CMAGE

Cyber Security Maturity Assessment Global Ecosystem

Nigeria 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 (CMAGE).

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

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 Nigeria's cyber security ecosystem.

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

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

While it will never be complete, it has been externally validated. The relational database containing the CMAGE model has helped facilitate consistent application of the assessment and allows for ease of update and maintenance of the data, the ability to interrogate the data and to extend the model to include other factors.

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

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

Unashamedly, the endpoint – at least from a CREST perspective - is that every financial services institution in Nigeria 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 Nigeria 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 that we are all now undertaking.

Ian Glover
President
CREST International

Highlights Report

Background

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

Maturity Model Assessment Summary

Overall Nigeria Ecosystem

Maturity Level 2

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

Nigeria 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 Maturity Level 3 by adopting international good practice and utilising IPR-free guidance (being created by CREST International as part of the project's second stage).

Highlights Report

Summary of Observations

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

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

Dimensions and Indicators

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

Qualitative Assessments — **1-4**

Qualitative Assessments — **5**

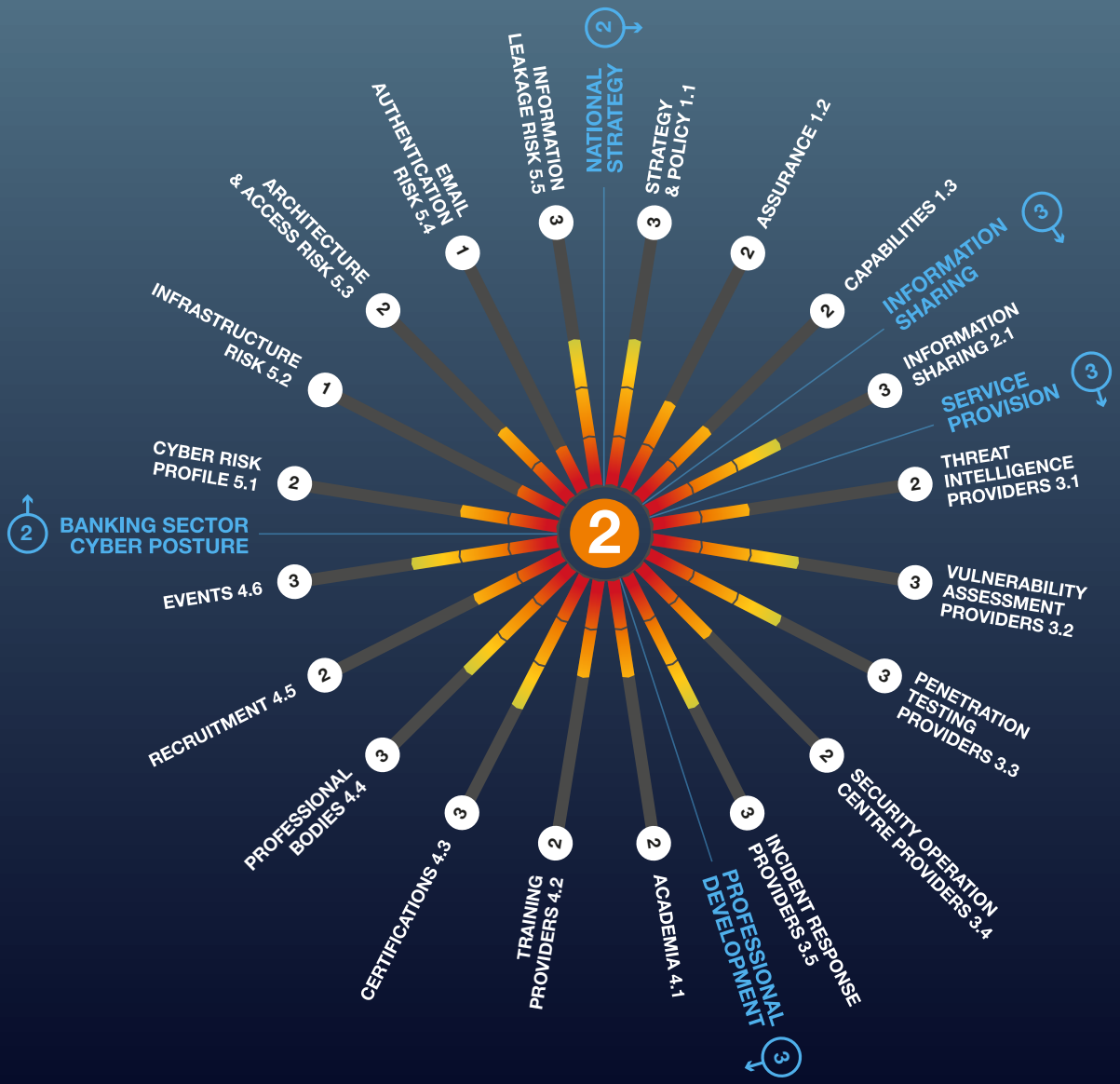
Maturity Scores

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

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

Highlights Report

Summary of Observations (continued)



Maturity Levels

1 Emerging
2 Transitional
3 Organised
4 Dynamic
5 Leading

Summary Assessment

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

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

From a strategy and policy perspective, Nigeria is assessed as being in a strong position. The National Cyber Security Strategy was published in 2014.

Subsequent actions taken by the Nigerian government are highly commendable.

The recent publication of **Cyber Security Guidelines by the Central Bank of Nigeria (CBN)** is certainly a step in the right direction. Turning the CBN guidelines into a fully functioning cyber security assurance scheme should be a priority.

There is anecdotal evidence that the Nigeria Police Force has a specialist unit to tackle cybercrime, but few details of the unit could be found. There also appears to be no quick and obvious route to reporting cybercrimes.

Detailed research has not identified evidence of any serious investment in the investigation or prevention of cybercrimes, nor the use of an intervention programme to divert young people with talent away from involvement in cybercrime. **Good practice from other countries could undoubtedly help to speed the development and effectiveness of the cybercrime unit.**

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 2

Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

CERTs & Information Sharing

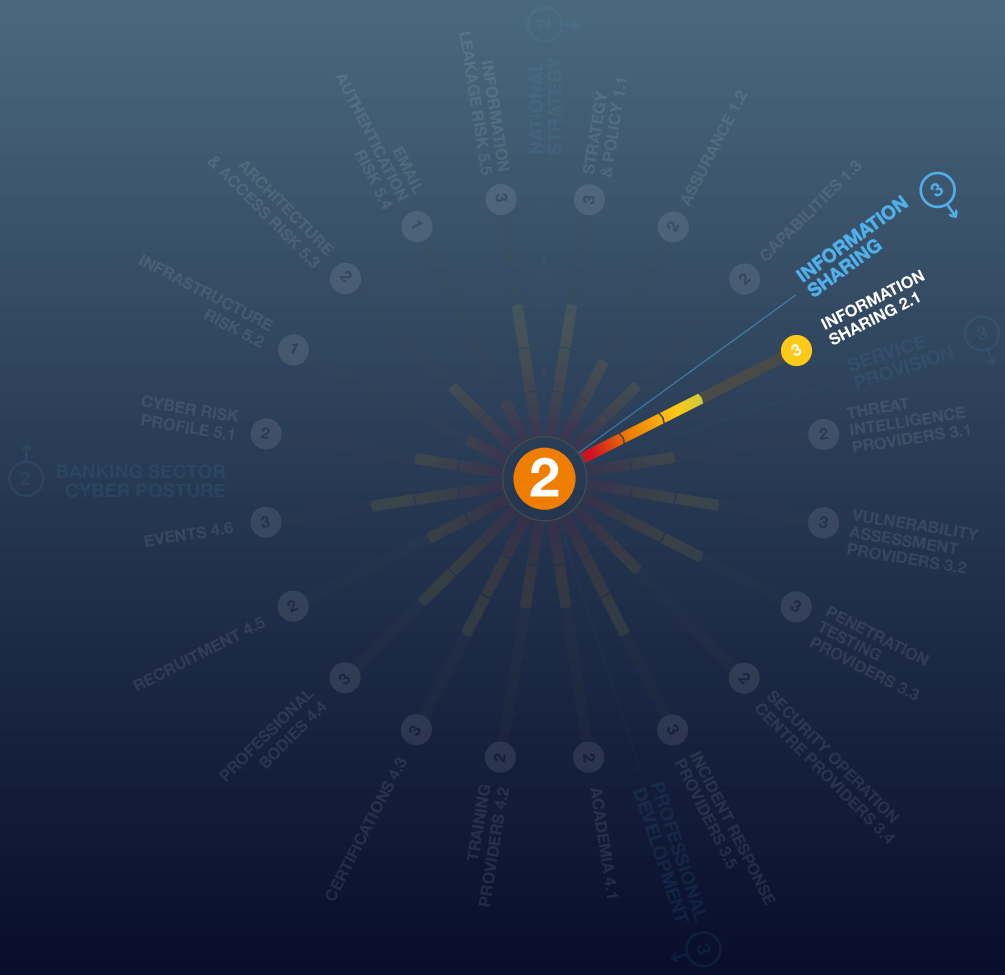
Nigeria has two Computer Emergency Response Teams, **ngCERT and CERRTng. Both have regional links through membership of AfricaCERT.** ngCERT has international links and is a member of the global CERTforum, FIRST.

CERRTng is part of the National IT Development Agency and the de facto government CERT. It is not a member of FIRST and appears to be structured more on the lines of an information exchange. There appears to be a lack of focus on information sharing in other critical sectors, such as financial services.

Dimension 2

Cyber Security Information Sharing

Maturity Level 3



Highlights Report

Key Observations - Dimension 3 - Cyber Security Service Provision

- Four CREST International member companies offer one or more cyber security services from in-country offices.
- Fourteen local companies were identified as offering such services, but their quality could not be assessed.
- Several CREST and non-CREST companies offer cyber security services to clients in Nigeria from regional offices in nearby countries.

Overall, a good mix of local, regional and international providers of cyber security services exist across most of the five disciplines examined. However, the provision of threat intelligence and security operation centre services were slightly weaker. With some stimulus and focussed investment, Nigeria 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

More than a dozen universities were identified as offering undergraduate and/or postgraduate studies in cyber security, with many more offering computer science and related degrees.

A first-class cyber security industry needs to be underpinned by a first-class array of cyber security education opportunities.

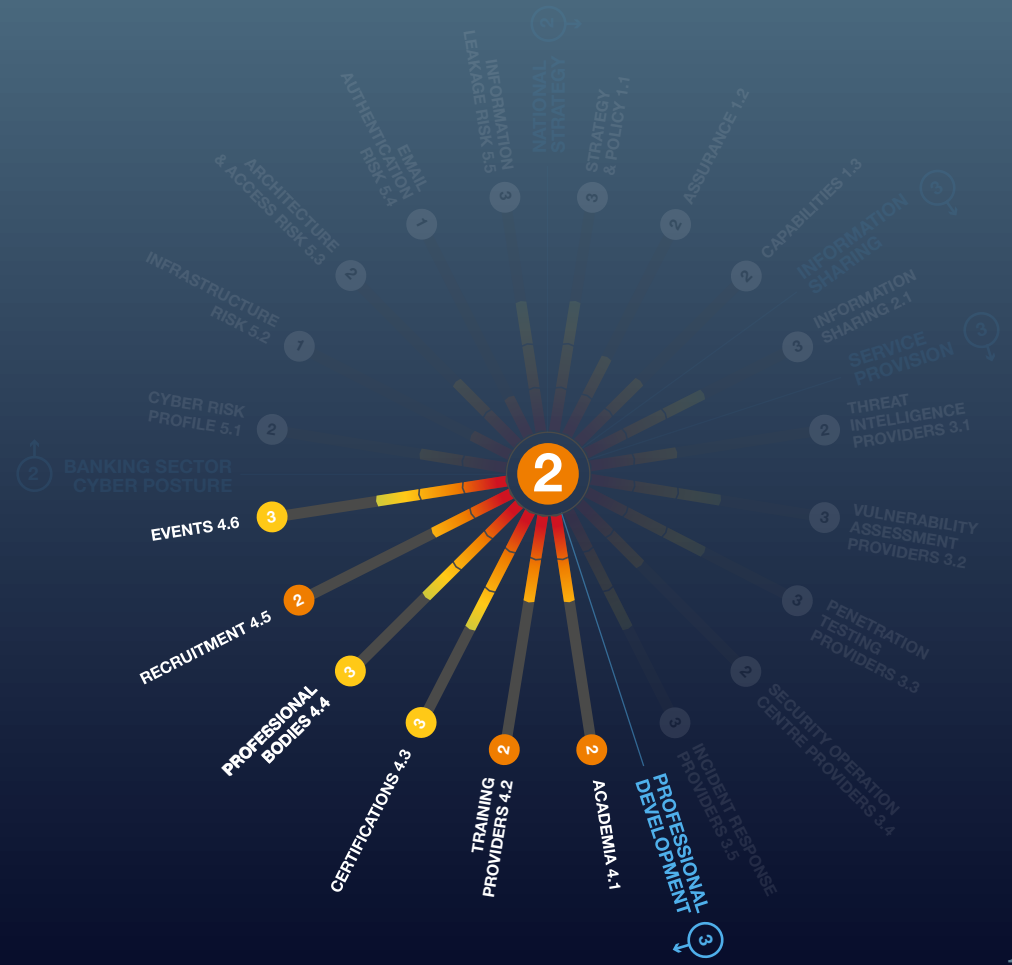
By utilising international good practice, Nigeria could build upon the current range of computer science degrees to support creating more specific cyber security courses and qualifications and become a regional beacon of excellence.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 3



Highlights Report

Key Observations - Dimension 4 (continued)

Thirty-five local and international training providers were identified offering cyber security training courses.

Some presented a small selection within a broad portfolio of other courses, but a significant number of providers were heavily focused on cyber security.

Diverse training opportunities should raise standards, as well as making the training more affordable, helping further develop the professional cyber security community.

Examinations for many international professional certifications are readily accessible in Nigeria.

From CREST's research, there appears to be a growing importance attached to using certifications to encourage the most talented people into the industry and retaining them.

The costs of some of these professional certificates may be prohibitive to many.

It is likely that once individuals and companies see the benefits of professional certifications, cost issues could be overcome.

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

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

There is evidence of international bodies operating in Nigeria. There are two local organisations, Cyber Security Experts Association Nigeria (CSEAN) and Information Security Society of Africa - Nigeria (ISSAN).

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

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

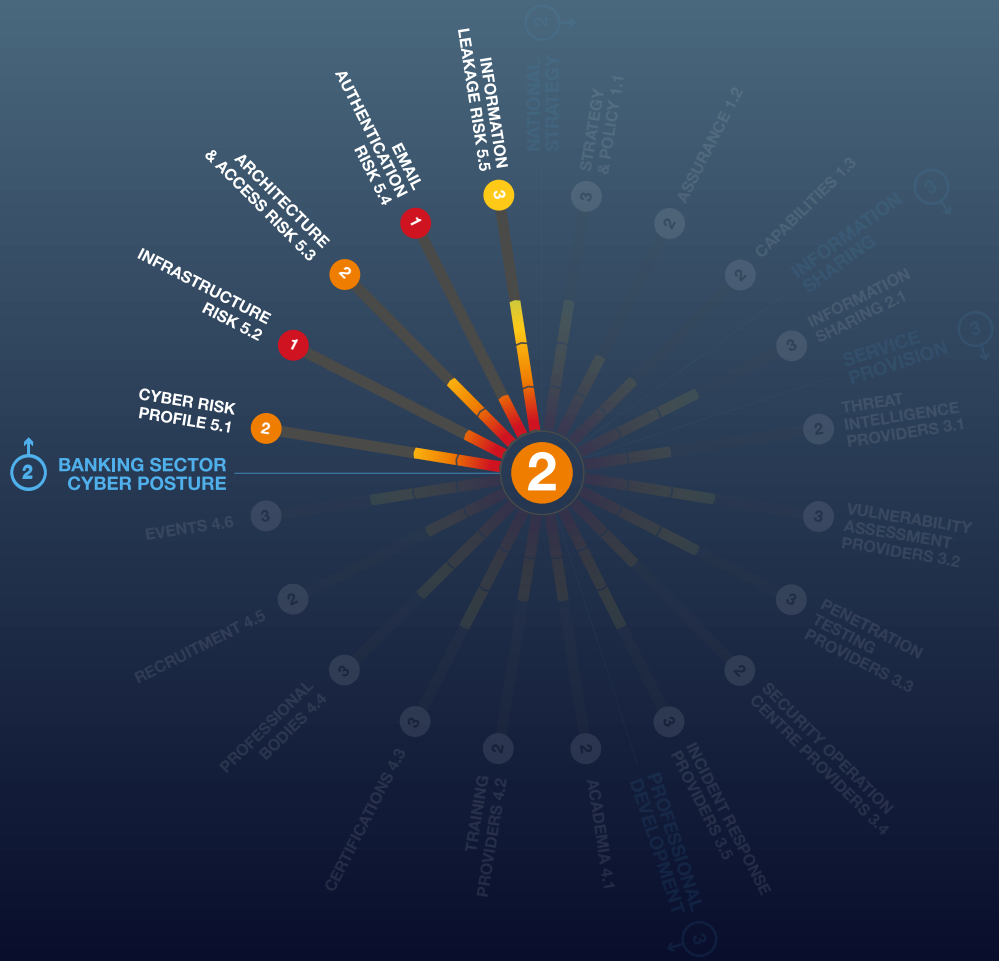
Directly assessing many of the key risk areas listed above is not possible. However, indirect passive (non-intrusive) assessment can be conducted on an organisation's internet-connected infrastructure.

Continued on next page...

Dimension 5

Banking Sector Cyber Security Posture

Maturity Level 2



Highlights Report

Key Observation - Dimension 5 (continued)

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

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

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

Passive external assessments were carried out on the public-facing IT infrastructure of a sample of 50 financial institutions. For obvious reasons, all results were anonymised.

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

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

42% Overall, **42%** were awarded a risk rating of 'Very High' or 'High', indicating Maturity Level 2 for Risk Profile.

14% Just **14%** of the sample had evidence of critical vulnerabilities within their infrastructure.

42% A further **42%** appeared to be carrying non-critical vulnerabilities. This indicates Maturity Level 1 for Infrastructure Vulnerability Risk.

16% In respect of Architecture and Access Risk, **16%** of the sample appeared to have one or more remote access ports open on the public-facing infrastructure.

28% Some **28%** appeared to have one or more database ports open, leading to the award of Maturity Level 2 for this risk category.

28% Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **28%** of the sample.

66% Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **66%** of the sample. Our research indicates Maturity Level 1 for Email Authentication Risk.

50% In **50%** of sampled institutions, at least some staff data was available online because of third-party data breaches, indicating Maturity Level 3 for Information Leakage Risk.

There is significant room for improvement in the cyber security posture of many of Nigeria'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 Nigeria'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 Nigeria**, to help create development pathways.

Highlights Report

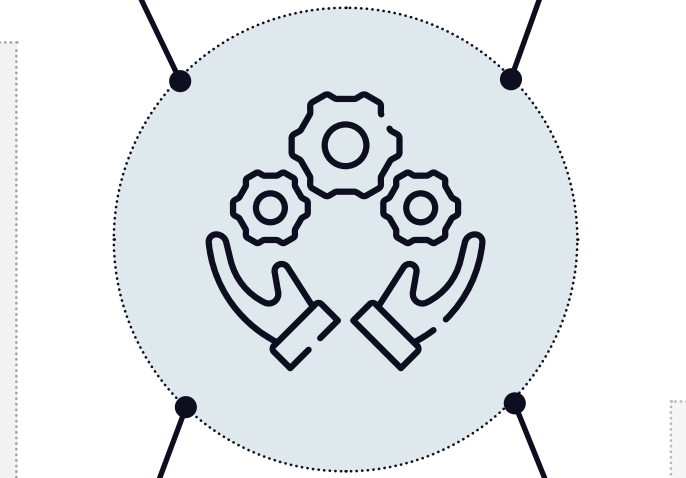
2021 Good Practices Guides and Tools

Goverment Strategy Policy

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

Service Suppliers

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



Training and Academia

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

Security Postures

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

Introduction

Introduction

Background

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

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

CREST International

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

Introduction

Research Methodology

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

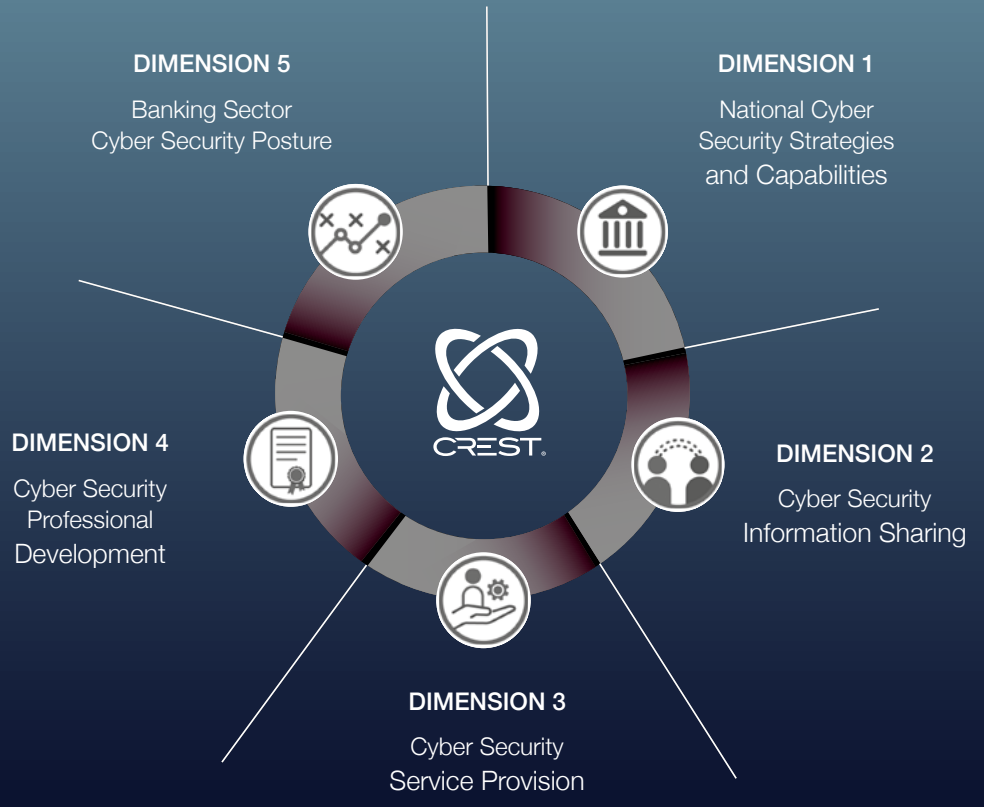
9. In respect of the banking sector cyber security posture, CREST worked with **Orpheus Cyber**[3], a leading Cyber Threat Intelligence service provider, to carry out a passive (non-intrusive) external assessment of the public-facing IT infrastructure from a sample of the country's financial institutions. The assessments were carried out by computer, to common standards, allowing for comparisons, benchmarking and periodic automated reassessments, if required. CREST believes this methodology is a global first - the first time rapid, automated mass assessment has been used as part of cyber security maturity modelling.

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

CMAGE Structure

11. 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

12. 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.
13. 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.
14. **In all cases, a generic label has been assigned to each of the five levels of the maturity model, as follows:**

15. 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.**

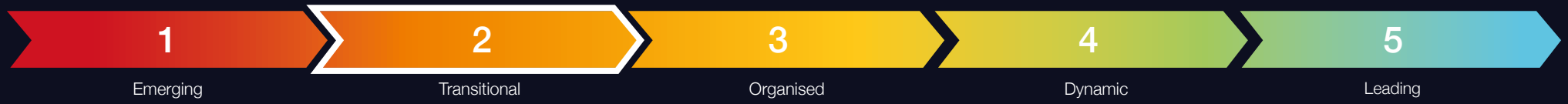
DIMENSION		INDICATOR	
QUALITATIVE ASSESSMENT			
1	**National Cyber Security Strategy & Capabilities**	1.1	Government Strategy & Policy
		1.2	Regulator/Government Operated Assurance Schemes
		1.3	Law Enforcement & Cyber Defence Capabilities
2	**Cyber Security Information Sharing**	2.1	Computer Emergency 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.

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

    It would also be difficult to justify and target research. 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 undermines 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.

17. 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 goverment departments and agencies to act, and if the strategy has been implemented and updated.

18. **The Office of the National Security Adviser (NSA)** is the authority that sits over the Directorate of Cybersecurity for the Nigerian government[4]. The Directorate of Cybersecurity was created in 2006, as the apex body for cybersecurity, to sustain the good work of Nigerian Cybersecurity Working Group. It is mandated to implement the National Cybersecurity Initiative (NCI) objectives[5]. **No specific websites for the Office of the National Security Advisor or The Directorate of Cybersecurity were found during research.**

19. The **Nigerian National Cybersecurity Initiative (NCI)** was established in 2003 as a corrective measure to Nigeria's cybercrime situation, with six objectives:

    (1). Enlighten Nigerians on the nature and danger cybercrime

    (2). Criminalise all online vices through new legislation

    (3). Build institutional capacity across law enforcement agencies, extending statutory functions on cybercrime related issues

    (4). Establish legal and technical frameworks to secure computer systems and networks, protecting the country's critical information infrastructure

    (5). Create a platform for public-private stakeholder collaboration to set cybersecurity guidelines and standards, and

    (6). Build international law enforcement cooperation and collaboration with other agencies worldwide to enable Nigeria to tackle cybercrime[6].

National Cyber Security Strategy & Capabilities

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

Overall Assessment

20. From a strategy and policy perspective, Nigeria is assessed as being a strong level 3. The recent publication of Cyber Security Framework and Guidelines (2018)[7] by the Central Bank is a step in the right direction towards developing a banking sector assurance regime. However, sustained efforts to tackle cybercrime are not as visible as they could be.

Development approach

21. A focus on visible improvements to law enforcement and cyber defence capabilities should be considered a priority. Turning the CBN guidelines into a fully functioning cyber security assurance scheme should be another priority.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy

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

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

22. The research sought to identify 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.

23. **The National Cybersecurity Strategy was issued by the Office of the National Security Advisor in 2014**[8]. The strategy recommended establishing a National Cybersecurity Coordinating Centre (NCCC), a National Advisory Council on Cybersecurity (NACC) and the Nigerian Computer Emergency Response Team (ngCERT). It also designated the IT and financial services sectors as National Critical Information Infrastructure (NCII)[9].

24. In a 2019 review of the Nigerian National Cybersecurity Strategy[10], it noted the following areas still need to be addressed:

    (1). A national incident management strategy to help generate a central repository of cybersecurity incidents, track them, and learn lessons from how they were resolved

    (2). Continuous monitoring and review of implementation and management of the National Cybersecurity Program, to provide assurance it can safeguard critical national infrastructure

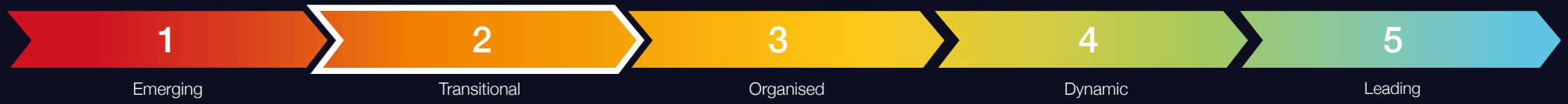
    (3). A national readiness strategy which empowers development of comprehensive, coherent, structural, and procedural capabilities at strategic and tactical levels to mitigate cyber risks[11]

25. The **Nigerian Government's National Information Technology Development Agency (NITDA)**[12] was established to implement the Nigerian Information Technology Policy and co-ordinate general IT development in the country. Its role is to develop, regulate and advise on information technology through regulatory standards, guidelines, and policies. It is the prime agency for e-government implementation, internet governance and general IT development in Nigeria. NITDA has a Cyber Security department[13], and is the authority over the Computer Emergency Readiness and Response Team (CERRTng)[14].

26. The Cybercrime (Prohibition, Prevention, Etc.) Act 2015 is the most recent cyber security legislation found during research. Section 5 criminalises all cyber-attacks on critical national infrastructure. Section 21 mandates that cybercrimes be reported to ngCERT. Failure to do so within seven days results in a fine of N2,000,000 (US$524) and denial of internet service. Section 42 covers establishment of the Nigerian Computer Emergency Response Team (ngCERT), sitting under The National Security Adviser, to act as a coordinating centre responsible for managing cyber incidents[15].

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



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

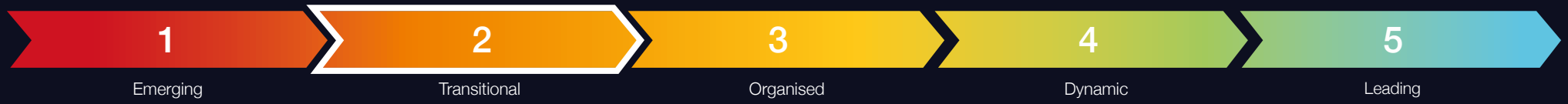
The central bank or other lead financial authority of any nation is essential in setting the ethical standards and operating frameworks for banks and financial institutions operating in the country.

27. CREST's research focused on looking for publicly available policies, regulations and laws which support and uphold financial ethics, integrity and cyber security.
28. **The Central Bank of Nigeria's (CBN) Cyber Security Framework and Guidelines**[16] came into effect on January 1, 2019 and were created because of a high incidence of cyber security breaches in the fintech industry and lack of serious action being taken by fintech companies themselves.

A 2019 article on cybersecurity regulations in the Nigerian fintech industry comments that the **CBN Cybersecurity Framework and Guidelines is a step in the right direction,** that it will increase security in the fintech industry and so increase investor confidence[17].

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.

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

30. **The Economic and Financial Crimes Commission (EFCC) was established by an Act of the same name in 2004[18].** It is the designated Financial Intelligence Unit (FIU) of Nigeria, and presides over the National Digital Forensics Laboratory[19]. The EFCC's mission is to rid Nigeria of economic and financial crimes, and to effectively coordinate domestic efforts in support of the global fight against money laundering and terrorist financing[20].

    It is responsible for advising the government on measures to prevent and combat cybercrime[21]. **In 2018 it received an investment of £500,000 from the UK government[22].** The EFCC and United States' FBI have been collaborating to combat cybercrime, with a transatlantic operation leading to the arrest of several Nigerians for cybercrimes in the USA[23].

31. According to a 2016 Symantec report (p81-82)[24] the Independent Corrupt Practices and Other Related Offences Commission (ICPC)[25] is one of the primary agencies charged with protecting against cybercrime. It, along with the Economic and Financial Crime Commission (EFCC), State Security Service (SSS) and the Nigerian Police[26] all play prominent roles in the fight against cybercrime.

32. The Nigerian Police are mentioned in a 2016 article on measures to tackle cybercrime[27] as having a cybercrime unit within the INTERPOL National Central Bureau[28]. Nothing about the cybercrime unit was found on the Nigerian Police or INTERPOL websites.

33. In 2019, Nigeria became a member of the West African Police Information System (WAPIS) programme with INTERPOL and 15 other ECOWAS (Economic Community of West African States) countries[29]. Although not strictly cybersecurity related, it is an information sharing organisation at regional and international level, so may include provision for sharing cybercrime information.

34. According to a 2016 article in Forbes magazine, **the Nigerian Army announced plans to take the war against insurgency to the nation's cyberspace with the Nigerian Army's Cyber Warfare Command.** Manned by 150 IT trained officers and men drawn from the corps and services in the Nigerian Army, the new corps aimed to protect the nation's data and network against cyber-attack and curb terrorism.

35. Their aim was to monitor, defend and assault in cyberspace through distributed denial of service (DDoS) attacks on criminals, nation states and terrorists[30]. An article in the Nigerian Military Blog (2019)[31] states the unit was set up in 2018, and is the first, and most advanced, in Africa. No specific website for this unit was found during research.

Dimension 2

Cyber Security Information Sharing

Cyber Security Information Sharing

Overall Dimension Assessment: *Maturity Level 3*

Information sharing is vital to achieving a collective understanding of cyber security risks and vulnerabilities, to counter threats posed by cybercriminals.

36. There is no commercial advantage to be gained by not sharing information. Open publication of academic research and the sector-specific information exchanges are example mechanisms for sharing information on cyber security risks, threats and vulnerabilities.

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

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

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

Overall Assessment

39. Nigeria is currently at Maturity Level 3, but there is evidence of some progress towards Level 4. **The Nigeria Computer Emergency Response Team (NgCERT)**[32] is a member of the **Forum of Incident Response and Security Teams (FIRST)**[33], which means it meets ENISA Maturity Model Tier 2 requirements[34].

    The **National IT Development Agency's (NITDA)**[35] **Computer Emergency Readiness and Response Team (CERRTng)**[36] is structured as a useful information exchange facility. Both NgCERT and CERRTng are members of AfricaCERT[37].

Development Approach

40. The establishment of a finance sector-specific information exchange mechanism would be a useful additional measure that would aid progress towards Maturity Level 4.

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs)

Assessment – *Maturity Level 3*
Evidence that National CERT has international links (FIRST etc) and is following international standards. Meets ENISA CERT Maturity Model Tier 2 requirements.

41. **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)

42. The establishment of ngCERT was covered in Part Six of the National Cybersecurity Strategy 2014[38] and created by the authority of Section 42 of the Cybercrimes Act 2015[39]. **Sitting under the National Cyber Security Centre (NCC), ngCERT acts as a coordination centre for cyber incidents,** implementing the National Incident Response Plan (NIRP) and monitoring the Cyber Emergency Monitoring System (CEMS)[40].

43. Part Six of the National Cybersecurity Strategy 2014 also covers establishment of other sector-specific CERTS, with ngCERT acting as national regulator and coordinator for the ecosystem[41].

44. The National IT Development Agency's CERRTng was established in 2014 in response to the increase in cybercrime and to fulfil the requirements of the National Cyber Security Strategy 2014[42]. CERRTng is another government-level CERT, providing networking, collaboration and a sharing platform to ensure a secure cyberspace.

CERRTng's services include a Fusion Centre which provides:

- Monitoring in support of ICT infrastructure
- Capacity building with the Nigerian public to raise awareness
- Youth empowerment programmes to help develop home-grown cyber security solutions, and
- A cyber forensic laboratory, which provides analysis to assist law enforcement agencies with investigations and evidence gathering[43].

45. In terms of other international information sharing organisations, Nigeria is a member of the Cyber Security Alliance for Mutual Progress (CAMP), an international information sharing forum which aims to improve cyber security among its 61 members[44].

Dimension 3

Cyber Security Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 3*

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

46. CREST's research into how cyber security services are currently provided in Nigeria involved:
    - Identifying cyber security service providers
    - Examining what services they were offering
    - Identifying what accreditations they held, and
    - Identifying whose accredited services and certifications they provided.
47. Company office location and customer reach were also recorded. Were they local companies, registered and based only in Nigeria? CREST examined if they were regional companies, registered in another African country, but with offices and the ability to reach customers in other countries in the region. Or were they a large international organisation, with multiple global office locations which may be located in-country? If not, do they have the ability to provide services into Nigeria without having a permanent physical presence in country or anywhere in the African region? When examined together, these factors combined give an idea of the maturity of the cyber security industry.
48. Several of the companies identified 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

49. Across the five service provision disciplines, three are at Level 3 and two are at Level 2. Four CREST International member companies offer one or more services from in-country offices and a further 14 locally based non-CREST companies also offer some cyber services. Overall, this places Nigeria at Maturity Level 3.

Development Approach

50. Government and regulators should lead the adoption of benchmarked standards. This is likely to create demand-led growth in the number of service providers and encourage investment. It should also drive local providers to raise standards by seeking CREST membership.

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers

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

Assessment – *Maturity Level 2*

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

Cyber Threat Intelligence

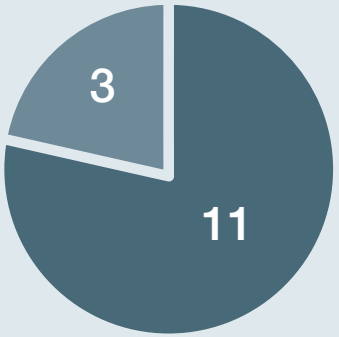
51. Cyber Threat Intelligence (CTI) is information about current and future cyber threats and actors that adversly affect a nation's or organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks[45]. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark web sources.

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

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	1	5
Regional	0	0	0
International	3	11	14
Total	**7**	**12**	**19**

53. There are five companies offering cyber threat intelligence services from offices in Nigeria. The CREST-accredited company is a global organisation with an office in Lagos. Two of the non-CREST-accredited companies, while based in Nigeria, also provide services across the African region, and another is an international organisation with an office in Nigeria.

54.



Of the **14 international companies, 11 are CREST-accredited.** All can offer their services into Nigeria, though there was no evidence found during CREST's research as to how often they do so.

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment 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.

Vulnerability Assessment (VA)

55. **Vulnerability Assessment (VA) is defined by CREST as being:** *"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*[46]*."* As with Threat Intelligence, research focused on looking for companies which provide VA services in Nigeria, ideally based in-country.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	14	3	17
Regional	0	0	0
International	0	28	28
Total	**14**	**31**	**45**

56. CREST's research found **45 companies in total that provide VA services into Nigeria.** Of the companies with offices in Nigeria, **the three CREST-accredited ones are large international firms.** Of the non-CREST accredited companies with offices in Nigeria, three are international organisations, three operate in the Africa region and one is the Nigerian Computer Emergency Response Team (ngCERT)[47].

57.

As with CTI services, **of the 28 International companies, all of which are CREST-accredited,** no evidence was found as to how often they are providing VA services to Nigeria-based clients.

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

58. **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*[48]."

59. 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 Nigeria as could be identified.

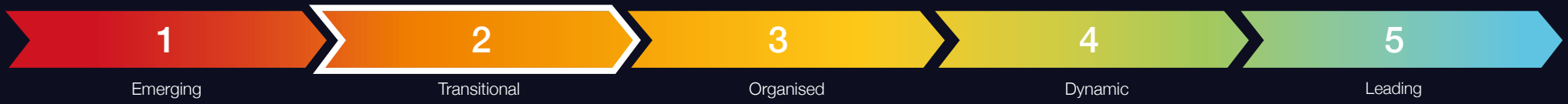
Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	11	4	15
Regional	0	0	0
International	2	79	81
Total	**13**	**83**	**96**

60. The research identified **96 companies providing Penetration Testing services into Nigeria**. Of the 15 with offices in Nigeria, **four were CREST-accredited international organisations.** Of the remaining 11, **one is ngCERT, three offered their services regionally,** and a further three were international organisations.

61. **81 International CREST-accredited organisations were identified, who could, if required, provide services into Nigeria.**

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

62. **CREST defines a Security Operations Centre as:** "*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*[49]*.*"

63. 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	3	1	4
Regional	0	0	0
International	0	9	9
Total	3	10	13

64. **13 companies were found providing SOC services into Nigeria.** Four are based in-country, one of which is a CREST-accredited international organisation. **Two are international (non-CREST) organisations with offices in Nigeria.** No regional companies were found. **Of the nine international companies found, all were international organisations who could provide their SOC services into Nigeria if requested to do so by a client.**

Cyber Security Service Provision

Indicator 3.5 Incident Response 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.

Incident Response Providers

65. **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*[50]."

66. 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 that country's cyber industry.

67. There are **41 companies providing Incident Response services into Nigeria.** Of the ten with offices in Nigeria, **the three CREST-accredited companies are large international organisations.** Of the non-CREST-accredited companies, **one is ngCERT, two operate regionally, and three are international organisations.**

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	7	3	10
Regional	0	0	0
International	0	31	31
Total	**7**	**34**	**41**

68. **There are 31 international organisations offering Incident Response services into Nigeria, all of which are CREST-accredited.**

Dimension 4

Cyber Security Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 3*

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

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

70. To determine the health of Cyber Security Professional Development there is a need to identify which higher education establishments and professional training providers offer cyber security qualifications and certifications - and what qualifications and certifications are available. CREST examined what (if any) professional membership organisations were undertaking in Nigeria 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.

71. During a literature review on the cyber security profession in Nigeria, several articles and reports provided deeper context to education and professional development in Nigeria. This can be found in **Appendix D.**

Overall Assessment

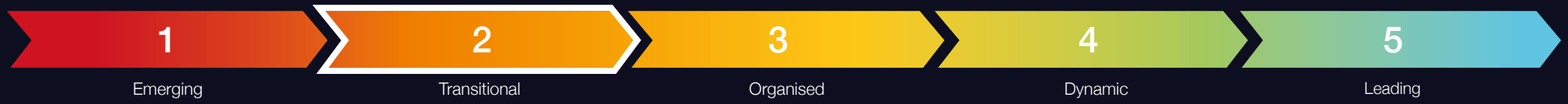
72. The individual assessment of the six distinct Professional Development indicators shows that three are at Level 3, and three at Level 2. There are already some excellent examples of good practice in Nigeria, which can be quickly built upon. Very encouragingly, Section B of the 2014 National Cybersecurity Strategy[51] focuses on the skills agenda.

Development Approach

73. Efforts should be concentrated on nurturing training providers and specialist recruitment. Partnerships between academia, professional bodies and event organisers to showcase career pathways would be of benefit. An investment in certification would also assist.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education



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

Academia and Higher Education

74. Higher education takes place after secondary schooling, usually in further education colleges or universities. It aims to equip people with the skills and qualifications needed in their future workplace 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 their students, and the level of these courses – diploma, degree, masters etc. The more students graduating with ICT- or cyber-related degrees, potentially results in more people following an ICT-related career.

76. **The Nigerian Universities Commission lists 200+ universities in Nigeria (including 44 Federal, 48 State, 99 Private, 12 distance learning centres and 15 universities with approved affiliations)**[52]**.** For this report, a sample of 25 universities was examined. An exhaustive search of the curricula of all 200 universities has not been undertaken.

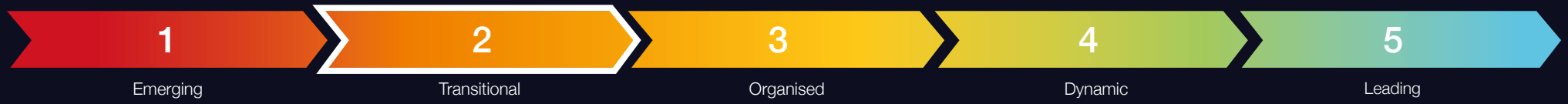
77. Of the **25 universities selected for CREST's research, universities providing ICT courses were the priority.** Not all provided equal information regarding the level and number of degrees they provide, so figures in the table below are an educated estimate. **For the universities that only listed their ICT departments an assumption was made that they will provide at least one ICT course.**

	Cert/ Dip	ICT Depts named - no course detail	BA/ BSc	Pg Dip	MSc	PhD	Total
ICT Courses	0	16	40	3	5	7	71
Cyber Cources	1	0	13	1	1	1	17
Total	**1**	**16**	**53**	**4**	**6**	**8**	**88**

78. Of the small sample of universities researched, and of the 88 courses found, **19% were cyber related courses provided by 13 of the researched universities.** It is positive to see numerous cyber security-related undergraduate degrees on offer - and these numbers will grow.

Cyber Security Professional Development

Indicator 4.2 Training Providers



Assessment – *Maturity Level 2*
Remote (online) delivery of training is supplemented with some regional instructor-led provision and a few local providers. No CREST International training provider members with local offices. Some competition but with no measure of quality of service.

Training Providers

79. Training providers are qualified to deliver training via established courses 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. A total of **35 training providers were found during research.** While some offer a few cyber courses as part of a broad range of courses, many are heavily focused on cyber security, with a good mix of online and instructor-led training, which is encouraging.

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

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

82. **During CREST's research, 15 international certification bodies were found operating in Nigeria.** Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres available in Nigeria. Some certifications requiring practical exams offer this online or through connection to a remote network, although some bodies require a physical testing site, which have limited availability in Africa. Take-up of certifications is moderate in Nigeria.

    Two organisations have active chapters (one under development), with monthly meetings, training and seminars organised, and conference events like Africa CACS 2020 hosted in Lagos. Several certification bodies organise training in Nigeria, either themselves or with accredited training partners. There was high recruitment activity noted, with numerous online job postings and advertisements. Certifications are highly desired in recruitment, typically featuring a wider range and more technical certifications across a certification body.

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

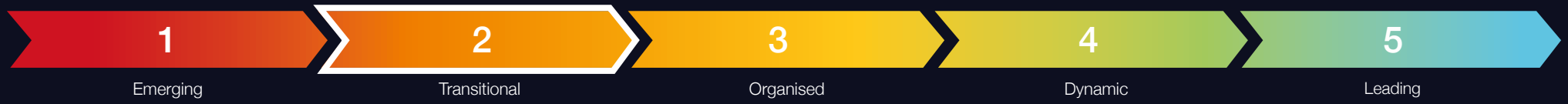
83. Professional membership organisations or associations usually focus on furthering the profession they represent. They provide membership by subscription. Membership benefits range from gaining access to further professional development and training, access to discounted products and events, networking and collaboration with like-minded people and increasing professional credibility. These organisations can frequently be not-for-profit organisations.

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

85. **Eight cyber security-related professional membership organisations were identified as active in Nigeria.** This is a healthy number, placing the country at Maturity Level 3. Many of these professional membership bodies were also counted as certifications bodies.

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment



Assessment – *Maturity Level 2*
Some evidence of in-country cyber security recruitment.

Specialist Cyber Recruitment

86. The presence and activity levels of recruitment companies and platforms provides 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 Nigeria, or marketed cyber qualified freelance professionals registered with them.

87. No specific cyber-security recruiters were found. Of the 10 that research identified, most are well-known international recruiting companies, and all offered ICT- and cyber security-related jobs. **One recruitment company focused specifically on Africa.**

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

88. **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 or exhibitors to pay the ticket price and attend.** CREST's research looked for any cyber or information security events held recently in Nigeria, what level the events were, and how frequently they were held. This provides evidence of the appetite for both cyber security knowledge and services in country. The impact of events can be far reaching, as they are effective hubs for networking, collaboration and information sharing - which helps sow seeds of cyber security inspiration in their audience.

89. **CREST's research found 20 recent cyber security related events, providing good evidence of a healthy number of dedicated cyber security events on offer throughout a typical year.** While currently assessed as Level 3, it was positive to see a mix of locally organised, and a few internationally organised, events taking place.

Dimension 5

Banking Sector Cyber Security Posture

Banking Sector Cyber Security Posture

Overall Dimension Assessment: *Maturity Level 2*

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

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

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

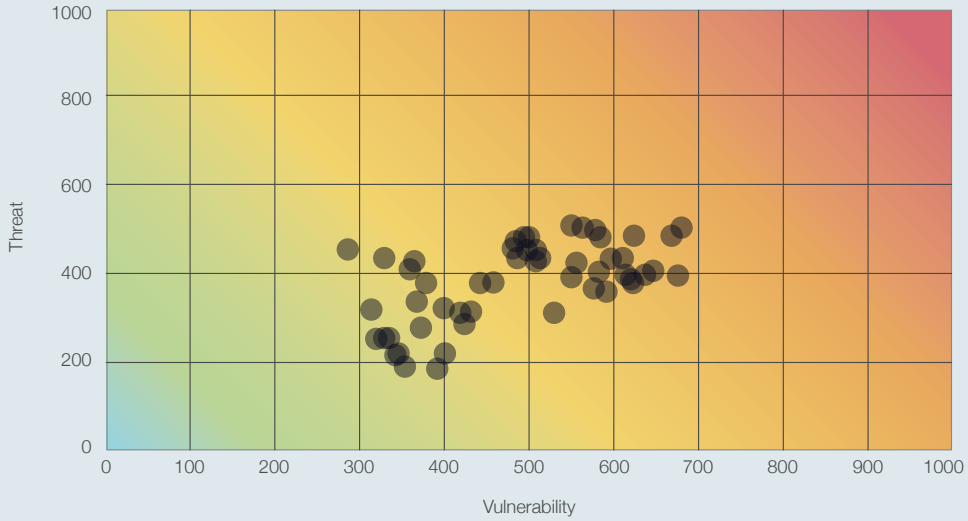
    - The presence of vulnerabilities on public-facing IT infrastructure
    - The presence of open ports on internet-facing servers
    - The adoption of anti-phishing mechanisms
    - Availability of breached employee credentials on online forums and marketplaces frequented by cybercriminals.

91. 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.**

Comparative Risk Rating

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

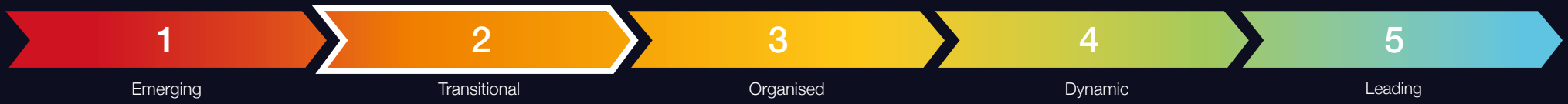


92. In determining the financial institutions to be assessed, the first source was the list of supervised institutions maintained by the Central Bank of Nigeria[53]. This information was cross-checked against the corporate membership list of the Chartered Institute of Bankers of Nigeria[54], Wikipedia[55] and the websites of the financial institutions themselves, to generate a representative sample of national and international banks and microfinance institutions (MFIs) operating in Nigeria.

    Very few of the more than 1000 MFIs had identifiable websites. The website addresses and email domains of 50 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

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

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

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

As visible in the scatter diagram on the previous page, the assessed financial institutions have been found to have **individual vulnerability scores (X-axis) ranging between 281 and 675.** The **average cyber risk score for the sample is 428,** which corresponds to a national average risk rating of **'Medium'**.

95. Note that no active (intrusive) assessment was undertaken, nor was any assessment made of IT infrastructure elements that are not internet-facing. If a comprehensive assessment were made of entire IT infrastructures, internet-facing and otherwise, results may have differed.

However, the level of access required for such assessment are far beyond the scope of this report.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile (continued)

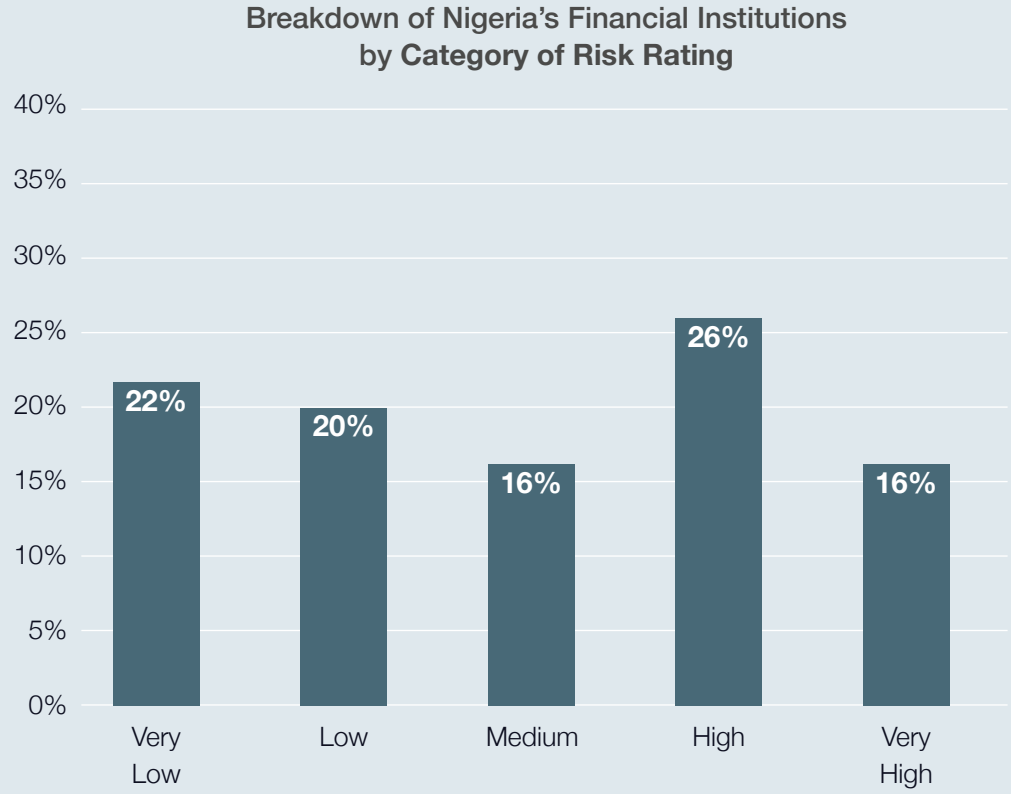
1 Emerging | 2 Transitional | 3 Organised | 4 Dynamic | 5 Leading

Assessment – *Maturity Level 2*

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

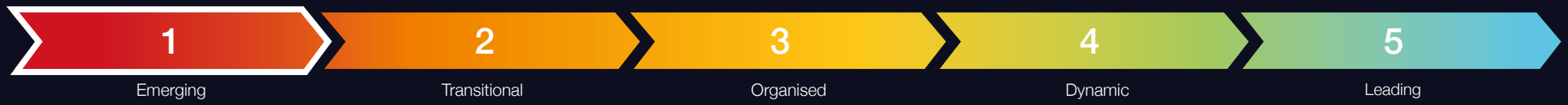
For research purposes, the cyber risk rating of the public-facing infrastructure is considered sufficient to indicate the general security posture of the whole financial services sector. There appears to be significant room for improvement in the cyber security posture of many of the individual financial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

96. A breakdown by category of risk rating of the assessed sample of financial institutions is shown above, and results anonymised. Encouragingly, **42% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'.** But, **42% of the financial institutions surveyed have an overall cyber risk rating of 'Very High' or 'High',** leading to the award of Maturity Level 2 for this indicator. Institutions in these two categories appear likely to not be implementing good cyber hygiene practices and/or to be operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.



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

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

    Ethically, research was limited to carrying out non-intrusive examinations of those infrastructure elements directly connected to the internet. Formally, the results are similarly constrained, but it is reasonable to assume the results are typical of the state of patching across each financial institution's complete IT infrastructure.

98. Vulnerabilities, often referred to as CVEs[56], (Common Vulnerabilities and Exposures) are software and hardware flaws 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 research followed a similar approach, scanning the public-facing IT infrastructure of the 50 financial institutions being assessed. By restricting themselves to passive reconnaissance only, researchers were unable to confirm if the vulnerabilities they detected actually existed. There is a possibility that in some cases they were false positives.

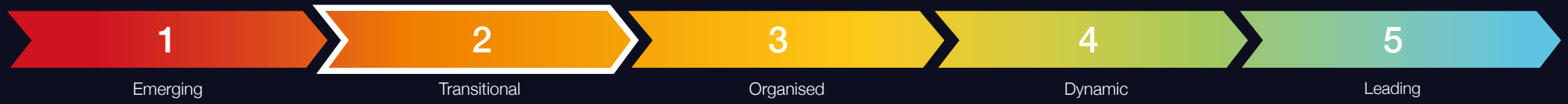
99. The investigation revealed that **56% of Nigeria's financial institutions appear to operate an unsecure internet-facing infrastructure featuring at least one known vulnerability.** The vulnerabilities detected mostly have patches available. Their presence on an internet-facing infrastructure suggests lax patching practices.

100. 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[57] (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 **14% of Nigeria's assessed financial institutions were operating internet-facing IT infrastructure with at least one critical vulnerability.** In those financial institutions with critical vulnerabilities, these results are indicative of a failure to adopt an 'attacker's eye perspective' and prioritise critical CVEs for remediation.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk



Assessment – *Maturity Level 2*

Architecture & Access risk is poor; 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

101. Security architecture and access management are the most common means by which networks and information are secured. “Security by design” is the essential foundation upon which all other cyber defences are built. Insufficient segregation between key assets and unguarded routes to gain unauthorised access are examples of gaps that can be exploited by an attacker. Ethically, the researchers were limited to only examine those assets directly connected to the internet. Therefore, they only focused on the remote access and database ports of internet-facing servers as a simple indicator of the configuration management underpinning the network and, by inference, the likely approach to “security by design”.

102. 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.

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

104.

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)

CREST's research showed that 16% of assessed financial institutions maintain at least one port associated with remote access services open to the internet.

105. In most cases, these ports will have been configured to accept incoming data packets from the internet for a valid business requirement and will have adequate security measures in place. Although banks with open remote access ports on their IT infrastructure remain susceptible to a potential compromise, they are a small subset. Evidence suggests Nigeria's financial services sector is not highly vulnerable to the threat emanating from ports associated with remote access services.

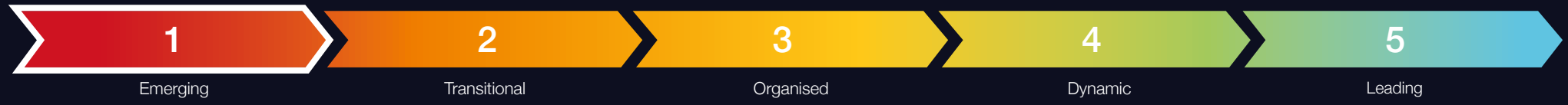
106. Another set of computer server ports cybercriminals often deliberately target are those used by database services. CREST's research showed **28% of assessed financial institutions have at least one database-related port open on their public-facing infrastructure.** Although some of these internet-accessible database services are in place to meet valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.

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

108. Understanding the threat associated with exposed database instances - and reducing the possibility of suffering a data leak - would also reduce the risk of fines under **Nigeria's Data Protection and Privacy Act 2019**[58].

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

109. **Having an inherent susceptibility to social engineering and phishing campaigns is human nature.** While training and education can help prevent successful attacks, using 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.

110. **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 the risk of spoofing, and helping block spam messages, malware and phishing attempts.

111. 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[59].

112. Having SPF and DMARC correctly enabled does not entirely negate the threat from phishing. However, it reduces the chance of falling victim to impersonation attempts and **business email compromise (BEC) scams**. Both are common threats in the financial services sector[60].

113. In a BEC scam, cybercriminals target victims with spear-phishing emails devised to impersonate the company's CEO, an employee with the authority to approve money transfers, or a key supplier, for example. 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 prove highly profitable for cybercriminals. In its **2019 Internet Crime Report**, the FBI estimated that globally BEC scams cost businesses approximately **US$1.8 billion**[61].

114.

28%

CREST's research revealed that **28% of the sample of financial institutions had not implemented basic email authentication measures (SPF)**.

66%

Some 66% 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 3*

Information leakage risk is assessed as average. Fewer than half of the surveyed financial institutions identified as having had some employee credentials compromised in recent years by third-party breaches.

Information Leakage Risk

115. **The more that 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.

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

50%

CREST's research revealed **that 50% of the assessed financial institutions had had at least some employees' credentials leaked online after unconnected attacks on third-party website-based service providers.**

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

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

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

Banking Sector Cyber Security Posture

Mitigation Measures

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

Infrastructure Vulnerability

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

Architecture & Access

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

Email Authentication

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

Information Leakage

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

Appendices

Appendix A

Glossary

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

Appendix A

Glossary (continued)

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

Appendix B

Summary of Maturity Level Definitions

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

Indicator 1.1
Government Strategy & Policy

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

Indicator 1.2
Regulator/Government Operated Assurance Schemes

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 1.3
Law Enforcement & Cyber Defence Capabilities

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1
CERTs & Information Sharing

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

Indicator 3.1
Threat Intelligence Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2
Vulnerability Assessment Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3
Penetration Testing Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4
Security Operation Centre Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5
Incident Response Service providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1
Academia & Higher Education

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

Indicator 4.2
Training Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3
Professional Certifications

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

Indicator 4.4
Professional Cyber Membership Organisations

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5
Specialist Recruitment

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

Indicator 4.6
Events & Exhibitions

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1
Banking Sector Cyber Risk Profile

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

Indicator 5.2
Infrastructure Vulnerability Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3
Architecture & Access Risk

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

Indicator 5.4
Email Authentication Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5
Information Leakage Risk

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

Appendix C

Professional Certifications and Member Organisations

Background

1. Knowledge, skills and experience are factors used by a company when determining who to hire or promote. They are also used by buyers when selecting service providers to award a contract to. Experience is a matter of record and can be underpinned by endorsements from previous employers or previous 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 certifications held. Buyers can use certifications as a benchmark when looking to award contracts. The availability and use of certifications in both scenarios are a useful indicator of the maturity of a marketplace.

Career progression model

2. For ease of evaluation, the 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 offering one or more certification of relevance to the cyber security profession. Together, they offer 142 different certifications, including 118 with differing degrees of technical content (grouped as 'Technical Certificates of Relevance') and 24 more focused on security management and other skillsets (grouped at 'Other Certificates of Relevance'). In some cases, certification organisations also act as professional membership organisations, holding events and contributing to member's career development.

4. Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres. Some certifications requiring practical exams offer this online or through connection to a remote network. Some bodies require a physical testing site, with much more limited availability in Africa.

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 (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[62]		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council[63]	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA[64]		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2[65]		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS[66]		GSEC GPEN GWAPT GICSP GCIP GCWN GCUX GAWN GPYC GWEB GCIH GCFE GASF GREM GCFA GNFA GSSP-Java GSSP-.Net GICSP GMOB GBFA GCSA	GXPN GCCC GSED GPPA GMON GCIA GRID GCDA GCTI GCED GPPA GDSA GDAT GEVA GNSA		GSE	✓	✓			
CompTIA[67]	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security[68]		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance[69]		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[70]		PCIP PCI-DSS QPA	PCI-DSS ISA PCI-DSS AQSA		PCI-DSS QSA PA-QSA PCI-DSS 3DS PCI-DSS P2PE PCI-DSS Secure Software Lifecycle Assessor PCI-DSS Secure Software Assessor PCI-DSS CPSA	✓	✓			
Cisco[71]		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft[72]	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services[73]	AWS Certified Security					✓	✓	✓		
OTHER CERTIFICATES OF RELEVANCE										
EC Council	CNDA CSCU			CCISO		✓	✓		✓	
ISACA		Cybersecurity Audit Scheme COBIT Program	CDPSE			✓		✓		
(ISC)2	Associate of (ISC)2						✓			
SANS	GISF	GLEG GSNA	GISP GCPM	GSLC	GSTRT	✓	✓			
IRCA (ISMS)[74]	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS[75]	CiSMP	BCM CIAA	CIRM				✓		✓	✓
IET[76]	ICTTech									✓

Appendix D

Country Context

Geography

1. The Federal Republic of Nigeria is a commonwealth nation situated in the West of Africa with Niger, Cameroon, Benin and the Atlantic Ocean as neighbours. Abuja is the capital city, but former capital Lagos is the leading commercial and industrial city[77].

Population

2. Nigeria is Africa's most populated country. In 2019 the population was 200,788,00, giving it the sixth largest population in the world. There are 250 different ethnic groups[78]. In 2018, the urban-rural split was 50.3% urban to[79] rural. In 2017, 42.9% of the population was under 15 years old and 26.7% were aged between 15 and 29 years old[80].

3. English is the official language, with Hausa, Igbo and Yoruba also spoken. Male literacy (for those over 15), was 68.9%, female 49.3%[81]. Nigeria has the world's highest number of out-of-school children, 10.5 million - and 60% of those are girls[82].

4. As of 2017, Nigeria sends more students abroad than any other African nation. According to the Joint Administration and Matriculations Board (JAMB), the number of applicants to Nigerian universities exceeds places available by 2:1. In 2016, 1,579,027 students sat the Unified Tertiary Matriculation Examination (UTE) and 45% of University graduates are unemployed[83].

5. In politics, Muhammadu Buhari won the national elections and was sworn in for a second term on May 29, 2019. He has identified fighting corruption, increasing security, tackling unemployment, diversifying the economy, enhancing climate resilience, and boosting the living standards of Nigerians as main policy priorities his government will continue to pursue in his second term – until 2023[84].

6. Nigeria's human capital development remains weak due to under-investment. The country is ranked 152 of 157 countries in the World Bank's 2018 Human Capital Index[85]. Nigeria has massive developmental challenges, including the need to reduce oil dependency and diversify the economy, address insufficient infrastructure, and build strong and effective institutions, as well as governance issues and public financial management systems[86].

Economy

7. The Nigerian economy is one of the largest in Africa, mainly based on the oil industry[87]. It is Africa's biggest oil exporter[88]. Economic growth is slow, or been in recession since 2015[89]. Unemployment in 2018 was 23%, while underemployment stood at 20%[90]. According to a PwC survey dated 2018, corruption will cost 37% of GDP by 2030[91]. As of 2017, GNI per capita is US$2,080[92].

8. According to Serianu's Nigeria Cyber Security Report 2017 - "Demystifying Africa's Cyber Security Poverty Line," the annual cost of cyber attacks in Nigeria is US$649m, with banks being the most targeted sector[93].

Internet connectivity

9. In 2020, Nigeria had 99.05 million internet users. This figure is projected to grow to 131.7 million internet users in 2023. Internet penetration amounted to 46.6% of the population in 2020 and is set to reach 65.2% in 2025[94].

Appendix D

Country Context (continued)

Cyber crime

10. With regards to cybercrime, the 2017 Serianu report cited above identified top trends including fake news, insider threat and ransomware - and that some 81% of cyber incidents go unreported[95]. More than 95% of organisations in both the private and public sectors are either operating on or below the "Security Poverty Line", with most only spending US$1,500 annually on cybersecurity technologies and services. Over 90% of people are affected by cyber bullying - including citizens, media personalities and government officials[96].

11. On page 11, Key Highlights of the Serianu 2017 report[97], there is a chart listing African nations by population and key cyber statistics. Nigeria, Uganda, Tanzania, Kenya and Ghana are five of the nine countries listed. In addition to similar statistics mentioned in the Nigerian report, cyber-attacks cost Africa US$3.9b annually. The report says 90% of parents do not know what measures to take to protect their children from cyber bullying[98].

12. An article in Threatpost (2019)[99], suggests Nigerian cybercrime, such as scam emails distributing malware, and Business Email Compromise (BEC), surged 54% in 2018 across a breadth of industry[100].

13. A 2019 Nigerian Guardian article (*Is Nigeria Really The Headquarters of Cybercrime in the World?*[101]) questioned Nigeria's negative reputation regarding cybercrime. It stated 7% of all online transactions within Africa in 2013 were fraudulent, almost three times the size of Europe's 2% and North America's 1%. The article quoted FBI estimates that between October 2013 and December 2016 more than 40,000 BEC incidents worldwide resulted in losses of US$5.3 billion. But the article states that Nigerians were more focused on social cons, such as romance cons, foreign money exchange and business scam emails, which are more popular and visible rather than digital manipulation.

    These methods are less profitable than investment scams, moving scams and cryptocurrency scams, types of scam that are more popular in Russia, China, India and Brazil. The article concludes that Nigeria's cybercrime reputation has more to do with public visibility than actual profit[102]. Nigeria is one of the largest countries in Africa, and the combination of corruption, unemployment and a large youth population mean a high amount of the population resort to scamming as a means of livelihood[103].

14. A 2020 article from analytical business magazine Stears Business, entitled "*Nigeria's Cybersecurity Problem*"[104], states that not forcing companies to report data breaches is a critical missing piece in the 2019 National Information Technology Development Agency's (NITDA), Nigeria Data Protection Regulation (NDPR). Stears' goes on to say the regulation undermines the National Cybersecurity Strategy - the lack of public information regarding breaches makes it much harder for both customers and other companies to take action[105].

15. A Palo Alto Networks' article, "*Silver Terrier: 2019 Nigerian Business Email Compromise Update (2020)*"[106], reported on its ongoing research into Nigerian cybercrime, and the enormity of BEC attacks originating from the region. Palo Alto Networks has assigned a team of researchers dedicated to exploring cybercrimes emanating from Nigeria, called SilverTerrier, which, at the time of the article, had unearthed more than 81,300 samples of malware linked to 2.1 million attacks. In the five years from 2014 to 2019, SilverTerrier has noted that Nigerian cybercriminals have evolved from being novice threat adversaries to mature cybercriminals. For example, there was a 1,163% increase in BEC attacks against the professional and legal services industry in 2019[107].

Appendix D

Country Context (continued)

16. An EFCC article, "*FBI Commends EFCC on Indictment of Six Nigerians for Cyber Crime (2020)*"[108], describes the investigation and prosecution of six Nigerians involved in Business Email Compromise (BEC) and wire fraud in the USA, where US$6m was stolen. The six Nigerians indicted by the FBI were accused of "...violations of federal laws: 1) Conspiracy to commit wire fraud and wire fraud, punishable by up to 20 years of imprisonment and a fine of up to $250,000; 2) Identity theft and access device fraud, each punishable by up to 10 years imprisonment and a fine of up to $250,000"[109].

Cyber Security Professional Development

17. Serianu's Nigeria Cyber Security Report (2017) – Demystifying Africa's Cybersecurity Poverty Line, says (in 2017) there were an estimated 1800 cyber professionals working in Nigeria[110]. It summarises the gaps in Nigeria's cybersecurity, including combatting insider threats, and a lack of training for board member and IT teams on cyber security[111].

18. The 2016 Cyber Security Trends Report Africa by Symantec covers Nigeria on pp81-82[112]. It states the main challenges Nigeria's government faces is a general lack of awareness of cybersecurity measures and the risks associated with cybercrime. The focus for the government (at the time of the report) on cybercrimes issues was with the private sector, as the economy is driven by this sector. Nigeria has fruitful relations with international communities when managing and responding to cyber threats, and promotes confidence building measures (CBM) and international cooperation in cyberspace, by exchanging information on cyber incidents and best practices for cybersecurity[113].

Other maturity models

19. The Global Cyber Security Index has undertaken a Cybersecurity Capacity Maturity Model for Nations (CMM) exercise on Nigeria dated 2019, but findings remain unpublished[114].

20. The National Cyber Security Index currently ranks Nigeria as 45th of 160 on the National Index, 57th on the Global Index, 143rd on the ICT Development Index and 119th on the Networked Readiness Index[115].

Appendix E

Bibliography

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

Africa CERT, 2020,
https://www.africacert.org/about-us/
(accessed Mar 2020 Jan 21)

African Centre for Media Excellence,
https://acme-ug.org/
(accessed July and Oct 2020)

Areo, Oluwatosin. (2019). Nigeria: Experts Urge Govt to establish Cyber Security Centre.
Nigeria: *The Guardian.* (online)
Available from: **https://crestuk.sharepoint.com/sites/GatesFoundationTeam812-GatesCountries/Shared%20Documents/Gates%20Countries/Nigeria/Archive** (accessed Jan 20)

Balancing Act (2007). Nigerians Federal Government Okays N1.2B for Cybersecurity Directorate.
Nigeria: *Balancing Act* Issue no 350 15th April 2007. (online).
https://www.balancingact-africa.com/news/telecoms-en/4250/nigerias-federal-government-okays-n12b-for-cybersecurity-directorate

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

Bola-Balogun, Florence. (2019). Nigeria: The Evolution of Cyber Security in The Nigerian Banking Sector.
UK: *Mondaq.* (online)
https://www.mondaq.com/Nigeria/Technology/799360/The-Evolution-Of-Cyber-Security-In-The-Nigerian-Banking-Sector

Central Bank of Nigeria.
https://www.cbn.gov.ng/
(accessed Jan 20, Feb 21)

Central Bank of Nigeria (2018). DRAFT Risk-Based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers.
Nigeria: *Author.* (online)
https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20Exposure%20Draft%20June.pdf
(accessed Jan 20, Feb 21)

Collaboration on International ICT Policy in East and Southern Africa (CIPESA),
https://cipesa.org/about-us/
(accessed July 2020)

Computer Emergency Readiness and Response Team (CERRTng) (2020). *NITDA*
https://www.cerrt.ng/ (accessed Mar 20)

Council of Europe, (2020). Nigeria Cybercrime Legislation.
France: *Author.* (online)
https://rm.coe.int/octocom-legal-profile-nigeria/16809e5325 (accessed Jan 20)

Council of Europe, (2020). Nigeria Cybercrime Policies and Strategies.
France: *Author.* (online)
https://www.coe.int/en/web/octopus/country-wiki
(accessed Jan 20 and 21)

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

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

Crowdstrike Global Intelligence Team., (2018). Nigerian Confraternities Emerge as Business Email Compromise Threat. CSIR-18004.
USA: *Author.* (online)
https://www.crowdstrike.com/wp-content/uploads/2020/03/NigerianReport.pdf
(accessed Jan 20 and Feb 21)

Appendix E

Bibliography (continued)

CyberSecFill, (2020) Nigeria. (Online)
https://www.cybersecfill.com/
(accessed Feb 2020 and Jan 21)

Economic Financial Crimes Commission, (EFCC) (2021)
https://www.efccnigeria.org/efcc/
(accessed Jan 20)

Economic and Financial Crimes Commission (EFCC) Act 2004.
https://efccnigeria.org/efcc/about-efcc/the-establishment-act
(accessed Jan 20 and 21)

Economic Financial Crimes Commission (EFCC). (2020). FBI Commands EFCC on Indictment of Six Nigerian for Cyber Crime.
Nigeria: *Author.* (online).
https://www.efccnigeria.org/efcc/news/5782-fbi-commends-efcc-on-indictment-of-six-nigerians-for-cyber-crime? (accessed Jan 20)

Economic Financial Crimes Commission (EFCC). (2018). UK to support EFCC's Anti-Corruption Fight with Digital Forensic Technology.
Nigeria: *Author* (online).
https://www.efccnigeria.org/efcc/news/3328-uk-to-support-efcc-s-anti-corruption-fight-with-digital-forensic-technology? (accessed Jan 20).

Elearning Infographics, (2018). UNICEF Statistics On Education In Nigeria Infographic. *Author.* (online)
https://elearninginfographics.com/education-in-nigeria-infographic-unicef-statistics-on/
(accessed Jul 20)

Enoch, John (Date Unknown). Design and Implementation of Visualisation Tool for Terroirst & Cyber Threat Detection and Prevention in Nigeria.
UK: *IOT Security Institute.* (online).
https://iotsecurityinstitute.com/iotsec/index.php/cti?task=document.viewdoc&id=23
(accessed Jan 20)

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

European Union Institute of Security Studies (ISS), African Future 2030 Task Force.
France: *Author.* (online)
https://www.iss.europa.eu/content/african-futures-2030-task-force (accessed Jan 20)

Famsville Solicitors. (2018). Cybersecurity Understanding the Threat Landscape and Lessons from the GDPR for Nigerian Entities.
Nigeria: *Author*. (online).
https://www.famsvillelaw.com/cybersecurity-understanding-the-threat-landscape-and-lessons-from-the-gdpr-for-nigerian-entities/
(accessed Jan 20)

Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria.
USA: *Encyclopaedia Britannica.* (online)
https://www.britannica.com/place/Nigeria
(Accessed Jan 20 and 2 Feb 2021).

Federal Government of Nigeria. (2015). Cybercrimes (Prohibition, Prevention Ect) Act 2015.
Nigeria: *Author* (online)
Available from: **https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf** (accessed Jan 20 and Jan 21)

Federal Government of Nigeria, National Information Technology Development Agency, (2021).
https://nitda.gov.ng/department/cyber-security/
(accessed Mar 20 and Jan 21).

Federal Government of Nigeria, Office of The National Security Advisor (NSA), (2014) National Cybersecurity Strategy.
Nigeria: *ngCERT* (online).
https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf
(accessed Mar 20, Jan 21)

Forum of Incident Response and Security Teams (FIRST), 2015-2020,
https://www.first.org/about/mission
(accessed 20 Mar 2020)

Frank, Ibikunle Dr, Odunayo Eweniyi (2013). Approach to Cyber Security Issues in Nigeria, Challenges and Solutions. *International Journal of Cognitive Research in Science, Engineering and Education: Vol 1, No1 2013. and Academia.Edu* (online)
https://www.academia.edu/5118994/APPROACH_TO_CYBER_SECURITY_ISSUES_IN_NIGERIA_CHALLENGES_AND_SOLUTION
(accessed Jan 20 and Jan 21)

Appendix E

Bibliography (continued)

Global Cyber Security Capacity Centre (2021). Nigeria (GCSCC) 2019 – not yet published.
Oxford: *Author,* 2016,
https://gcscc.web.ox.ac.uk/cmm-reviews
(accessed Mar 2020)

Iasiello, Emillo. (2018). Nigeria: Will a Cyber Command Solve its Cybercrime Problems?
London: *Technative.* (online).
https://technative.io/nigeria-will-a-cyber-command-solve-its-cyber-crime-problems/
(accessed Jan 20)

Idris, Ismaila & Majigi, Muhammad & Olalere, Morufu & Rambo, Saidu & Abdulhamid, Shafi'i. (2017). Vulnerability Assessment of Some Key Nigeria Government Websites. International Journal of Digital Information and Wireless Communications (IJDIWC). 7. 143-152. 10.17781/P002309. (online)
Available From: **https://www.researchgate.net/publication/321579059_Vulnerability_Assessment_of_Some_Key_Nigeria_Government_Websites**
(accessed Jan 20).

Independent Corrupt Practices and Other Related Offences Commission, (2020).
https://icpc.gov.ng/ (accessed Jan 20 and Jan 21)

INTERPOL (2021). How INTERPOL supports Nigeria to tackle International Crime.
France: *Author* (Online)
https://www.interpol.int/en/Who-we-are/Member-countries/Africa/NIGERIA (accessed Feb 21)

INTERPOL, (2019). Nigeria and INTERPOL formalise West African Police Information System Cooperation.
France: *Author.* (online).
https://www.interpol.int/en/News-and-Events/News/2019/Nigeria-and-INTERPOL-formalize-West-African-Police-Information-System-cooperation
(accessed Jan 20 and Feb 21)

ITedge News (2016). Nigerian Police Force Pans Technology Deployment to Combat Cybercrime.
Nigeria: *Author* (online).
https://itedgenews.ng/2016/10/28/nigeria-police-force-plans-technology-deployment-to-combat-cyber-crime/ (accessed Jan 20 and Feb 21)

Johnson, Joseph (2021).
Nigeria: *Number of Online Users 2015-2025. Statista.* (online)
https://www.statista.com/statistics/183849/internet-users-nigeria/ (accessed Jan 20 and Jan 21)

Lateef, Hazmat.(2019). A Review of the Nigeria National Cybersecurity Strategy.
Nigeria: *CyberSecFill.* (online)
https://www.cybersecfill.com/nigeria-cybersecurity-strategy/ (accessed Feb 20 and Jan 21)

Makeri Ajiji, Yakubu. (2017). Cyber Security Issues in Nigeria and Challenges. International Journal of Advanced Research in Computer Science and Software Engineering. 7. 315-321. 10.23956/ijarcsse/V6I12/01204. (online) Available from: **https://www.researchgate.net/publication/318668652_Cyber_Security_Issues_in_Nigeria_and_Challenges/citation/download**
(accessed Jan 20)

Mallick, Bolakale (2019). Cybersecurity Regulation in The Nigerian Fintech Industry.
UK: *Mondaq.* (online)
https://www.mondaq.com/Nigeria/Technology/872530/Cybersecurity-Regulation-In-The-Nigerian-Fintech-Industry (accessed Jan 20)

Maska, M U, (2009). Building National Cybersecurity Capacity in Nigeria: The Journey So Far. Nigeria: Director of Cybersecurity, Office of National Security Advisor. (online) Available from: **https://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf**

Mordi, Melisaa (2019). Is Nigeria The headquarters of Cybercrime in the World?.
Nigeria: *The Guardian.*
https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/
(accessed Jan 20)

National Assembly of the Federal Republic of Nigeria, (2021)
https://www.nassnig.org/default
(accessed Mar 20 and Jan 21)

National Assembly of the Federal Republic of Nigeria (2015). Cybercrimes (Prohibition Prevention etc) Act 2015.
Nigeria: *ngCERT* (online)
https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf (accessed Mar 20 and Jan 21)

Appendix E

Bibliography (continued)

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

National Cyber Security Index. Estonia: *e-Governance Academy,* (online) **https://ncsi.ega.ee/ncsi-index/** (accessed Feb 21)

National Information Technology Development Agency (NITDA), (2021). Nigeria: *Author* (online) **https://nitda.gov.ng** (accessed Jan 21)

National Information Technology Development Agency (NITDA), (2021). Computer Emergency Readiness and Response Team. Nigeria: *Author* (online) **https://nitda.gov.ng/computer-emergency-readiness-and-response-team-unit/** (accessed Jan 21)

National Information Technology Development Agency (NITDA), (2021). Cybersecurity Department. Nigeria: *Author* online **https://nitda.gov.ng/department/cyber-security/** (accessed Jan 21)

Newman, Hay L. (2018). Nigerian Email Scammer are More Effective than Ever. USA: *Wired* (online) **https://www.wired.com/story/nigerian-email-scammers-more-effective-than-ever/** (accessed Jan 20)

Nigeria Computer Emergency Response Team NgCERT, (2019). **https://www.cert.gov.ng/** (accessed Feb 20)

Nigerian Communication Commission (2021). **https://www.ncc.gov.ng/** (accessed Jan 20 and 21)

Nigerian Communications Commission, (2021). Understanding the Concept of Cyber Security. Nigeria: *Policy Competition & Economic Analysis Dept.* (online) **https://www.ncc.gov.ng/docman-main/industry-statistics/research-reports/682-understanding-the-concept-of-cyber-security/file** (accessed Jan 20 and Jan 21)

Nigerian Military Blog (2019). The Nigerian Army Cyber warfare Command, The most advanced and first in Africa. Nigeria: *Author* (online). **https://africastrongestmilitary.wordpress.com/2019/09/13/the-nigerian-army-cyberwarfare-command-the-most-advance-and-first-in-africa/** (accessed Jan 20, and Jan 21)

Nigerian Police (2019). **https://www.npf.gov.ng/** (accessed Jan 20 and 5 Feb 21)

Nigerian Universities Commission. **https://www.nuc.edu.ng/** (accessed Jan 20 and Jan 21)

O'Donnell, Lindsey. (2019). Threatlist: Nigerian Cybercrime Surged 54 Percent in 2019 USA: *Threatpost.* (online). **https://threatpost.com/threatlist-nigerian-cybercrime-surged-54-percent-in-2018/144561/** (accessed Jan 20)

O'Flaherty, Kate (2018). The Nigerian Cyber Warfare Command: Waging War in Cyberspace. USA: *Forbes* (online). **https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=27ed18ce2fba** (accessed Jan 20 and Feb 21).

Oforji Jerome, C. Udensi Ezinne, J. Ibegbu Kelechi, C. (2017). CYBERSECURITY CHALLENGES IN NIGERIA: THE WAY FORWARD. NIGERIA: *SosPoly Journal of Science & Agriculture, Vol. 2, (Dec, 2017) ISSN: 2536-7161.* (online) Available From: **https://www.uaspolysok.edu.ng/sospolyjsa/view/172203.pdf** (accessed Jan 20 and 21)

Omodunbi, Bolaji & Odiase, P. & Olaniyan, Olatayo & Esan, Adebimpe. (2016). Cybercrimes in Nigeria: Analysis, Detection and Prevention. FUOYE Journal of Engineering and Technology. vol. 1. 37-42. 10.46792/fuoyejet.v1i1.16. (Online) Available from: **https://www.researchgate.net/publication/320411102_Cybercrimes_in_Nigeria_Analysis_Detection_and_Prevention** (accessed Jan 20 and 21)

PWC. (2018). 2018 Nigerian Family Business Survey. Nigeria: *Author.* (online) **https://www.pwc.com/ng/en/press-room/2018-nigeria-family-business-survey.html** (accessed Jan 20)

Appendix E

Bibliography (continued)

Renals, Peter (2020). Silver Terrier: 2019 Nigerian Business Email Compromise Update.
Palo Alto Networks. (online).
https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (accessed Jan 20).

Reuters. (2018). Nigerian Unemployment rises to 23% in Q3.
South Africa: *CBN Africa.* (online).
https://www.cnbcafrica.com/2018/nigerias-unemployment-rate-rises-to-23-1-percent-in-q3/
(accessed Jan 20)

Serianu, (2017). Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line' Kenya, *Author.* (online)
https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf
(accessed Jan and Jul 2020)

Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line.
Kenya: *Author.* (online)
https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf
(accessed Jan 20)

Stears business, (2020), Nigeria's Cyber Security Problem.
Nigeria: *Author.* (online).
https://www.stearsng.com/article/nigerias-cybersecurity-problem (accessed Jan 20)

Symantec (2016). Cyber Security Trends Report Africa.
USA: *Author.* (online)
Available from: **https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf** (accessed Jan 20 and 21)

The World Bank. (2020). The World Bank in Nigeria – Overview. *Author.* (online)
https://www.worldbank.org/en/country/nigeria/overview (accessed Jul 20)

Umar, Hassan & Umar, Kasim. (2016). The Economic and Financial Crimes Commission and Corruption Management in Nigeria: a Perceptual Assessment of its Legal Framework. Journal of Siberian Federal University. Humanities & Social Sciences. 9. 310-317. 10.17516/1997-1370-2016-9-2-310-317. (online)
Available from: **https://www.researchgate.net/publication/308755015_The_Economic_and_Financial_Crimes_Commission_and_Corruption_Management_in_Nigeria_a_Perceptual_Assessment_of_its_Legal_Framework** (accessed Jan 20 and 21)

UN, 'UNDIR Cyber Security Portal (2019).
Nigeria. *Author* (online)
https://cyberpolicyportal.org/en/states/nigeria
(accessed Jan 20 and Jan 21)

Vanguard (2018). UK Crime Agency aids EFCC's Forensic Lab with £500,000.
Nigeria: *Author* (online).
https://www.vanguardngr.com/2018/07/uk-crime-agency-aids-efccs-forensic-lab-with-500000/
(accessed Jan 20, Feb 21)

World Education News and Reviews. WENR, (2017). Education In Nigeria. *Author.* (online)
https://wenr.wes.org/2017/03/education-in-nigeria
(accessed Jan 20)

Appendix F

Endnotes

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

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

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

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

4. Balancing Act (2007). Nigerians Federal Government Okays N1.2B for Cybersecurity Directorate. Nigeria: *Balancing Act Issue no 350 15th April 2007.* (online). **https://www.balancingact-africa.com/news/telecoms-en/4250/nigerias-federal-government-okays-n12b-for-cybersecurity-directorate**

5. Maska, M U, (2009). Building National Cybersecurity Capacity in Nigeria: The Journey So Far. Nigeria: *Director of Cybersecurity, Office of National Security Advisor.* (online). Slide 11. Available from: **https://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf**

6. Maska, M U, (2009). Building National Cybersecurity Capacity in Nigeria: The Journey So Far. Nigeria: *Director of Cybersecurity, Office of National Security Advisor.* (online) Available from: **https://www.itu.int/ITU-D/cyb/events/2009/tunis/docs/maska-nigeria-cybersecurity-june-09.pdf**

7. Central Bank of Nigeria (2018). DRAFT Risk-Based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers. Nigeria: *Author.* (online) **https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20Exposure%20Draft%20June.pdf** (accessed Jan 20, Feb 21)

8. Federal Government of Nigeria, Office of The National Security Advisor (NSA), (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

9. Federal Government of Nigeria, Office of The National Security Advisor (NSA), (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

10. Lateef, Hazmat.(2019). A Review of the Nigeria National Cybersecurity Strategy. Nigeria: *CyberSecFill.* (online) **https://www.cybersecfill.com/nigeria-cybersecurity-strategy/** (accessed Feb 20 and Jan 21)

11. Lateef, Hazmat.(2019). A Review of the Nigeria National Cybersecurity Strategy. Nigeria: *CyberSecFill.* (online) **https://www.cybersecfill.com/nigeria-cybersecurity-strategy/** (accessed Feb 20 and Jan 21)

12. National Information Technology Development Agency, (2021). Nigeria: *Author* (online) **https://nitda.gov.ng** (accessed Jan 21)

13. National Information Technology Development Agency, (2021). Cybersecurity Department. Nigeria: *Author* (online) **https://nitda.gov.ng/department/cyber-security/** (accessed Jan 21)

Appendix F

Endnotes (continued)

14. National Information Technology Development Agency, (2021). Computer Emergency Readiness and Response Team.
Nigeria: *Author* (online)
https://nitda.gov.ng/computer-emergency-readiness-and-response-team-unit/
(accessed Jan 21)

15. Federal Government of Nigeria. (2015). Cybercrimes (Prohibition, Prevention Ect) Act 2015.
Nigeria: *Author* (online)
Available from: **https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf** (accessed Jan 20 and Jan 21)

16. Central Bank of Nigeria (2018). DRAFT Risk-Based Cybersecurity Framework and Guidelines For Deposit Money Banks and Payment Service Providers.
Nigeria: *Author.* (online)
https://www.cbn.gov.ng/Out/2018/BSD/RISK%20BASED%20CYBERSECURITY%20FRAMEWORK%20Exposure%20Draft%20June.pdf
(accessed Jan 20, Feb 21)

17. Mallick, Bolakale (2019). Cybersecurity Regulation in The Nigerian Fintech Industry.
UK: *Mondaq.* (online)
https://www.mondaq.com/Nigeria/Technology/872530/Cybersecurity-Regulation-In-The-Nigerian-Fintech-Industry (accessed Jan 20)

18. Economic and Financial Crimes Commission (EFCC) Act 2004.
https://efccnigeria.org/efcc/about-efcc/the-establishment-act (accessed Jan 20 and 21)

19. Vanguard (2018). UK Crime Agency aids EFCC's Forensic Lab with £500,000.
Nigeria: *Author* (online).
https://www.vanguardngr.com/2018/07/uk-crime-agency-aids-efccs-forensic-lab-with-500000/
(accessed Jan 20, Feb 21)

20. Economic Financial Crimes Commission, (EFCC) (2021)
https://www.efccnigeria.org/efcc/
(accessed Jan 20)

21. Famsville Solicitors. (2018). Cybersecurity Understanding the Threat Landscape and Lessons from the GDPR for Nigerian Entities.
Nigeria: *Author.* (online).
https://www.famsvillelaw.com/cybersecurity-understanding-the-threat-landscape-and-lessons-from-the-gdpr-for-nigerian-entities/
(accessed Jan 20)

22. Vanguard (2018). UK Crime Agency aids EFCC's Forensic Lab with £500,000.
Nigeria: *Author* (online).
https://www.vanguardngr.com/2018/07/uk-crime-agency-aids-efccs-forensic-lab-with-500000/
(accessed Jan 20, Feb 21)

23. Economic Financial Crimes Commission (EFCC). (2020). FBI Commands EFCC on Indictment of Six Nigerian for Cyber Crime.
Nigeria: *Author.* (online).
https://www.efccnigeria.org/efcc/news/5782-fbi-commends-efcc-on-indictment-of-six-nigerians-for-cyber-crime? (accessed Jan 20)

24. Symantec (2016). Cyber Security Trends Report Africa.
USA: *Author.* (online)
Available from: **https://www.thehaguesecuritydelta.com/media/com_hsd/report/135/document/Cyber-security-trends-report-Africa-en.pdf**
(accessed Jan 20 and 21)

25. Independent Corrupt Practices and Other Related Offences Commission, (2020).
https://icpc.gov.ng/ (accessed Jan 20 and Jan 21)

26. Nigerian Police (2019).
https://www.npf.gov.ng/
(accessed Jan 20 and 5 Feb 21)

27. ITedge News (2016). Nigerian Police Force Plans Technology Deployment to Combat Cybercrime.
Nigeria: *Author* (online).
https://itedgenews.ng/2016/10/28/nigeria-police-force-plans-technology-deployment-to-combat-cyber-crime/ (accessed Jan 20 and Feb 21)

28. INTERPOL (2021). How INTERPOL supports Nigeria to tackle International Crime.
France: *Author* (Online)
https://www.interpol.int/en/Who-we-are/Member-countries/Africa/NIGERIA (accessed Feb 21)

29. INTERPOL, (2019). Nigeria and INTERPOL formalise West African Police Information System Cooperation.
France: *Author.* (online).
https://www.interpol.int/en/News-and-Events/News/2019/Nigeria-and-INTERPOL-formalize-West-African-Police-Information-System-cooperation (accessed Jan 20 and Feb 21)

Appendix F

Endnotes (continued)

30. O'Flaherty, Kate (2018). The Nigerian Cyber Warfare Command: Waging War in Cyberspace. USA: *Forbes* (online). **https://www.forbes.com/sites/kateoflahertyuk/2018/11/26/the-nigerian-cyber-warfare-command-waging-war-in-cyberspace/?sh=27ed18ce2fba** (accessed Jan 20 and Feb 21).

31. Nigerian Military Blog (2019). The Nigerian Army Cyber warfare Command, The most advanced and first in Africa. Nigeria: *Author* (online). **https://africastrongestmilitary.wordpress.com/2019/09/13/the-nigerian-army-cyberwarfare-command-the-most-advance-and-first-in-africa/** (accessed Jan 20, and Jan 21)

32. Nigeria Computer Emergency Response Team Ng CERT, (2019). **https://www.cert.gov.ng/** (accessed Feb 20)

33. Forum of Incident Response and Security Teams (FIRST), 2015-2020, **https://www.first.org/about/mission** (accessed 20 Mar 2020)

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

35. Federal Government of Nigeria, National Information Technology Development Agency, (2021). **https://nitda.gov.ng/department/cyber-security/** (accessed Mar 20 and Jan 21)

36. Computer Emergency Readiness and Response Team (CERRTng) (2020) **https://www.cerrt.ng/** (accessed Mar 20)

37. AfricaCERT (2020) **https://www.africacert.org/** (accessed Mar 20)

38. Federal Government of Nigeria, National Security Advisor, (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). Ch 6.1 p34. **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

39. National Assembly of the Federal Republic of Nigeria (2015). Cybercrimes (Prohibition Prevention etc) Act 2015. Nigeria: *ngCERT* (online) **https://www.cert.gov.ng/ngcert/resources/CyberCrime__Prohibition_Prevention_etc__Act__2015.pdf** (accessed Mar 20 and Jan 21)

40. Federal Government of Nigeria, National Security Advisor, (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). Ch 6.2 p34-35. **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

41. Federal Government of Nigeria, National Security Advisor, (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). Ch 6.7 p37. **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

42. National Information Technology Development Agency, (2021). Computer Emergency Readiness and Response Team. Nigeria: *Author* (online) **https://nitda.gov.ng/computer-emergency-readiness-and-response-team-unit/** (accessed Jan 21)

43. Computer Emergency Readiness and Response Team (CERRTng) (2020) **https://www.cerrt.ng/** (accessed Mar 20 and Jan 21)

44. Cyber Security Alliance for Mutual Progress (CAMP), (2020). About CAMP. Korea: *Author.* **https://www.cybersec-alliance.org/camp/membership.do** (accessed July 20 and Jan 21)

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

Appendix F

Endnotes (continued)

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

47. Nigeria Computer Emergency Response Team NgCERT, (2019). **https://www.cert.gov.ng/** (accessed Feb 20)

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

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

50. 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)

51. Federal Government of Nigeria, Office of The National Security Advisor (NSA), (2014) National Cybersecurity Strategy. Nigeria: *ngCERT* (online). **https://www.cert.gov.ng/ngcert/resources/NATIONAL_CYBESECURITY_STRATEGY.pdf** (accessed Mar 20, Jan 21)

52. Nigerian Universities Commission. **https://www.nuc.edu.ng/** (accessed Jan 20 and Jan 21)

53. Central Bank of Nigeria, Supervised Institutions, **https://www.cbn.gov.ng/Supervision/finstitutions.asp** (accessed 9 May 2020)

54. Chartered Institute of Bankers of Nigeria, **https://www.cibng.org/bank-directory** (accessed 9 May 2020)

55. Wikipedia, List of Banks in Nigeria, **https://en.wikipedia.org/wiki/List_of_banks_in_Nigeria** (accessed 9 May 2020)

56. 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)

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

58. Nigeria Data Protection Laws and regulations 2020, **https://iclg.com/practice-areas/data-protection-laws-and-regulations/nigeria** (accessed 23 Dec 20)

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

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

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

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

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

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

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

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

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

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

Appendix F

Endnotes (continued)

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

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

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

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

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

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

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

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

77. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria- Introduction and Quick Facts. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

78. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria - Introduction and Quick Facts. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

79. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria - Introduction and Quick Facts. USA: *Encyclopaedia Britannica*. (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

80. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria Introduction and Quick Facts. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

81. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria - Introduction and Quick Facts. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

82. Elearning Infographics, (2018). UNICEF Statistics on Education in Nigeria Infographic. *Author*. (online) **https://elearninginfographics.com/education-in-nigeria-infographic-unicef-statistics-on/** (accessed Jul 20)

83. World Education News and Reviews. WENR, (2017). Education in Nigeria. *Author*. (online) **https://wenr.wes.org/2017/03/education-in-nigeria** (accessed Jan 20)

84. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author*. (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

85. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author.* (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

86. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author.* (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

87. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria - Economy. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

Appendix F

Endnotes (continued)

88. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author.* (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

89. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author.* (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

90. The World Bank. (2020). The World Bank in Nigeria – Overview. *Author*. (online) **https://www.worldbank.org/en/country/nigeria/overview** (accessed Jul 20)

91. PWC. (2018). 2018 Nigerian Family Business Survey. Nigeria: *Author.* (online) **https://www.pwc.com/ng/en/press-room/2018-nigeria-family-business-survey.html** (accessed Jan 20)

92. Falola, Toyin O. Kirk-Greene, Anthony Hamilton Millard. Udo, Reuben Kenrick. Ajayi, J.F. Ade. (2020). Nigeria - Introduction and Quick Facts. USA: *Encyclopaedia Britannica.* (online) **https://www.britannica.com/place/Nigeria** (Accessed Jan 20 and 2 Feb 2021).

93. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line. Kenya: *Author.* P11. (online) **https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf** (accessed Jan 20)

94. Johnson, Joseph (2021). Nigeria: Number of Online Users 2015-2025. *Statista.* (online) **https://www.statista.com/statistics/183849/internet-users-nigeria/** (accessed Jan 20 and Jan 21)

95. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line. Kenya: Author. p11 (online) **https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf** (accessed Jan 20)

96. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line. Kenya: Author. p11 (online) **https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf** (accessed Jan 20)

97. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line. Kenya: Author. p11 (online) **https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf** (accessed Jan 20)

98. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line. Kenya: Author. p11 (online) **https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf** (accessed Jan 20)

99. O'Donnell, Lindsey. (2019). Threatlist: Nigerian Cybercrime Surged 54 Percent in 2019. USA: *Threatpost.* (online). **https://threatpost.com/threatlist-nigerian-cybercrime-surged-54-percent-in-2018/144561/** (accessed Jan 20)

100. O'Donnell, Lindsey. (2019). Threatlist: Nigerian Cybercrime Surged 54 Percent in 2019. USA: *Threatpost.* (online). **https://threatpost.com/threatlist-nigerian-cybercrime-surged-54-percent-in-2018/144561/** (accessed Jan 20)

101. Mordi, Melisaa (2019). Is Nigeria The headquarters of Cybercrime in the World?. Nigeria: *The Guardian.* **https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/** (accessed Jan 20)

102. Mordi, Melisaa (2019). Is Nigeria The headquarters of Cybercrime in the World?. Nigeria: *The Guardian.* **https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/** (accessed Jan 20)

103. Mordi, Melisaa (2019). Is Nigeria The headquarters of Cybercrime in the World?. Nigeria: *The Guardian*. **https://guardian.ng/news/is-nigeria-really-the-headquarters-of-cybercrime-in-the-world/** (accessed Jan 20)

Appendix F

Endnotes (continued)

104. Stears business, (2020), Nigeria's Cyber Security Problem.
Nigeria: *Author.* (online).
https://www.stearsng.com/article/nigerias-cybersecurity-problem (accessed Jan 20)

105. Stears business, (2020), Nigeria's Cyber Security Problem.
Nigeria: *Author.* (online).
https://www.stearsng.com/article/nigerias-cybersecurity-problem (accessed Jan 20)

106. Renals, Peter (2020). Silver Terrier: 2019 Nigerian Business Email Compromise Update. *Palo Alto Networks.* (online).
https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (accessed Jan 20).

107. Renals, Peter (2020). Silver Terrier: 2019 Nigerian Business Email Compromise Update.
Palo Alto Networks. (online).
https://unit42.paloaltonetworks.com/silverterrier-2019-update/ (accessed Jan 20).

108. Economic Financial Crimes Commission (EFCC). (2020). FBI Commands EFCC on Indictment of Six Nigerian for Cyber Crime. *Author.* (online).
https://www.efccnigeria.org/efcc/news/5782-fbi-commends-efcc-on-indictment-of-six-nigerians-for-cyber-crime? (accessed Jan 20)

109. Economic Financial Crimes Commission (EFCC). (2020). FBI Commands EFCC on Indictment of Six Nigerian for Cyber Crime. *Author.* (online).
https://www.efccnigeria.org/efcc/news/5782-fbi-commends-efcc-on-indictment-of-six-nigerians-for-cyber-crime? (accessed Jan 20)

110. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line.
Kenya: *Author.* P11 (online)
https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf
(accessed Jan 20)

111. Serianu, (2017) Nigeria Cyber Security Report 2017 – Demystifying Africa's Cyber Security Poverty Line.
Kenya: *Author.* P49 (online)
https://www.serianu.com/downloads/NigeriaCyberSecurityReport2017.pdf
(accessed Jan 20)

112. Symantec (2016). Cyber Security Trends Report Africa.
USA: *Author.* pp81-82 (online)
Available from: **https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf** (accessed Jan 20 and 21)

113. Symantec (2016). Cyber Security Trends Report Africa.
USA: *Author.* pp81-82 (online)
Available from: **https://thegfce.org/wp-content/uploads/2020/06/CybersecuritytrendsreportAfrica-en-2.pdf** (accessed Jan 20 and 21)

114. Global Cyber Security Capacity Centre (2021). Nigeria (GCSCC) 2019 – not yet published.
Oxford: *Author,* 2016,
https://gcscc.web.ox.ac.uk/cmm-reviews
(accessed Mar 2020)

115. National Cyber Security Index.
Estonia: *e-Governance Academy,* (online)
https://ncsi.ega.ee/ncsi-index/
(accessed Feb 21)