2020)

Federal Investigation Agency, Ministry of Interior, Government of Pakistan. <http://fia.gov.pk/>

Federal Investigation Agency, National Responses Centre for Cyber Crime, Pakistan: *Author*. <http://www.nr3c.gov.pk/cscouts.html> (accessed July and Oct 2020)

Forum of Incident Response Teams (FIRST), (2015-2020). <https://www.first.org/about/mission> (accessed 26 Oct 2020)



# Appendix E

## Bibliography (continued)

Goud, Naveen (2018).

Almost all Banks in Pakistan became victims to Cyber Attack. *Cybersecurity Insiders (online)*

<https://www.cybersecurity-insiders.com/almost-all-banks-in-pakistan-become-victim-to-cyber-attack/> (accessed May and Dec 20)

Government of Pakistan (2016).

The Prevention of Electronic Crimes Act (2016),

*Pakistan: Laws Of Pakistan (online)*

<http://www.lawsofpakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf> (accessed Dec 20)

Government of Pakistan, (2018).

The Prevention of Electronic Crimes Investigation Rules of 2018, Pakistan: *Federal Investigation Agency (FIA) (online)*

<http://www.fia.gov.pk/en/law/PECARULES.pdf> (accessed Jul and Dec 20)

Global Cyber Security Capacity Centre, Oxford, *Author*.

<https://gcsc.web.ox.ac.uk/cmm-reviews> (accessed Nov 20)

Global Information Security Society for Professionals of Pakistan (GISPP),

Pakistan, *Author*,

<https://www.gispp.org/> (accessed Dec 20)

Hope Alice, (15 May 20).

Information of Over 115 Million Pakistani Mobile Subscribers Exposed in a Massive Data Leak.

*CPO Magazine (online)*

<https://www.cpomagazine.com/cyber-security/information-of-over-115-million-pakistani-mobile-subscribers-exposed-in-a-massive-data-leak/> (accessed May and Dec 20)

Ifra, Erum (2016) Perspectives from Pakistan Women in ICT Engineering.

Switzerland: *International Telecommunication Union (ITU)*.

<https://news.itu.int/perspectives-from-pakistan-women-in-ict-engineering/> (accessed 27 Nov 2020)

International Telecommunication Union (2019). Global Cybersecurity Index 2018,

Switzerland: *Author*,

[https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf) (accessed Dec 20)

ISACA (2020). USA.

[www.isaca.org](http://www.isaca.org) (accessed Dec 20)

ISO 27000 Series – Information Technology, Security Techniques, Information Security Management Systems, Requirements.

Switzerland: *ISO*.

<https://www.iso.org/standard/54534.html> (accessed Dec 20)

Khali, Basma (22 Mar 2020) Cybercrime effecting banking sector / economy of Pakistan.

*Modern Diplomacy (online)*

<https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/> (accessed 30 Dec 20)

Macrotrends, (2020).

Pakistan 2020. *Author (online)*

<https://www.macrotrends.net/countries/PAK/pakistan/> (accessed 30 Dec 20)

Ministry of Interior, Government of Pakistan (2020).

Personal Data Protection Bill 2020, Consultation Draft: V2. 09.04.2020.

Pakistan: *Author*. Ch VI Para 32 p21.

<https://moitt.gov.pk/SitelImage/Downloads/Personal%20Data%20Protection%20Bill%202020%20Updated.pdf>

National Cyber Security Centre (NCSC),

*Author*, UK,

<https://www.ncsc.gov.uk/> (accessed Nov 2020)

National Centre for Cyber Security (NCCS),

*Author*, Pakistan,

<https://www.nccs.pk/> (accessed Dec 2020)

National Cyber Security Index, (2020) Pakistan.

Estonia: *e-Governance Academy Foundation*,

<https://ncsi.ega.ee/country/pk/> (Accessed Nov 2020)

National Cyber Training Programme (NCTP),

<https://www.nctp.pk/> (accessed Jul and Dec 20)

# Appendix E

## Bibliography (continued)

National Institute of Standards and Technology (NIST) (2020). USA.

<https://www.iso.org/standards.html>

(accessed Dec 20)

National Response Centre for Cyber Crime (NRC3)

<http://www.nr3c.gov.pk/> (accessed Jul and Dec 20)

National Response Centre for Cyber Crime.

Cyber Scouts. *author*,

<http://www.nr3c.gov.pk/cscouts.html>

(accessed July and Dec 20)

Onsite,

<https://www.onsite.com.pk>

(accessed July and Nov 2020)

Organisation of the Islamic Cooperation CERT

(OIC-CERT)

<https://www.oic-cert.org/en>

(accessed Dec 20)

PakCERT,

<https://www.pakcert.org>

(accessed July and Nov 2020)

Pakistan International Security Authority (PISA)

<http://www.pisa.org.pk/>

(accessed July and Dec 20)

Pakistan Telecommunications Authority (PTA), (2019).

Annual Report 2018-2019. Pakistan. *Author*.

<https://pta.gov.pk/en/data-&-research/publications/annual-reports>

(accessed Dec 20)

Pakistan Today (2018).

FIA says record number of cybercrimes reported in 2018.

*Author (online)*

<https://www.pakistantoday.com.pk/2018/10/23/fia-says-record-number-of-cyber-crimes-reported-in-2018/amp/> (accessed Jul and Dec 20)

Qadeer Muhammad Abdul (2020).

The Cyber Threat Facing Pakistan.

Washington, USA: *The Diplomat*.

<https://thedi diplomat.com/2020/06/the-cyber-threat-facing-pakistan/> (accessed Dec 20)

UN, 'UNDIR Cyber Security Portal (2020). Pakistan'

*Author*.

<https://unidir.org/cpp/en/states/pakistan>

(accessed 27 Nov 2020)

Shabbir Ambreen, (2018).

Pakistan Rated 7th Worst is Cyber Security.

*ProPakistani (online)*,

<https://propakistani.pk/2019/02/14/pakistan-ranked-7th-worst-in-cyber-security-report/>

(accessed 27 Dec 20)

State Bank of Pakistan (2004).

Guidelines on Information Technology Security.

Pakistan: *Author. (online)*

[https://www.sbp.org.pk/bsd/2004/Guidelines\\_on\\_IT\\_Security.pdf](https://www.sbp.org.pk/bsd/2004/Guidelines_on_IT_Security.pdf) (accessed Dec 20)

State Bank of Pakistan (2016).

Prevention Against Cyber Attack.

Pakistan: *Author, BPRD Circular No. 07 of 2016. (online)*

<https://www.sbp.org.pk/bprd/2016/C7.htm>

(accessed Dec 20)

State Bank of Pakistan, (2017).

Enterprise Technology Governance & Risk Management Framework for Financial Institutions.

Pakistan: *Author, BPRD Circular no 5 of 2017.*

<https://www.sbp.org.pk/bprd/2017/C5.htm>

(accessed Dec 20)

State Bank of Pakistan. (2018)

Security of Digital Payments.

Pakistan: *Author, PSD Circular no 9 of 2019.*

<https://www.sbp.org.pk/psd/2018/C9.htm>

(accessed Dec 20)

State Bank of Pakistan (2020).

Measures to Enhance Cyber Resilience amid Covid-19

Threat. Pakistan: *Author, PSD - Circular no 3 of 2020.*

<https://www.sbp.org.pk/psd/2020/C3.htm>

(accessed Dec 20)

Syed Rubab, Khaver Ahmed Awais, Yasin Muhammad,

(2019). Cyber Security: Where Does Pakistan Stand?.

Pakistan: *Sustainable Development Policy Institute (SDPI). (online)*

<https://think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1>

# Appendix E

## Bibliography (continued)

The Inclusive Internet 2020, Pakistan,  
<https://theinclusiveinternet.eiu.com/explore/countries/PK/> (accessed Dec 20)

The Express Tribune, (2020) Cybercrime Registers Sharp Decline Amid Covid-19 Lockdown. *Author*  
<https://tribune.com.pk/story/2213373/1-cybercrime-registers-sharp-decline-amid-covid-19-lockdown?amp=1> (accessed July and Dec 20)

The Securities and Exchange Commission of Pakistan (2020). Guidelines on Cybersecurity Framework for the Insurance Sector 2020.  
Pakistan: *Author (online)*.  
<https://www.secp.gov.pk/document/sec-guidelines-on-cybersecurity-framework-for-the-insurance-sector-2020/?wpdmdl=38763&refresh=5febaea1501331609281185> (accessed Dec 20)

TF-CSIRT,  
<https://tf-csirt.org/tf-csirt/>  
(accessed Dec 20)

World Bank, (2020).  
Pakistan Overview, *Author. (online)*  
<https://www.worldbank.org/en/country/pakistan/overview>  
(Accessed Nov 2020)

World Population Review,  
Pakistan Population 2020, *Author*  
<https://worldpopulationreview.com/world-cities/karachi-population>  
(accessed Nov 20)  
Ziring, Lawrence (2020) Pakistan.  
Chicago USA: *Britannica*  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)



# 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.

<sup>1</sup> 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)

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

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

<sup>4</sup> Centre for Strategic and International Studies, (2020). Global Cyber Strategies Index. Washington USA: *Author*. (online) <https://www.csis.org/programs/strategic-technologies-program/cybersecurity-and-governance/global-cyber-strategies-index> (accessed 27 Dec 20)

<sup>5</sup> National Centre for Cyber Security (NCCS), Pakistan: *Author*. <https://www.nccs.pk/> (accessed Dec 2020)

<sup>6</sup> National Cyber Training Programme (NCTP), <https://www.nctp.pk/> (accessed Jul and Dec 20)

<sup>7</sup> National Centre for Cyber Security (NCCS), (2020). <https://www.nccs.pk/> (accessed Dec 2020)

<sup>8</sup> National Centre for Cyber Security (NCCS) (2020). What we do?. *Author* (online) <https://www.nccs.pk/> (accessed Dec 2020)

<sup>9</sup> National Cyber Training Program (NCTP) (2020) (online) <https://www.nccs.pk/> (accessed Jul and Dec 20)

<sup>10</sup> Government of Pakistan (2016). The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) <http://www.lawsopakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>11</sup> Government of Pakistan (2016). The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) Ch III, Para 29(1) p 12. <http://www.lawsopakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>12</sup> Government of Pakistan (2016). The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) Ch IV, Para 42 p 19. <http://www.lawsopakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>13</sup> Government of Pakistan (2016).

The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) Ch VI Para 48-49 pp24-25 <http://www.lawsopakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>14</sup> Government of Pakistan, (2018).

The Prevention of Electronic Crimes Investigation Rules of 2018, Pakistan: *Federal Investigation Agency (FIA)* (online) <http://fia.gov.pk/en/law/PECARULES.pdf> (accessed Jul and Dec 20)

<sup>15</sup> Pakistan Telecommunications Authority (PTA), (2019). Annual Report 2018-2019. Pakistan. *Author*. Ch4 p 32. <https://pta.gov.pk/en/data-&-research/publications/annual-reports> (accessed Dec 20)

<sup>16</sup> Ministry of Interior, Government of Pakistan (2020). Personal Data Protection Bill 2020, Consultation Draft: V2. 09.04.2020. Pakistan: *Author*. Ch VI Para 32 p21. [http://www.moit.gov.pk/Sitelmage/Misc/files/Personal%20Data%20Protection%20Bill%202020\(3\).pdf](http://www.moit.gov.pk/Sitelmage/Misc/files/Personal%20Data%20Protection%20Bill%202020(3).pdf)

<sup>17</sup> State Bank of Pakistan (2004). Guidelines on Information Technology Security. Pakistan: *Author*. [https://www.sbp.org.pk/bsd/2004/Guidelines\\_on\\_IT\\_Security.pdf](https://www.sbp.org.pk/bsd/2004/Guidelines_on_IT_Security.pdf) (accessed Dec 20)

# Appendix F

## Endnotes (continued)

<sup>18</sup> State Bank of Pakistan (2016). Prevention Against Cyber Attack. Pakistan: *Author*, BPRD Circular No. 07 of 2016. (online) <https://www.sbp.org.pk/bprd/2016/C7.html> (accessed Dec 20)

<sup>19</sup> State Bank of Pakistan, (2017). Enterprise Technology Governance & Risk Management Framework for Financial Institutions. Pakistan: *Author*, BPRD Circular no 5 of 2017. <https://www.sbp.org.pk/bprd/2017/C5.htm> (accessed Dec 20)

<sup>20</sup> State Bank of Pakistan. (2018). Security of Digital Payments. Pakistan: *Author*, PSD Circular no 9 of 2019. <https://www.sbp.org.pk/psd/2018/C9.htm> (accessed Dec 20)

<sup>21</sup> State Bank of Pakistan (2020). Measures to Enhance Cyber Resilience amid Covid-19 Threat. Pakistan: *Author*, PSD - Circular no 3 of 2020. <https://www.sbp.org.pk/psd/2020/C3.htm> (accessed Dec 20)

<sup>22</sup> National Institute of Standards and Technology (NIST) (2020). USA. <https://www.iso.org/standards.html> (accessed Dec 20)

<sup>23</sup> ISACA (2020). USA. [www.isaca.org](http://www.isaca.org) (accessed Dec 20)

<sup>24</sup> ISO 27000 Series – Information Technology, Security Techniques, Information Security Management Systems, Requirements. Switzerland: *ISO*. <https://www.iso.org/standard/54534.html> (accessed Dec 20)

<sup>25</sup> The Securities and Exchange Commission of Pakistan (2020). Guidelines on Cybersecurity Framework for the Insurance Sector 2020. Pakistan: *Author* (online). P1-6. <https://www.secp.gov.pk/document/sec-guidelines-on-cybersecurity-framework-for-the-insurance-sector-2020/?wpdmdl=38763&refresh=5febaea1501331609281185> (accessed Dec 20)

<sup>26</sup> Government of Pakistan (2016). The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) <http://www.lawsofpakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>27</sup> Federal Investigation Agency, Ministry of Interior, Government of Pakistan. <http://fia.gov.pk/en/index.php>

<sup>28</sup> Government of Pakistan, (2018). The Prevention of Electronic Crimes Investigation Rules of 2018, Pakistan: *Federal Investigation Agency (FIA)* (online), Para 3 and 18 <http://fia.gov.pk/en/law/PECARULES.pdf> (accessed Jul and Dec 20)

<sup>29</sup> Federal Investigation Agency, National Responses Centre for Cyber Crime, Pakistan: *Author*. <http://www.nr3c.gov.pk/cscouts.html> (accessed July and Oct 2020)

<sup>30</sup> PakCERT, <https://www.pakcert.org/aboutus.html> (accessed July and Nov 2020)

<sup>31</sup> Onsite, <https://www.onsite.co.pk> (accessed July and Nov 2020)

<sup>32</sup> Forum of Incident Response Teams (FIRST), 2015-2020, <https://www.first.org/about/mission> (accessed 26 Oct 2020)

<sup>33</sup> PCERT, Member Teams, <https://www.apcert.org/about/structure/members.html> (accessed Dec 20)

<sup>34</sup> Pakistan International Security Authority (PISA) <http://www.pisa.org.pk/> (accessed July and Dec 20)

<sup>35</sup> Organisation of the Islamic Cooperation CERT (OIC-CERT) <https://www.oic-cert.org/en> (accessed Dec 20)

<sup>36</sup> Government of Pakistan (2016). The Prevention of Electronic Crimes Act (2016), Pakistan: *Laws Of Pakistan* (online) pp-24-25. <http://www.lawsofpakistan.com/wp-content/uploads/2016/07/the-prevention-of-electronic-crime-act-2016.pdf>

<sup>37</sup> Syed Rubab, Khaver Ahmed Awais, Yasin Muhammad, (2019). Cyber Security: Where Does Pakistan Stand?. Pakistan: *Sustainable Development Policy Institute (SDPI)*. (online) pp9-10 <https://think-asia.org/bitstream/handle/11540/9714/Cyber-security-where-does-pakistan-stand%28W-167%29.pdf?sequence=1>

# Appendix F

## Endnotes (continued)

38. Pakistan Telecommunications Authority (PTA), (2019). Annual Report 2018-2019. Pakistan. *Author*. Ch4 p 32.  
<https://pta.gov.pk/en/data-&-research/publications/annual-reports> (accessed Dec 20)

39. PakCERT,  
<https://www.pakcert.org/aboutus.html>  
(accessed July and Nov 2020)

40. Onsite,  
<https://www.onsite.co.pk>  
(accessed July and Nov 2020)

41. APCERT, (2020) Press Release 11 Mar 2020, Cyber Drill 2020, Bankers Doubles Down on Miner. *Author*, (online)  
[https://www.apcert.org/documents/pdf/APCERT\\_Drill2020\\_Press%20Release.pdf](https://www.apcert.org/documents/pdf/APCERT_Drill2020_Press%20Release.pdf) (accessed Dec 20)

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

43. CREST, (2020) Accredited Companies Providing Vulnerability Assessment Services.  
UK: *Author* (online)  
[https://service-selection-platform.crest-approved.org/accredited\\_companies/vulnerability\\_assessment/](https://service-selection-platform.crest-approved.org/accredited_companies/vulnerability_assessment/)  
(accessed Nov 2020)

44. National Cyber Security Centre (NCSC), (2017). Penetration Testing.  
UK: *Author*. (online)  
<https://www.ncsc.gov.uk/guidance/penetration-testing> (accessed Nov 2020)

45. CREST, (2020). Accredited Companies providing Security Operations Centres (SOC).  
UK: *Author*. (online)  
[https://service-selection-platform.crest-approved.org/accredited\\_companies/soc/](https://service-selection-platform.crest-approved.org/accredited_companies/soc/) (accessed Nov 2020)

46. 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)

47. PakCERT,  
<https://www.pakcert.org/aboutus.html>  
(accessed July and Nov 2020)

48. The National Response Centre for Cyber Crime (NRC3)  
<http://www.nr3c.gov.pk/> (accessed Jul and Dec 20)

49. National Centre for Cyber Security (NCCS) (2020). What we do?. *Author* (online)  
<https://www.nccs.pk/> (accessed Dec 2020)

50. National Response Centre for Cyber Crime (NRC3)  
<http://www.nr3c.gov.pk/> (accessed Jul and Dec 20)

51. National Response Centre for Cyber Crime, 'Cyber Scouts', *Author*,  
<http://www.nr3c.gov.pk/cscouts.html>  
(accessed July and Dec 20)

52. National Cyber Training Programme (NCTP), (2020) (online) <https://www.nctp.pk/>  
(accessed Jul and Dec 20)

53. National Cyber Training Program (NCTP) (2020) (online)  
<https://www.nctp.pk/> (accessed Jul and Dec 20)

54. Pakistan International Security Authority (PISA)  
<http://www.pisa.org.pk/> (accessed July and Dec 20)

55. Global Information Security Society for Professionals of Pakistan (GISPP), Pakistan, *Author*,  
<https://www.gispp.org/> (accessed Dec 20)

56. State Bank of Pakistan, SBP Regulated Institutes,  
[http://www.sbp.org.pk/f\\_links/f-links.asp](http://www.sbp.org.pk/f_links/f-links.asp)  
(accessed 14 May 2020)

57. Pakistan Banks' Association,  
<http://pakistanbanks.org/> (accessed 14 May 2020)

58. Wikipedia, List of Banks in Pakistan,  
[https://en.wikipedia.org/wiki/List\\_of\\_banks\\_in\\_Pakistan](https://en.wikipedia.org/wiki/List_of_banks_in_Pakistan) (accessed 14 May 2020)

59. 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)

60. Further information on CVSS available on Wikipedia,  
[https://en.wikipedia.org/wiki/Common\\_Vulnerability\\_Scoring\\_System](https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System) (accessed on 29 Oct 2020)

61. Data Guidance News,  
<https://www.dataguidance.com/news/pakistan-moitt-finalises-personal-data-protection-bill>  
(accessed 2 Dec 20)

# Appendix F

## Endnotes (continued)

62. Valimail report on DMARC, 2019,  
<https://www.valimail.com/resources/domain-spoofing-declines-as-protective-measures-grow/>  
(accessed 30 Oct 2020)
63. Finance Digest Report, 2019,  
<https://www.financedigest.com/rise-sophisticated-bec-scams-finance-industry> (accessed 30 Oct 2020)
64. FBI Internet Crime Report, 2019,  
<https://www.ic3.gov/Media/Y2019/PSA190910>  
(accessed 31 Oct 2020)
65. CREST International,  
<https://www.crest-approved.org/> (accessed Aug 20)
66. EC Council,  
<https://www.eccouncil.org/> (accessed Aug 20)
67. ISACA,  
<https://www.isaca.org/> (accessed Aug 20)
68. (ISC)2,  
<https://www.isc2.org/> (accessed Aug 20)
69. SANS,  
<https://www.sans.org/> (accessed Aug 20)
70. CompTIA,  
<https://www.comptia.org/> (accessed Aug 20)
71. Offensive Security,  
<https://www.offensive-security.com/>  
(accessed Aug 20)
72. Cloud Security Alliance,  
<https://cloudsecurityalliance.org/education/>  
(accessed Aug 20)
73. PCI,  
[https://www.pcisecuritystandards.org/program\\_training\\_and\\_qualification/](https://www.pcisecuritystandards.org/program_training_and_qualification/) (accessed Aug 20)
74. Cisco,  
<https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html>  
(accessed Aug 20)
75. Microsoft,  
<https://www.microsoft.com/en-us/learning/browse-all-certifications.aspx> (accessed Aug 20)
76. Amazon Web Services,  
[https://aws.amazon.com/training/path-security/?nc2=sb\\_lp\\_se](https://aws.amazon.com/training/path-security/?nc2=sb_lp_se) (accessed Aug 20)
77. IRCA(ISMS),  
<https://www.quality.org/> (accessed Aug 20)
78. BCS,  
<https://www.bcs.org/get-qualified/certifications-for-professionals/information-security-and-ccp-scheme-certifications/> (accessed Aug 20)
79. IET,  
<https://www.theiet.org/career/professional-registration/ict-technician/> (accessed Aug 20)
80. Ziring, Lawrence,(2020). Pakistan – Land. Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
81. Ziring, Lawrence,(2020) Pakistan – Relief and Drainage, Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
82. World Population Review,  
Pakistan Population 2020, *Author*  
<https://worldpopulationreview.com/world-cities/karachi-population> (accessed Nov 20)
83. Ziring, Lawrence,(2020)  
Pakistan – Resources and Power. Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
84. World Population Review,(2020)  
Pakistan Population 2020, *Author*  
<https://worldpopulationreview.com/world-cities/karachi-population> (accessed Nov 20)
85. World Population Review,(2020).  
Pakistan Population 2020, *Author*  
<https://worldpopulationreview.com/world-cities/karachi-population> (accessed Nov 20)
86. Ziring, Lawrence, (2020)  
Pakistan – Demographic Trends. Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
87. Ziring, Lawrence,(2020)  
Pakistan – Introduction and Quick Facts. Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)



# Appendix F

## Endnotes (continued)

- <sup>88</sup>. Ziring, Lawrence, (2020).  
Pakistan – Education.  
Chicago USA: *Britannica*.  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
- <sup>89</sup>. Ziring, Lawrence, (2020).  
Pakistan – Introduction and Quick Facts.  
Chicago USA: *Britannica*  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
- <sup>90</sup>. Ziring, Lawrence, (2020).  
Pakistan – People Linguistic Composition.  
Chicago USA: *Britannica* (online)  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
- <sup>91</sup>. Ziring, Lawrence, (2020).  
Pakistan – Economy.  
Chicago USA: *Britannica* (online)  
<https://www.britannica.com/place/Pakistan>  
(accessed Nov 2020)
- <sup>92</sup>. Macrotrends, (2020).  
Pakistan GNI 1962-2020. *Author* (online)  
<https://www.macrotrends.net/countries/PAK/pakistan/gni-gross-national-income>  
(accessed 30 Dec 20)
- <sup>93</sup>. Macrotrends, (2020).  
Pakistan GDP Growth Rate 1961-2020. *Author* (online)  
<https://www.macrotrends.net/countries/PAK/pakistan/gdp-growth-rate>  
(accessed 30 Dec 20)
- <sup>94</sup>. World Bank, (2020).  
Pakistan Overview, *Author*. (online)  
<https://www.worldbank.org/en/country/pakistan/overview> (Accessed Nov 2020)
- <sup>95</sup>. Khali, Basma (22 Mar 2020)  
Cybercrime effecting banking sector / economy of Pakistan. *Modern Diplomacy* (online)  
<https://moderndiplomacy.eu/2020/03/22/cybercrime-effecting-banking-sector-economy-of-pakistan/>  
(accessed 30 Dec 20)
- <sup>96</sup>. Baloch Shah Meer, Musyani Zafar, (8 July 2020).  
Pakistan's Great Digital Divide.  
USA: *The Diplomat* (online)  
[https://thediplomat.com/2020/07/pakistans-great-digital-divide/#:~:text=Internet%20access%20in%20Pakistan%20stands,\(3%2F4G\)%20connections.&text=Around%2065%20percent%20of%20people%20in%20Pakistan%20live%20in%20rural%20areas.](https://thediplomat.com/2020/07/pakistans-great-digital-divide/#:~:text=Internet%20access%20in%20Pakistan%20stands,(3%2F4G)%20connections.&text=Around%2065%20percent%20of%20people%20in%20Pakistan%20live%20in%20rural%20areas.) (accessed Dec 20)
- <sup>97</sup>. The Inclusive Internet 2020, Pakistan,  
<https://theinclusiveinternet.eiu.com/explore/countries/PK/> (accessed Dec 20)
- <sup>98</sup>. Pakistan Today (2018).  
FIA says record number of cybercrimes reported in 2018.  
*Author*  
<https://www.pakistantoday.com.pk/2018/10/23/fia-says-record-number-of-cyber-crimes-reported-in-2018/amp/> (accessed Jul and Dec 20)
- <sup>99</sup>. Shabbir Ambreen, (2018).  
Pakistan Rated 7th Worst is Cyber Security.  
*ProPakistani* (online),  
<https://propakistani.pk/2019/02/14/pakistan-ranked-7th-worst-in-cyber-security-report/>  
(accessed 27 Dec 20)
- <sup>100</sup>. Bischoff Mark (3 Mar 2020)  
Which Countries have the worst (and best) Cyber Security? UK: *Comparitech*.  
<https://www.comparitech.com/blog/vpn-privacy/cybersecurity-by-country/> (accessed 27 Dec 20)
- <sup>101</sup>. Qadeer Muhammad Abdul (2020).  
The Cyber Threat Facing Pakistan.  
Washington, USA: *The Diplomat*.  
<https://thediplomat.com/2020/06/the-cyber-threat-facing-pakistan/> (accessed Dec 20)
- <sup>102</sup>. Ahmed, Qazi Mohammad Misbahuddin, (2018).  
Analysis of the Recent Attack on Pakistan Banks.  
*PakCERT Threat Intelligence Report* PCTI-2018-0111  
(online)  
<https://www.pakcert.org/img/PakCERT%20Threat%20Intelligence%20Report%20-%20web.pdf>  
(accessed 30 Dec 20)
- <sup>103</sup>. Goud, Naveen (2018).  
Almost all Banks in Pakistan became victims to Cyber Attack. *Cybersecurity Insiders* (online)  
<https://www.cybersecurity-insiders.com/almost-all-banks-in-pakistan-become-victim-to-cyber-attack/>  
(accessed May and Dec 20)

# Appendix F

## Endnotes (continued)

<sup>104</sup>. Hope Alice, (15 May 20).

Information of Over 115 Million Pakistani Mobile Subscribers Exposed in a Massive Data Leak. *CPO Magazine* (online)

<https://www.cpomagazine.com/cyber-security/information-of-over-115-million-pakistani-mobile-subscribers-exposed-in-a-massive-data-leak/> (accessed May and Dec 20)

<sup>105</sup>. The Express Tribune, Cybercrime Registers Sharp Decline Amid Covid-19 Lockdown, 03 May 20, *Author* <https://tribune.com.pk/story/2213373/1-cybercrime-registers-sharp-decline-amid-covid-19-lockdown?amp=1> (accessed July and Dec 20)

<sup>106</sup>. Global Cybersecurity Index 2018, International Telecoms Union (ITU), Switzerland, 2019, p58-59,p65, [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf) (accessed Dec 20)

<sup>107</sup>. Global Cybersecurity Index 2018, International Telecoms Union (ITU), Switzerland, 2019, pp13-14, [https://www.itu.int/dms\\_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf](https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf) (accessed Dec 20)

<sup>108</sup>. National Cyber Security Index, (23 Mar 2020). Pakistan. *Estonia: e-Governance Academy Foundation*, <https://ncsi.ega.ee/country/pk/> (Accessed Nov 2020)

<sup>109</sup>. The Inclusive Internet 2020, Pakistan, <https://theinclusiveinternet.eiu.com/explore/countries/PK/> accessed Dec 20

<sup>110</sup>. Global Cyber Security Capacity Centre, Oxford: *Author*, <https://gcsc.web.ox.ac.uk/cmm-reviews> (accessed Nov 20)