

Kenya



CMAGE
Cyber Security Maturity Assessment Global Ecosystem

Kenya Report

Maturity Model Assessment

2021

Report Structure

This document begins with a Highlight Report setting out key observations. This is followed by an introduction to CREST maturity model's structure and an explanation of the assessment methodology used in the research. Five subsequent chapters contain detailed observations, one relating to each of the five dimensions of the Cyber security Maturity Assessment of the Global Ecosystem (CMAGE).

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

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

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

The report contains six appendices:

Appendix A Glossary

Appendix B Summary of Maturity Level Definitions

Appendix C Professional Certifications & Member Organisations

Appendix D Country Context

Appendix E Bibliography

Appendix F Endnotes

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

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

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



Navigation Key



Move back
a page



Move forward
a page

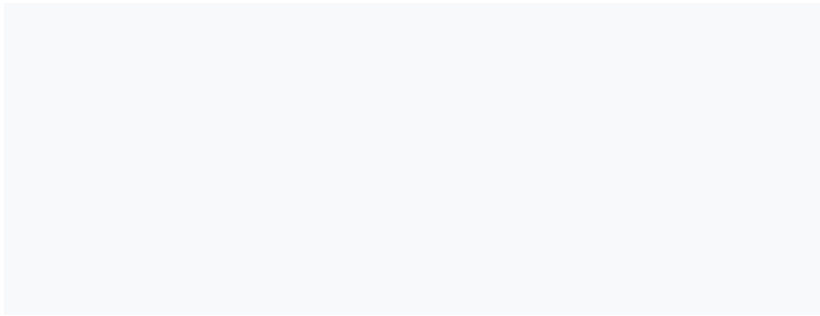
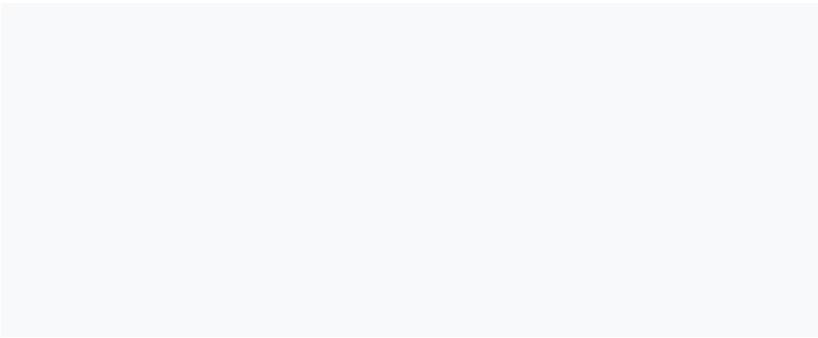
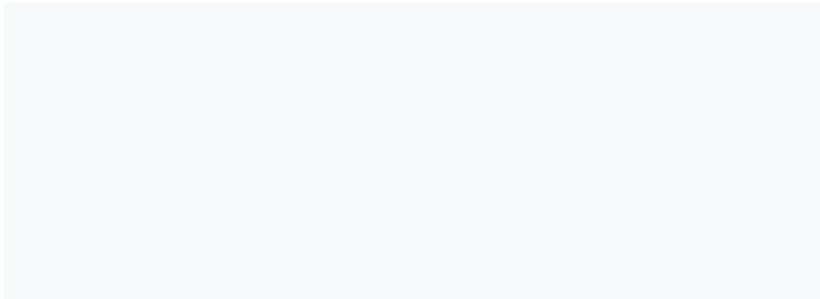


Return to
contents page



Move back to
previously
viewed page

Contents



Foreword from Ian Glover, President, CREST International

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

At the organisational level, the cyber security ecosystem comprises:

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

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

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

The relational database containing the CMAGE model has helped facilitate consistent application of the assessment, allowing for ease of update and 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 with a shared interest in improving Kenya's overall cyber security posture.

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

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



Ian Glover
President
CREST International



Highlights Report

Background

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

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

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

It is also a benchmark that allows relatively quick and easy re-assessments over time 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. Improvements in one part of the ecosystem will bring benefits to other areas as well.

Maturity Model Assessment Summary

Overall Uganda Ecosystem

Maturity Level 2

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

Kenya 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 Kenya's cyber security ecosystem is based upon the assessed maturity of five constituent Dimensions:

Dimensions and Indicators

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

Qualitative Assessments  **1-4**

Qualitative Assessments  **5**

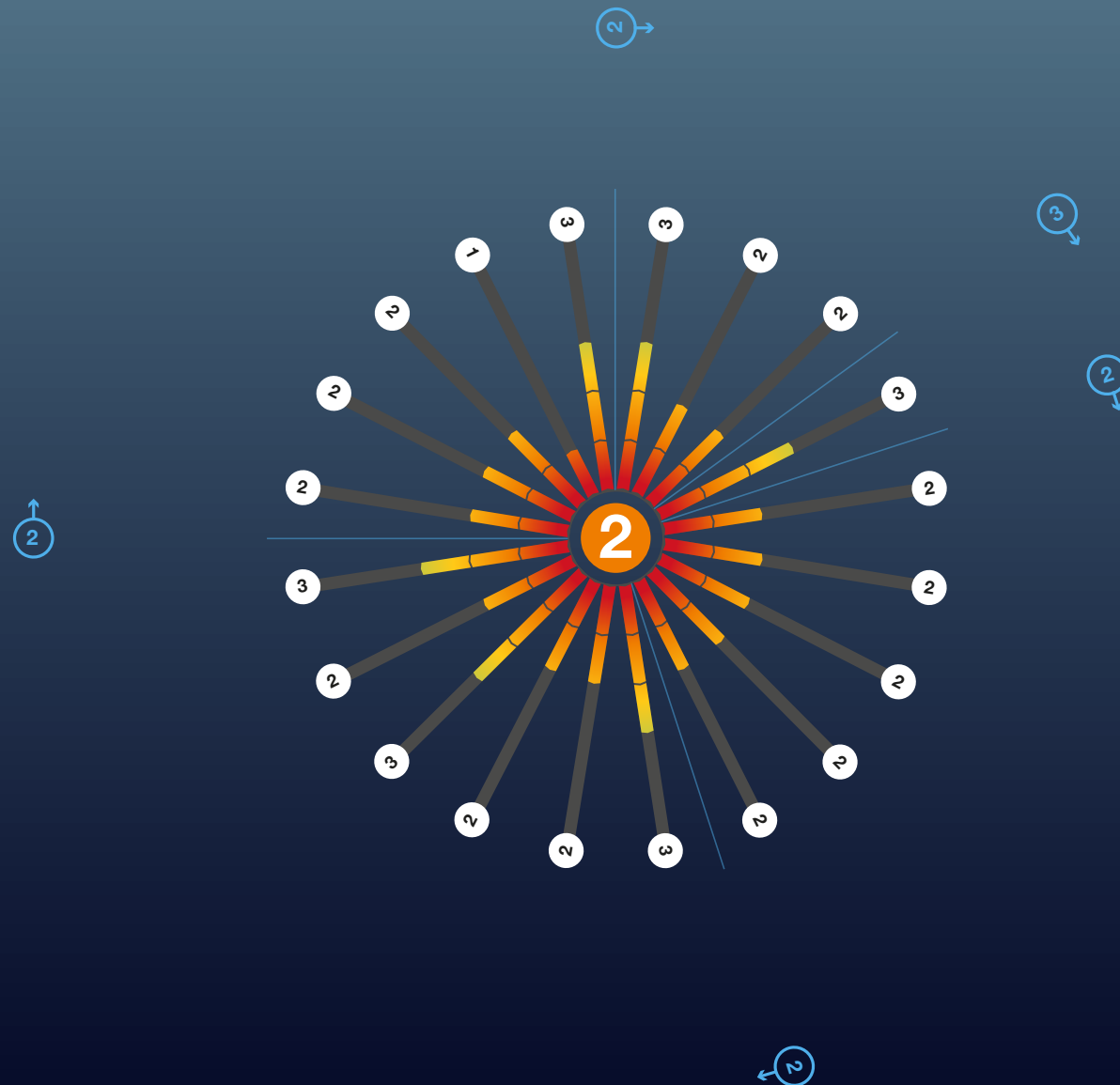
Maturity Scores

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

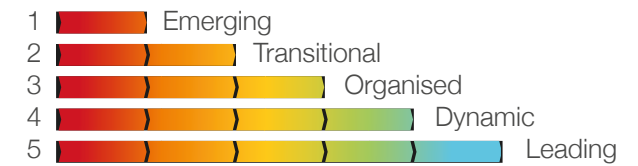
RED	Level 1
AMBER	Level 2
YELLOW	Level 3
GREEN	Level 4
BLUE	Level 5

Highlights Report

Summary of Observations (continued)



Maturity Levels



Summary Assessment

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

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

Kenya's 2014 National Cybersecurity Strategy is a solid foundation on which the country can build its cyber security policies and capabilities. The four headline goals listed in the strategy – enhancing the nation's cybersecurity posture, building national capability, fostering information sharing and collaboration, and providing national leadership – are the key cyber security challenges faced by most countries.

At the time, the self-assessment published alongside the strategy suggested the country was on the lowest tier of progress in respect of most evaluation areas. In the intervening years, headway has been made across a broad front, but implementation is probably not as far forward as might have been anticipated.

But the 2018 Computer Misuse & Cyber Crimes Act, the 2019 Data Protection Act and the Central Bank of Kenya's (CBK) guidelines on cyber security best practice are all positive signs that Kenya is moving in the right direction.

Indeed, guidelines from the **Central Bank of Kenya (CBK) and the Sacco Societies Regulatory Authority (SASRA)**, (the regulatory body charged with regulating deposit-taking Sacco Societies (Savings and Credit Cooperatives Societies)), are the foundations upon which an assurance scheme can be built for Kenya's financial sector.

The national cyber security focal point is the **National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC)**. This centre sits within the Communications Authority of Kenya. Its role was significantly strengthened by the 2018 Computer Misuse & Cyber Crimes Act.

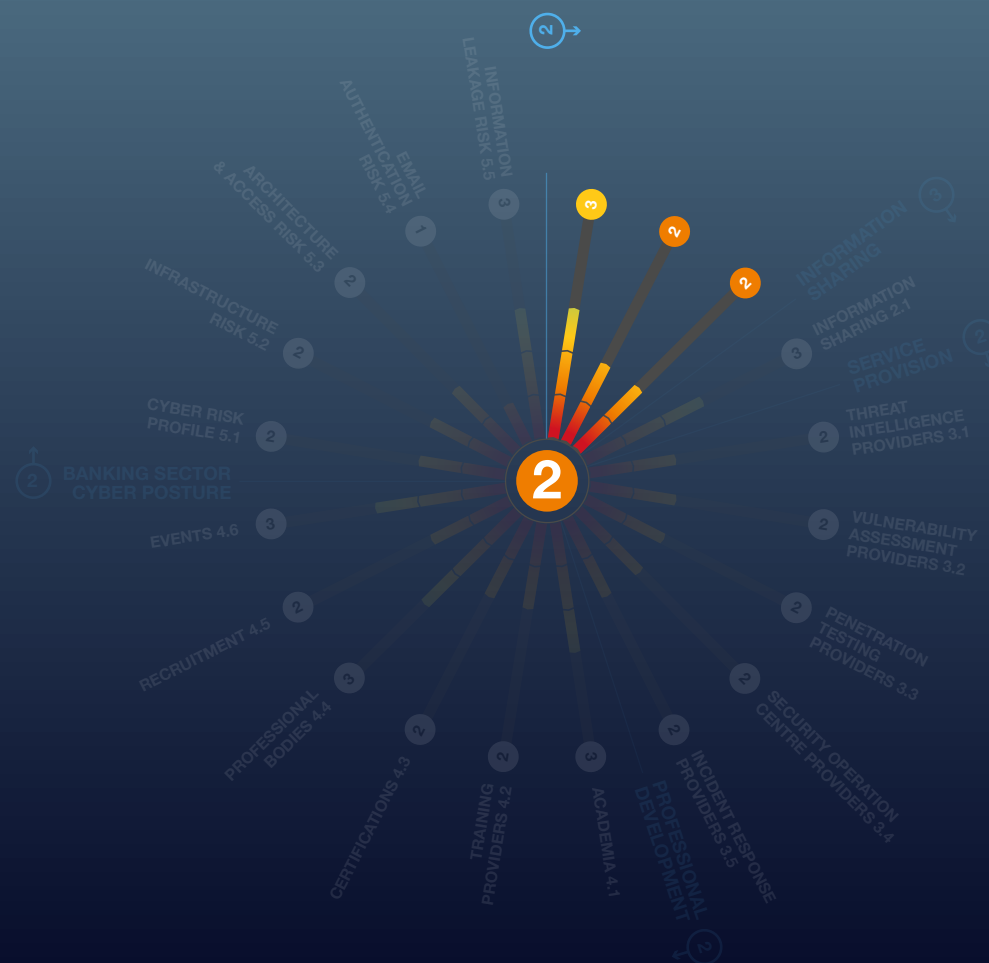
The Cyber Crime Unit and Banking Fraud Investigation Unit have both been recently established within the National Police Service (NPS). They provide the law enforcement response to cybercrime that complements the work of KE-CIRT/CC in providing the technical response.

Utilising good practice from other countries will help to speed the development and effectiveness of these law enforcement units. An intervention programme to divert talented youngsters away from cybercrime would also help.

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 2



Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

As well the national focal point for cyber security, KE-CIRT/CC is also the national CERT. It has well-established regional and international links, with membership of the global forum, FIRST, and also Africa CERT. Kenya also benefits from sector-specific CERTs, covering the technology services and education sectors.

KE-CIRT/CC's partnership with the Central Bank of Kenya bodes well for addressing cyber risks and incidents in the financial sector. There is also anecdotal evidence of informal banking sector information sharing via the Kenya Bankers Association. **Overall, the provision of CERT services in Kenya is very encouraging.**

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.



Twelve locally based companies also offer such services, but their quality could not be assessed.



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

Overall

There is a healthy mix of local, regional and international providers of cyber security services across all five disciplines examined. With some stimulus and focussed investment, Kenya 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

While many of Kenya's universities and colleges offer computer science degrees - some with a small element of cyber security content - very few offer specific cyber security courses.

A first-class cyber security industry needs to be underpinned by an expansion in cyber security education. By utilising international good practice, Kenya could relatively quickly build upon existing computer science and ICT courses to support creation of more specific cyber security courses and qualifications.

With a couple of notable exceptions, there is little evidence of independent academic research.

KE-CIRT/CC and private sector research appear to fill the void.

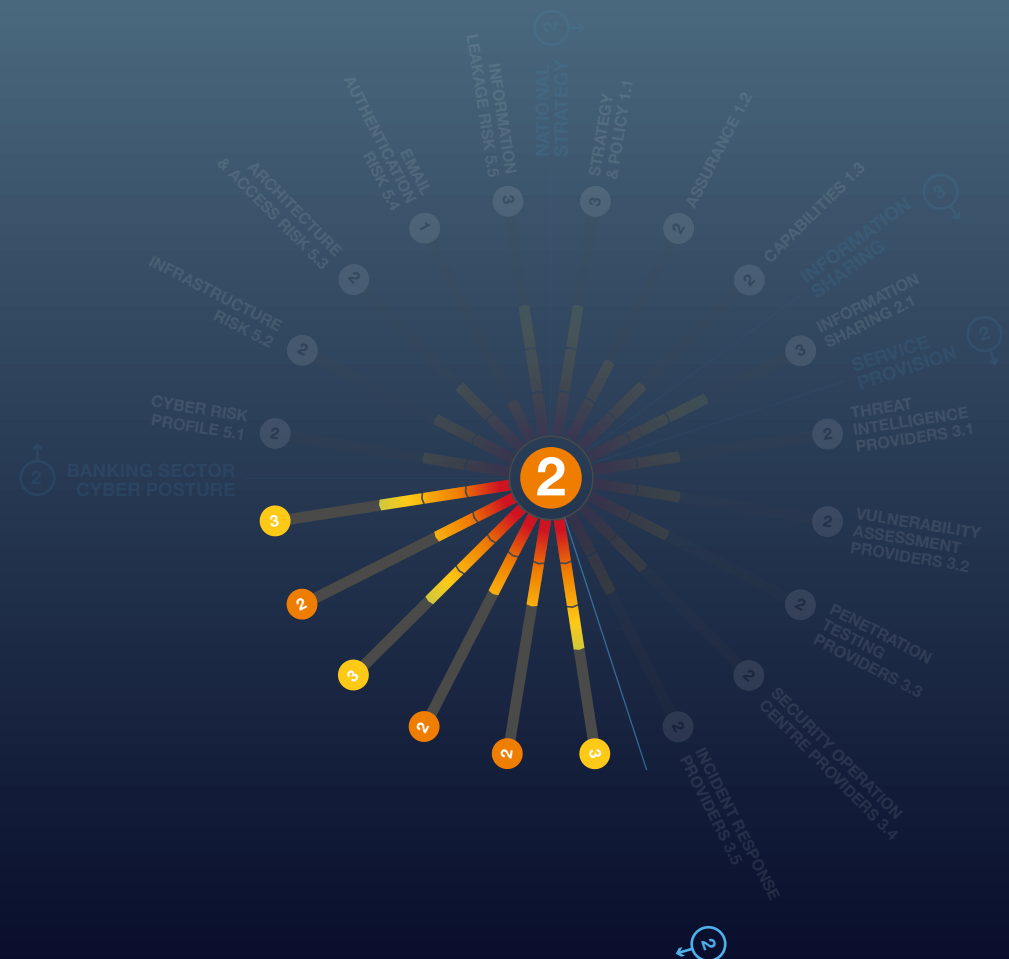
There are opportunities for further development of an academic research capability in Kenya, increasing the country's capacity for forward thinking in this important field.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 2



Highlights Report

Key Observations - Dimension 4 (continued)



There is a good blend of in-country and international cyber security training. The use of bootcamps and other outreach techniques are improving demand for cyber security training.



A greater level of local provision would expand opportunities for people to train at affordable cost and help develop the professional cyber security community.



With a couple of notable exceptions, there is little evidence of independent academic research.



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



There is evidence that take-up of certifications is improving, potentially thanks to links between some certification providers and academic institutions. Hopefully, this will encourage and nurture talent.



It is likely that cost is prohibitive to many, but once individuals and companies see the benefits of professional certification, these cost issues may be overcome.



As part of the project's Stage 2, 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 some international professional bodies operating in Kenya, but this needs to be extended and strengthened if it is to support national aspirations to grow the number of cyber security professionals.



On a positive note, SheHacks and Women in Cyber Security (WiCyS) both operate in Kenya. The Kenyan Cyber Security and Forensics Association (KCSFA) also appears to be an active community.

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

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

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

Continued on next page...

Dimension 5

Banking Sector Cyber Security Posture

Maturity Level 2



Highlights Report

Key Observation - Dimension 5 (continued)

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

Without explicit permission, any external observations undertaken 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 carried out on internet-connected portions of an organisation's infrastructure.

Using this approach, accessible, measurable indicators were used to gain implicit insights into many key risk areas. Overall, passive external assessments were carried out on the public-facing IT infrastructure of a sample of 60 financial institutions. For obvious reasons, all results have been anonymised.

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

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

30%

Overall, **30%** were awarded a risk rating of 'Very High' or 'High', indicating Maturity Level 2 for Risk Profile.

11%

11% had evidence of critical vulnerabilities on their infrastructure.

30%

30% appeared to be carrying non-critical vulnerabilities, indicating Maturity Level 2 for Infrastructure Vulnerability Risk.

0%

In respect of Architecture and Access Risk, none of the sample appeared to have any remote access ports open on the public-facing infrastructure.

30%

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

40%

Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **40%** of the sample.

75%

Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **75%** of the sample. Our research indicates Maturity Level 1 for Email Authentication Risk.

46%

In **46%** 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 Kenya'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 Kenya's cyber security ecosystem**.

3

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

4

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

5

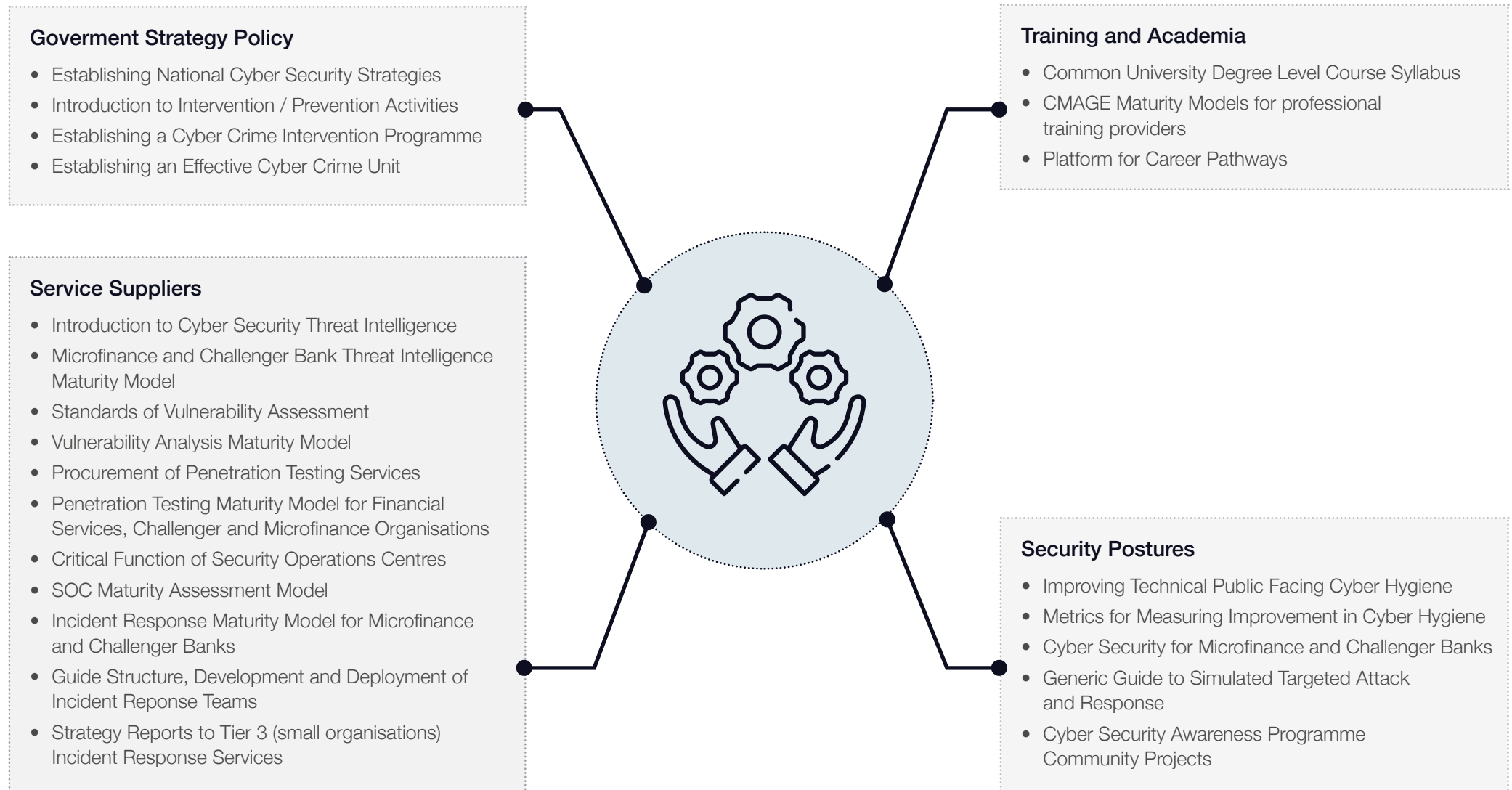
The library will be **available throughout 2021** and is shown on the next page.

6

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

Highlights Report

2021 Good Practices Guides and Tools





Introduction

Introduction

Background

This report seeks to provide a benchmarked assessment of the maturity of Kenya'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) programme¹** 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 market². 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. **Except for the section of this report dealing with the banking sector cyber security posture,** all evidence used in preparing this report has been gathered using open-source methods, including internet-based research supplemented - where needed for clarity - by email and telephone enquiries. The research has subsequently been presented to audiences of local and international subject matter experts for feedback and validation.

9. In terms of banking sector cyber security posture, CREST worked with **Orpheus Cyber³**, a leading cyber threat intelligence service provider, to carry out a passive (non-intrusive) external assessment of the public-facing IT infrastructure from a sample of the country's financial institutions.

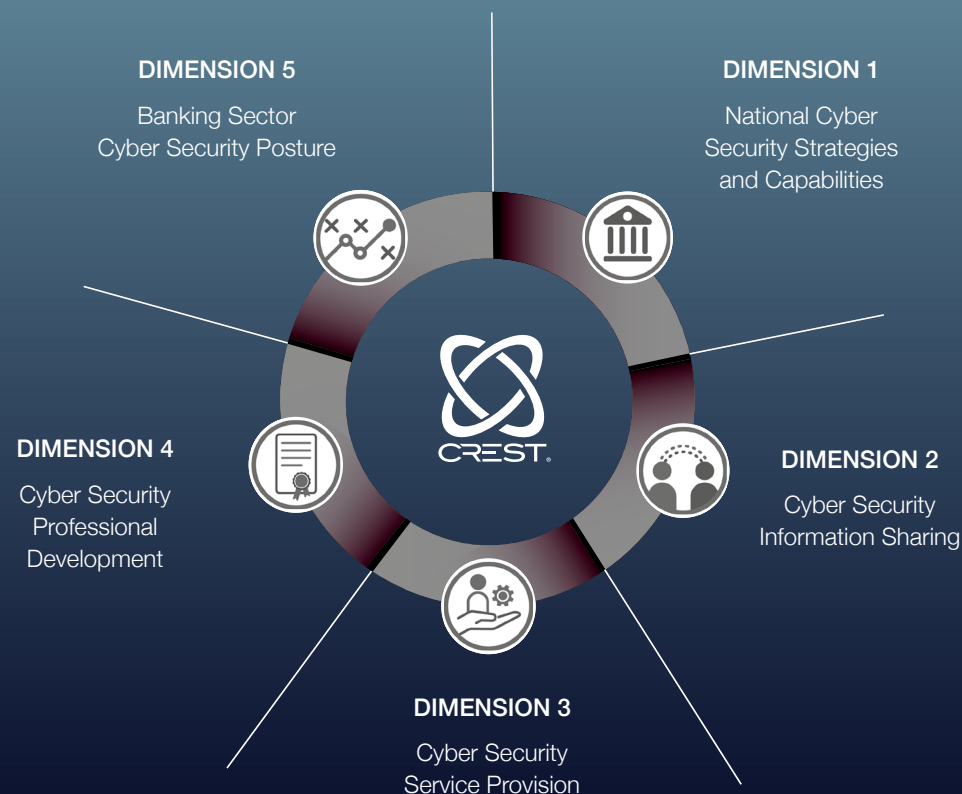
The assessments were carried out by computer, to common standards, allowing for comparisons, benchmarking and periodic automated reassessments, if required. CREST believes this methodology is a global first - the first time that rapid, automated mass assessment has been used as part of cyber security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

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

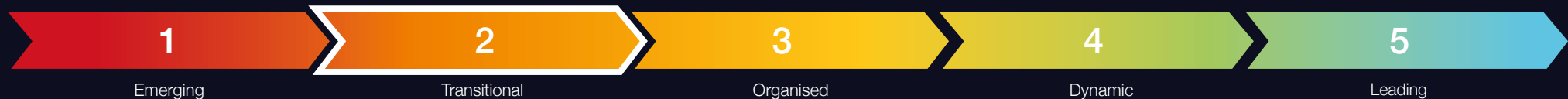


Dimension 1

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.

Without a national strategy, the public and private sectors would have no guidance or framework to base their own cyber security policies on. Ultimately, a lack of national cyber security strategy undermines economic growth.

Examining a nation's cyber security strategy provides good insight into its willingness to implement cyber security measures and to tackle cybercrime. A national strategy sets the standards for all other sectors to follow.

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

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

The following is a summary of the various National authoritative bodies that have responsibility towards information and communication technology and cyber security.

18. The Ministry of Information, Communications and Technology (MoICT)⁴ of Kenya holds responsibility for formulating, administering, managing and developing information, broadcasting and communication policy. The MoICT produced a National Cyber Security Strategy (2014)⁵, National ICT Masterplan (2014-2017)⁶, National ICT Policy (2016)⁷ and the latest National ICT Policy (2019)⁸.

National Cyber Security Strategy & Capabilities

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

19. **In 2016 the MoICT was split into two state departments: Broadcasting and Telecommunications and ICT and Innovation⁹.**

The Information and Communications Technology Authority (ICT-A)¹⁰ of Kenya sits under the latter.

20. The ICT-A was established in 2013, tasked with rationalising and streamlining government ICT functions. Its mandate is to enforce ICT standards in government and promote ICT literacy, capacity, innovation, and enterprise¹¹. The ICT-A recently published a Strategic Plan 2020-2040, the most recent plan or policy document found during CREST's research.

The plan states some of its key achievements from the Strategic Plan 2013-2018 as implementing a National Cyber Security Policy and National ICT Masterplan¹². The 2020-2040 plan covers cyber security in Strategic Objective 1¹³.

21. The Communications Authority of Kenya¹⁴ also sits under the MoICT¹⁵, and is the regulatory authority for communications in Kenya. Established by the Kenya Information and Communications Act of 1998, it is responsible for developing the information and communications sectors, including broadcasting, telecommunications, multimedia, electronic commerce, postal and courier services¹⁶.

The 1998 Act, amended by the Kenya Information and Communications (Amendment) Act 2013, gives the Communications Authority the power to work as an independent regulator, independent of political, commercial or government interests¹⁷. A search of its website for cybersecurity information resulted in links to multiple quarterly Cyber Security Sector Statistic Reports and some cyber security articles¹⁸. (See **Appendix D (Country Context)** for more detail). The Communications Authority is the parent body of the National Kenya Computer Incident Response Team Coordination Centre (KE-CIRT/CC)¹⁹.

Overall Assessment

22. The 2014 Kenyan National Cyber Security Strategy is a solid foundation upon which comprehensive cyber security policies and capabilities can be built. Progress has been made across a broad front, but implementation is probably not as far forward as would have been expected.

Development Approach

23. Enhancement to law enforcement and cyber defence capabilities should be considered a priority, particularly better reporting processes for cybercrime and better media coverage of successful prosecutions. Enlarging the pool of cyber talent available to the government and private sector through investment in education is also key.

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.

24. CREST's research sought information on publicly available strategic level policy and legislation relating to national cyber/information security, how up to date it is, and which agencies were empowered to uphold it.
25. The ICT-Authority Strategic Plan of 2020-2040 includes cyberterrorism as a threat in its SWOT analysis (on page 17). In Chapter 4, covering Strategic Pillars and Objectives, Strategic Objective 1 is to improve and maintain secure, reliable and accessible digital connectivity. Strategy 1 of this objective has various outputs, outcomes, and Key Performance Indicators (KPIs), including²⁰:
 - An online portal for cyber security reporting
 - An operationalised cyber security bill
 - A national certification and training centre
 - A review of information security and cyber security policies, published standards, methods and guidelines
 - Alignment of cyber security guidance to international best practices, and
 - A KPI of increasing the number of cyber security threats proactively reported to MCDAs²¹.
26. The MoICT's National ICT Policy (2019)²² is another recent publication, with objectives including:
 - Establish a cybersecurity legal framework
 - Support development of secure new technologies
 - Develop information security standards for the ICT sector
 - Create a culture of security awareness
 - Efficiently mitigate cyber threats
 - Develop protective measure for vulnerable groups, and
 - Develop defensive and offensive capabilities.
27. The Data Protection Act (2019) came into force in November 2019 and builds upon the 2018 Privacy and Data Protection Policy. The legislation borrows heavily from the EU's GDPR regulations from 2016 and establishes a Kenyan Data Protection Commissioner²³.
28. **The Computer Misuse and Cyber Crime Act 2018 provides for offences relating to computer systems.** It enables timely and effective detection, prohibition, prevention, response, investigation and prosecution of computer and cybercrimes. The Act also seeks to facilitate international co-operation in dealing with computer and cybercrime matters²⁴.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy (continued)



Assessment – Maturity Level 3

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

29. **The Kenyan National ICT Masterplan 2014 – 2017²⁵** outlines objectives and capacity-building strategies. Objective 6, Strategy S2 is to develop, implement and institutionalise a cyber security management framework, including implementation of a Cyber Security Master Plan. Objective 7, Strategy S3 is to develop a cyber security policy²⁶. In Chapter 6.6.3 (pp96-97), Legal Gaps and Recommendations, it recommends fast-track development of cybersecurity law²⁷. The Computer Misuse and Cyber Crime Act 2018 could be seen to fulfil this recommendation.

30. The 2014 National Cyber Security Strategy acknowledges the increasing trends of cyber security and threat from cybercrime, stating cybersecurity as a national priority.

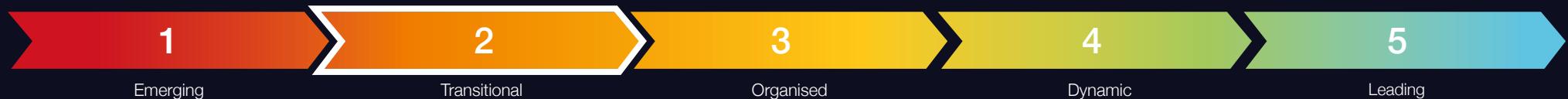
It has four specific goals:

- To enhance the nation's cybersecurity posture
- To build national capability
- To foster information sharing and collaboration, and
- To provide national leadership²⁸.

31. **The Information and Communication Act 1998 authorised establishment of the Communications Commission of Kenya²⁹**. In the 2013 amendment of the Act, cyber security as a term is added and Para 2c defines cyber security as: “a means of collecting technical tools, policies, security concepts, guidelines, risk management, adapting best practices, assurance and technologies that can be used to protect the cyber environment”³⁰. Para 24c of the same amendment Act, covering amendment of the original Act's section 83C, states that the Authority may make regulations with respect to cyber security³¹.

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



Assessment – Maturity Level 2

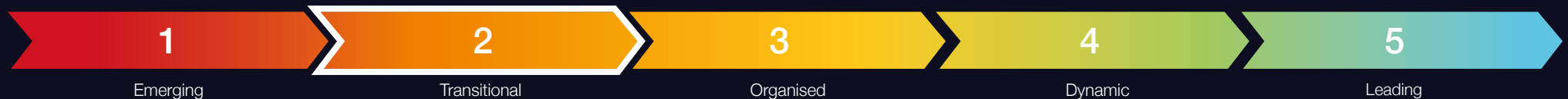
Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.

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

32. Research focused on looking for publicly available policies and laws which support and uphold financial ethics, integrity and cyber security.
33. **The Kenya Ministry of Finance and Central Bank are both members of the Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI)³².** The MEFMI is focused on macro-economic management, financial sector management, sovereign debt management and a fellow's development programme. It has conducted some cyber-related courses, including Cyber Security in the Financial Sector in 2020, and Cyber Financial Crimes in 2019³³, providing influence on the subject to members.
34. The Kenya Bankers Association (KBA), formed in 1962, aims to be the national voice of banking through thought leadership anchored in research and analysis³⁴. The KBA has an extensive research library on its website. During CREST's research, no publicly available evidence that the KBA provides a cyber security threats/vulnerabilities information sharing function was found. However, a 2019 article in Kenyan Wall Street commented that cybercrime and cyber security were being discussed by the KBA and banks³⁵.
35. The Central Bank of Kenya (CBK) published Guidance Notes on Cybersecurity for the Banking Sector in 2017³⁶. This was followed by Guidelines on Cybersecurity for Payment Service Providers in 2019³⁷. Both guidelines providing thorough guidance for Board and other management roles and functions within the banking sector and among payment service providers. Both sets of guidelines also cover training and awareness, and reporting of cyber security incidents.
36. According to the Serianu SACCO Cybersecurity report (2018), the SACCO Societies Regulatory Authority (SASRA)³⁸ has produced guidelines on cyber security risk management which set the minimum standards that deposit taking SACCOs should adopt to develop effective cyber security governance and risk management frameworks³⁹.
37. The only related document found on SASRA's website during CREST's research was a Guideline on Risk Management for Deposit Taking SACCO Societies (2015). Chapter 5 covers ICT risk management, mentioning information security and the risks of denial-of-service attacks and malware. But the term 'cyber security' is not actually mentioned in this⁴⁰.

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.

37. **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 what and where cybercrime was being reported, and what official action was being reported to combat it.

38. **In an article dated 2 Jan 2021 from the Communication Authority (CA)⁴¹,** it records (according to the CA's quarterly sector statistics report covering July-September 2020), a sharp increase in cyber threats during that period, with 35.1 million incidents detected, representing a 152.9% jump.

The article attributes the increased number of cyber-attacks to the fact that more people are working from home and buying online because of the COVID-19 pandemic. The article states that during this period, there were increases in online child abuse (1.7%), online abuse (36.2%), and online fraud (27.4%). **The article said in response to these incidences, 21,785 advisories from the CA were issued to various stakeholders⁴².**

39. The National Police Service (NPS)⁴³ Strategic Plan (2013/14-2017/18) describes the application of ICT to policing work as one of its strategic priorities. It recognises the need for continuous training for police in areas such as cyber, and that cybercrime will continue to influence Kenya both culturally and in terms of 'Build Your Success' Model⁴⁴. Strategic Objective 5 describes modernisation of the NPS. Proposed activities include constructing and equipping a forensic laboratory, and establishing a specialised unit to deal with cybercrime⁴⁵.

40. **The Digital Forensics Laboratory (DFL)⁴⁶** sits in the Forensic Section of the Directorate of Criminal Investigations⁴⁷, one of the services of the National Police Service. The DFL has several sub-units, including computer forensics, malware analysis and a Computer Incident Response Team (CIRT).

The CIRT's key responsibilities include:

- Investigating and analysing security breaches and intrusion incidents
- Managing internal communications and updates regarding incidents
- Mitigating incidents
- Recommending technology, policy and training changes, and
- Responding to attacks⁴⁸.

The KE-CSIRT/CC website states that KE-CSIRT/CC collaborates with the law enforcement CIRT⁴⁹.

41. **A Banking Fraud Investigation Unit sits within the Directorate of Criminal Investigations.** Its role is to investigate fraud complaints from commercial banks and other financial institutions, advise the financial industry on fraud prevention and detection strategies and develop greater public awareness of common types of frauds⁵⁰.



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.

42. **There is no commercial advantage to be gained in not sharing information.**
Open publication of academic research and sector-specific information exchanges are both example mechanisms for sharing information on cyber security risks, threats and vulnerabilities. There is not much evidence of either of these mechanisms being currently well-established in Kenya.
43. Information sharing enables the spread of best practice. **The research focused on looking for expert groups such as Computer Emergency Response Teams (CERTs)** - teams of information/cyber security experts responsible for protection against, detection, and response to cyber security incidents.
They provide cyber security services, as well as running cyber security awareness campaigns and 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 to enable greater sharing of best practice.
44. CREST's 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

45. Having two sector-specific CERTs, covering technology and academia, alongside the Kenyan national CERT, is hugely encouraging. The national CERT's international links via FIRST and Africa CERT are also encouraging, helping with both benchmarking and information sharing.

Development Approach

46. Establishing a CERT focused on the financial sector would help strengthen information sharing between banks and other financial institutions and support regulator's aims.

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.

47. **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)

48. The following is a summary of the different CERTS/CIRTS and other information sharing organisations found during CREST's research.

49. **The National Computer Security Incident Response Team Coordination Centre (KE-CIRT/CC)**⁵¹ is parented by the Communications Authority of Kenya. KE-CIIRT/CC is Kenya's national point of contact on cyber security matters, with responsibility for national coordination of cyber security issues and 24/7 response to cyber threats.

50. KE-CSIRT/CC's website states that it collaborates with other national CIRTS and CERTS such as the education sector CIRT, the law enforcement CIRT, the banking sector CIRT and the Internet service/telecoms provider sector CIRT. Internationally, it collaborates with the US-CERT and Japanese CERT (JP-CERT)⁵². It is also a member of both Africa CERT⁵³ and the Forum of Incident Response and Security Teams (FIRST)⁵⁴. So, it enjoys strong national, regional, and international links and influence. These regional and international links mean KE-CSIRT/CC meets Level 2 of the ENISA CSIRT Maturity Model⁵⁵.

Cyber Security Information Sharing

Indicator 2.1 Computer Emergency Response Teams (CERTs) (continued)



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.

51. **The Kenya Education Network CERT (KENET-CERT) is a Cybersecurity Emergency Response Team and Co-ordination Centre operated by the National Research and Education Network of Kenya.** It works closely with KE-CIRT/CC as a sector CIRT for academic institutions⁵⁶.
52. The law enforcement CIRT is operated by the Digital Forensics Laboratory of the Directorate of Criminal Investigations of the National Police Service (NPS)⁵⁷.
53. The Technology Service Providers of Kenya (TESPOK) is a non-profit organisation representing technology service providers' interests in Kenya⁵⁸. It is the parent body for the industry Computer Security and Incident Response Team (TESPOK-iCSIRT) which works closely with the information security community to detect, report and investigate incidents that threaten the security of TESPOK members' information systems⁵⁹. The iCSIRT is also a member of Africa CERT⁶⁰.
54. **The ICT-Authority of Kenya is a member of the Cybersecurity Alliance for Mutual Progress (CAMP) Initiative⁶¹.** CAMP serves as a network platform to lift the overall level of cybersecurity of its 59 members (from 45 countries). CAMP launched in July 2016, it is a network of an interactive international community, sharing information on cybersecurity issues to track the latest cybersecurity trends and strategic national policies. It responds in a collective manner on cyber issues to enhance political leveraging power at global stage⁶².
55. The Ministry of Higher Education⁶³, Science and Technology of Kenya is a member of IST-Africa⁶⁴ which is supported by the European Commission (EC) and African Union Commission (AUC). IST-Africa is a strategic collaboration between IIMC (Ireland) and Ministries and national councils responsible for innovation, science and technology adoption, policy, and research in 18 African countries.
It facilitates and supports:
 - Strategic engagement with Africa focused on international research, innovation, and policy cooperation
 - knowledge sharing, capacity building and skills transfer between IST-Africa partner countries and more⁶⁵.
 Its website includes the National ICT Research Capacity and Priorities for Cooperation for Kenya, which lists some of the universities and their areas of ICT-related research⁶⁶.

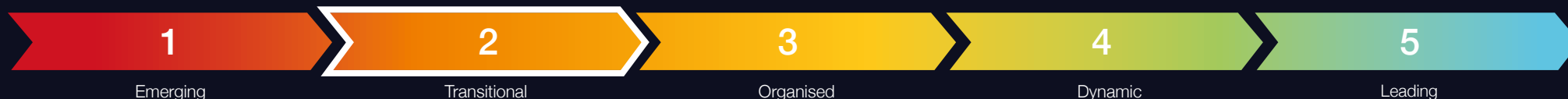


Dimension 3

Cyber Security
Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 2*



Provision of professional cyber security service is essential in any nation to protect individual organisations and, by default, the national economy.

56. Service providers form part of the front line in the fight against cybercrime. CREST's research into how cyber security services are currently provided in Kenya 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.

57. Company office location and customer reach were also recorded. Were they were local companies, registered and only based in Kenya? CREST asked 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 large international organisations, with multiple global office locations which may be located in-country? If not, can they provide services into Kenya 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.

58. Several 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 purchase of other technology products, such as software, were excluded from the research.

Overall Assessment

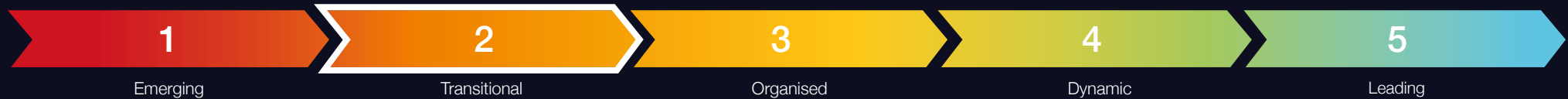
59. Across the board, Kenya is rated at Level 2 for all categories of service provision. Currently three CREST international member companies have local offices, and a further eight companies offer a variety of in-country services. While the market is starting to mature, it is not yet fully established.

Development Approach

60. Backing from government and regulators should lead to the adoption of benchmarked standards. This, in turn, should lead to demand-led growth in the number of service providers, encourage investment and maturing of the marketplace.

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers



Assessment – Maturity Level 2

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

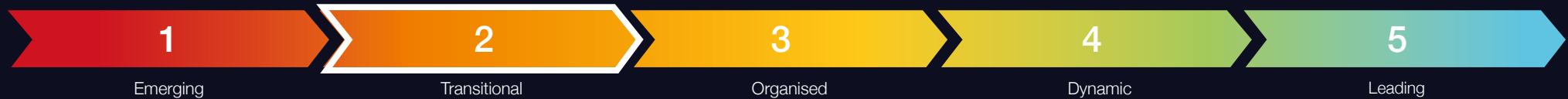
Cyber Threat Intelligence

61. Cyber Threat Intelligence (CTI) is information about current and future cyber threats and actors that adversely affect a nation's or individual organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks⁶⁷. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark-web sources.
62. The research looked for companies providing cyber threat intelligence services to organisations in Kenya and where these services were provided from. For the purposes of a robust cyber security environment, the ideal scenario is a host of Threat Intelligence service providers based in Kenya. Evidence of quality, though any accreditations or partnerships, was also sought.
63. **There are 16 companies offering Cyber Threat Intelligence Services into Kenya. Seven operate in-country, of which three are international CREST-accredited companies.** A further seven CREST-accredited international companies offer their services from another international location. **One international organisation providing support into Kenya is the Forum of Incident Response Teams (FIRST)⁶⁸.**

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	3	7
Regional	0	0	0
International	2	7	9
Total	6	10	16

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment Providers



Assessment – Maturity Level 2

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

Vulnerability Assessment (VA)

64. Vulnerability Assessment (VA) is defined by CREST as: “the examination of an information system or product to determine the adequacy of security measures. A vulnerability assessment will also identify security deficiencies and predict the effectiveness of the proposed security measures. It will also confirm the adequacy of such measures after implementation⁶⁹”. As with threat intelligence, research focused on looking for companies which provide VA services in Uganda, ideally based in the country.

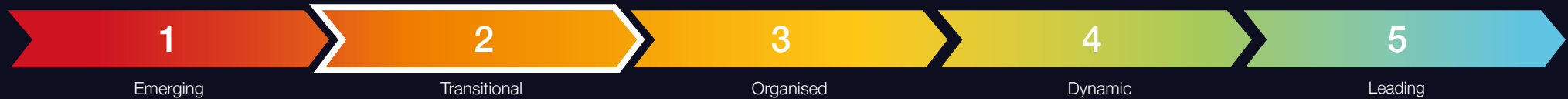
Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	12	3	15
Regional	2	0	2
International	1	26	27
Total	15	29	44

65. CREST’s research found **44 companies providing Vulnerability Assessment (VA) services into Kenya**. **Many companies operate in-country; three are CREST-accredited international organisations.**



Cyber Security Service Provision

Indicator 3.3 Penetration Testing Providers



Assessment – Maturity Level 2

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

Penetration Testing

66. 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 vulnerabilities⁷⁰."*
67. CREST's research found significantly more companies providing penetration testing than any other cyber security service, though many service providers provide more than one cyber security service. In assessing cyber industry maturity, efforts focused on looking for service providers based in Kenya.

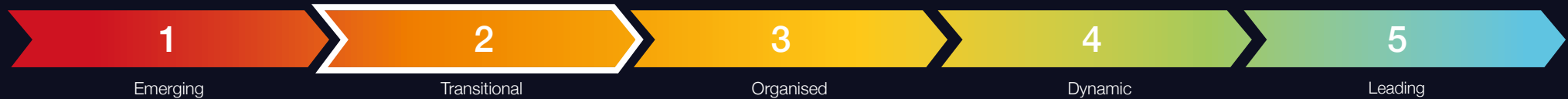
Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	10	3	13
Regional	1	2	3
International	2	76	78
Total	13	81	94

68. The research identified **94 companies providing Penetration Testing services into Kenya**. Of the 13 based in-country, **three are CREST-accredited international organisations**. There are a further **78 CREST-accredited organisations offering services into Kenya**, from either a regional or international location.



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

69. CREST provides a detailed definition of Security Operations Centres:

“An Information Security Operations Centre (SOC) is a facility where enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. Depending on the nature of the SOC, organisations may offer a variety of services including monitoring, detection, threat hunting, log analysis, incident management, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance. A range of response options may be available, from telephone or email triage through to onsite assistance as required. Where such services are not available within the organisation, the SOC will know where and how to procure appropriate services from third parties⁷¹.”

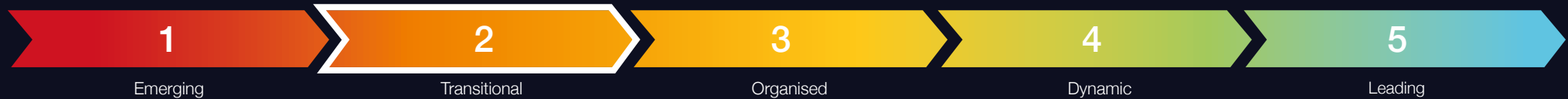
70. Security Operations Centres are specialised, so provision of this service is only likely to come from well-established companies, operating in an active cyber security industry market.

71. There are **15 companies that can provide Security Operations Centre services into Kenya. Six are based in-country and nine in regional or international offices.** The latter nine are all CREST-accredited organisations.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	6	0	6
Regional	0	1	1
International	0	8	8
Total	6	9	15

Cyber Security Service Provision

Indicator 3.5 Incident Response Providers



Assessment – Maturity Level 2

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

Incident Response Providers

72. 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 malfunction⁷².”

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

74. There are **41 organisations providing Incident Response Services into Kenya**. Three CREST-accredited international organisations have offices in Kenya, **the other 28 CREST-accredited organisations are either based in regional or international offices**, and it is unknown how often their services are called upon.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	9	3	12
Regional	0	1	1
International	1	27	28
Total	10	32	41

75. **Of the four CIRTs operating in-country, three offer an incident response service to member organisations and are included in the in-country numbers.** The TESPOK-iCSIRT provides incident response services to technology service providers, KENET-CERT to the education sector, and KE-CIRT/CC provides national incident response for all citizens and other organisations.

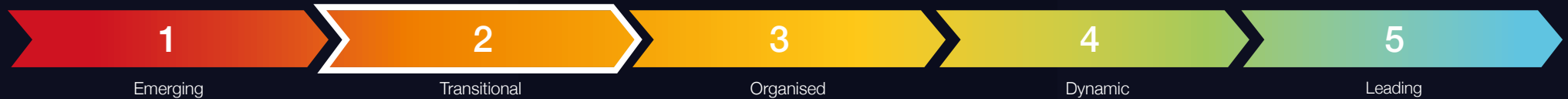


Dimension 4

Cyber Security
Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2*



76. Education and professional development are critical in providing students with skills and knowledge to thrive in the modern workplace. Without ICT and cyber security being taught in the 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 this threat, a country needs a vibrant cyber security industry with well-trained professionals.

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

78. CREST's research also looked at the most recent policy or commentary found regarding professional development. Below, and in **Appendix D**, is a snapshot of findings.

79. In the Information and Communications Technology Authority (ICT-A)'s Strategic Plan 2020-2040, Strategic Objective 3 describes creating a "*globally ethical and digitally competent workforce and citizenry for a digital economy*."

This strategic objective has sub-strategies with their own outputs, outcomes and KPIs relevant to this CMAGE⁷³, as follows:

Strategy 6: Develop and enhance training programs to empower professionals in the workplace and individuals with the digital skills necessary for improved productivity and inclusivity across all economic sectors.

Key Strategic Program/Initiative: Establish and enhance training programmes (the Digital Literacy Programme (DLP), the online youth employment programme (AJIRA), and the Presidential Digital Talent Program (PDTP)) to promote digital skills development for professionals in the workplace and individuals to enhance their competencies in performing basic and specialised task⁷⁴.

Strategy 7: Enhance strategic partnerships and collaborations to offer training in key strategic competencies, stimulating innovative thinking and improving performance for digital economy growth, in line with vision 2030.

Key Strategic Program/Initiative: Expand and enhance strategic partnerships and collaborations with training institutions, based on their competencies and capacity to support digital skills development at all skill levels⁷⁵.

Strategy 8: Enhance integration of 'soft skills' into the digital skills training and workplace.

Desired outcomes include: (1) Raising the profile of the ICT and digital technology sector and careers, and (2) Increased access to opportunities⁷⁶.

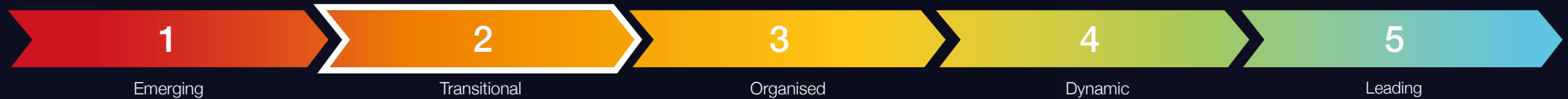
Strategy 9: Enhance access to technology and the digital skills needed to empower citizens to create, innovate and participate in a digital economy.

Desired outcomes include: (1) Reduce cyber security breaches and (2) Increase the number of ICT companies based in Kenya⁷⁷.

Strategy 10: Enhance policies and the legal framework to promote appropriate values and cultures for a successful digital economy⁷⁸.

Cyber Security Professional Development

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



All these strategies, desired outcomes and KPIs are positive signs that Kenya is willing - and actively making positive changes - to improve ICT capabilities, and to embrace the digital economy and its challenges, in terms of cyber threats and skill training for the population.

80. The Serianu Kenya 2018 - Cyber Security Skills Gap Report states Kenya needs at least 10,000 cyber security professionals to keep up with local sector demand. But each year, approximately 100 new personnel join the market. The report estimates that by 2023, going by the current rate of technology uptake, Kenya will need at least 50,000 cyber security professionals. The Serianu report summarises skills needed in three broad categories: understanding, attribution and deterrence⁷⁹.

Overall Assessment

81. A variety of cyber security-related courses, each focusing on a particular aspect of the discipline, are offered by a cross-section of higher education institutions. A diversity of courses and delivery formats also appear to be offered by training providers, but it is not immediately clear how many lead to recognised qualifications. Participation in professional bodies and events appears to be growing.

Development Approach

82. Partnering with universities and renowned institutions abroad could improve cyber security education opportunities. Investment in certifications would also improve matters.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education



Assessment – Maturity Level 3

Academia active in cyber security teaching and research. Significant local choice of cyber security degrees at BSc, MSc and PhD. Apprenticeship (or similar) programmes available.

Academia and Higher Education

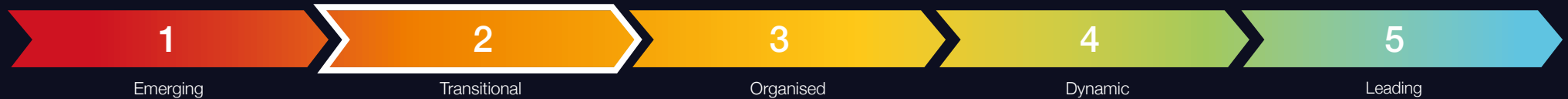
84. Higher education takes place after secondary schooling, usually in further education colleges or universities. It aims to equip people with the skills and qualifications needed in their future workplace or careers. Academia is the pursuit of research, higher level education and scholarship.
85. CREST's research sought to identify universities and colleges offering ICT or cyber security courses and modules, and the level of these courses – diploma, degree, masters, etc. The more students graduating with ICT or cyber-related degrees, potentially results in more people following an ICT-related career.
86. The table to the right shows approximate numbers of courses offered by the 29 universities and colleges researched. Information on courses provided was taken from the institutions' websites. Where information was offered, it was not all shown in the same level of detail, hence numbers are approximate. There is plenty of scope for increasing the number of cyber courses available to students.

	Diploma / Cert / Other	BA/ BSc	Pg Dip	MSc	PhD	Total
ICT Courses	0	6	0	5	1	12
Cyber Courses	12	5	0	0	0	17
Total	12	11	0	5	1	29

87. Of courses found, it was good to see a high proportion had cyber security content and that some of the courses were purely focused on cyber security. Of note is the Serianu-operated Africa Cyber Immersion Centre (ACIC)⁸⁰, which tailors a range of courses to corporate, university and high school level students.

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

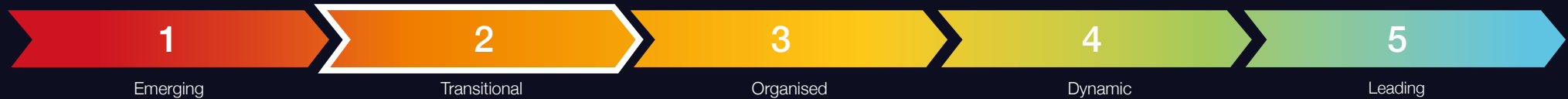
88. Training providers are qualified to provide training via an established course to clients in a particular subject matter area. CREST's research sought to identify the number of training providers, where they were located and what cyber courses they were providing.

89. **Twenty-seven training providers were identified during CREST's research.**

While the list of identified training providers appears to be reasonably healthy, several providers do not focus exclusively on cyber security. Only a few appear to offer in-country instructor-led training, and many courses appear to lack practical implementation. It is not immediately clear how many of the training courses lead to recognised certifications. Of note, Sentinel Africa offers undergraduate bursaries to support talented but less fortunate students via its Sentinel Talent Shield Program⁸¹, though at time of report writing this offer was closed.

Cyber Security Professional Development

Indicator 4.3 Professional Certifications



Assessment – Maturity Level 2

Some International Certification Bodies operate in country but take up is low. Some local institutions and professional associations in operation.

Professional Certifications

90. Professional certifications provide evidence of the holder's skills in that subject area at the time of certification. In the cyber security industry, there are a multitude of different certifications that can be attained, provided by a growing number of professional training providers. More detail of these training providers and the certifications they provide can be found in [Appendix C](#).

91. **Fifteen training providers offering professional certifications in Kenya were found during CREST's research.** Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres available in-country. Some certifications requiring practical exams offer this element online or through connection to a remote network, although some, e.g. CREST⁸², and Cisco⁸³ only offer exams at specific testing sites. From information gathered, indications are that take-up of certifications in Kenya is currently modest.

The ISACA⁸⁴ and (ISC)2⁸⁵ chapters in Kenya appear to be relatively active.

The most popular certifications appear to be CISA and CISM (both awarded by ISACA)⁸⁶, CEH (awarded by EC Council)⁸⁷, CISSP (awarded by (ISC)2)⁸⁸ and ISO 27001 (awarded by ISMS/IRCA)⁸⁹.

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.

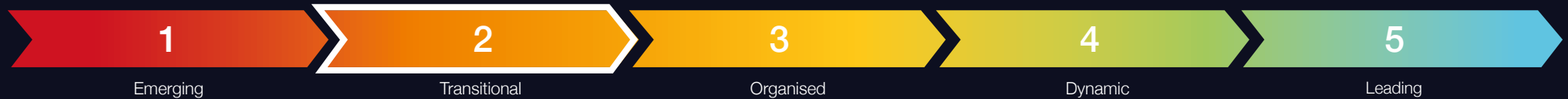
Professional Cyber Membership Organisations or Associations

92. **Professional membership organisations or associations usually focus on furthering the profession they represent.** They provide membership by subscription. Membership benefits include access to further professional development and training, access to discounted products and events, networking and collaboration with like-minded people and increasing professional credibility by virtue of membership. These organisations can frequently be not-for-profit.
93. Several international professional membership organisations operate in the cyber security industry, some with chapters based in individual countries and regions. The existence of chapters in a country or region is direct evidence of an appetite for membership of that organisation, but also 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 Kenya.**

94. **There are six cyber security membership bodies operating in Kenya, two of which, ISACA and (ISC)2, are international with local chapters in Nairobi.** The remaining four are local or regional membership organisations. Of note are **Women in Cyber Security (WiCyS)**, a global community with an affiliate group in East Africa which covers Kenya, Uganda and Tanzania⁹⁰; and SheHacks Kenya, founded in 2016 with the aim of giving Kenyan women in cybersecurity an interactive community⁹¹.

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment



Assessment – Maturity Level 2

Some evidence of in-country cyber security recruitment.

Specialist Cyber Recruitment

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

96. **Five recruitment companies were found operating in Kenya.** With the notable exception of Career Point Kenya which recruits for several sectors including IT and cyber⁹², there appears to be very little evidence of in-country specialist recruitment for cyber security roles.

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

97. Events and exhibitions take a great deal of commitment, finances, advanced planning and organisation to bring to life, and there needs to be an appetite from the target audience to pay the ticket price and attend. **CREST's research looked for any cyber or information security events recently held in Kenya, 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 these events can be far reaching, as they are effective hubs for networking, collaboration and information sharing - which helps sow seeds of cyber security inspiration in their audience.
98. **CREST's research found seven cyber security or information security events between summer 2019 and 2020, with some events planned for 2021.** The events are a good mix of in-country, regional and international organised events.

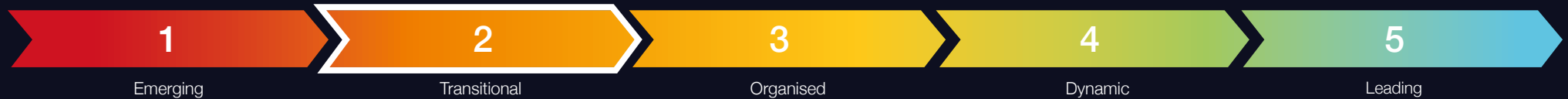


Dimension 5

Banking Sector Cyber
Security Posture

Banking Sector Cyber Security Posture

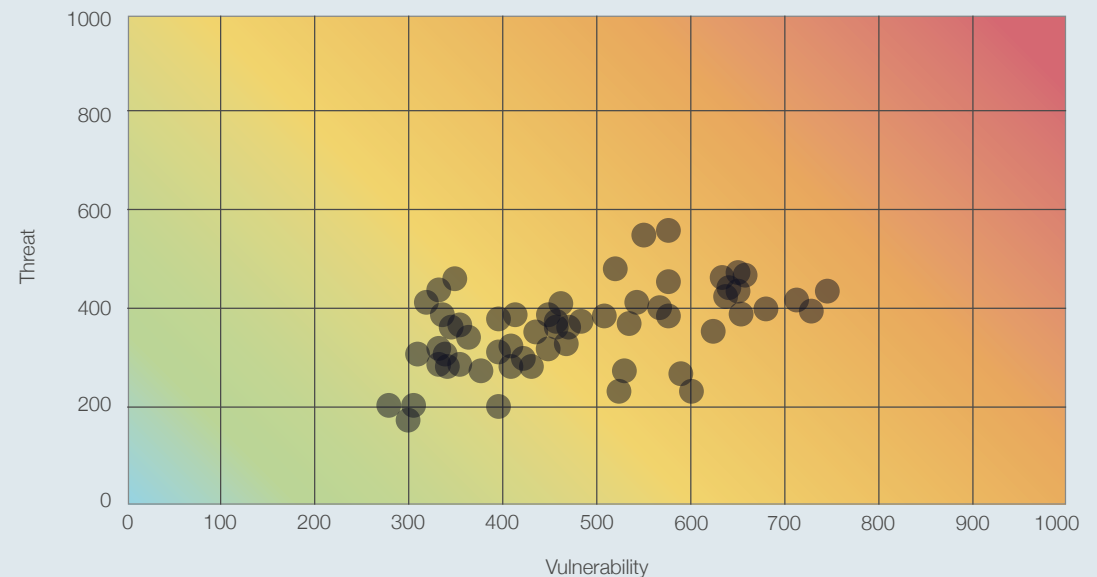
Overall Dimension Assessment: *Maturity Level 2*



99. To assess the current cyber security posture of the Ugandan 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.
100. 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.
101. The results of research into these four metrics are explained in more detail 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, left, 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

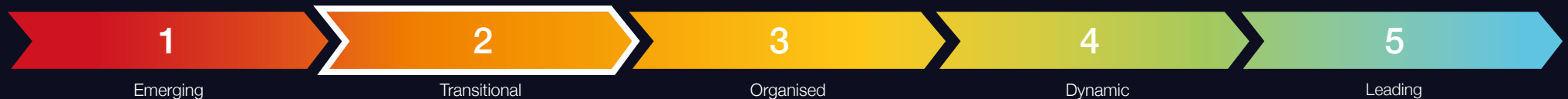
Figures represent CREST's cyber risk rating of each financial institution against a series of non-intrusive metrics



102. In determining the financial institutions to be assessed, the first source was the list of supervised institutions maintained by the Central Bank of Kenya⁹³. This information was cross-checked against the membership list of Kenya Bankers Association⁹⁴, Wikipedia⁹⁵ and the financial institutions' websites, to generate a representative sample of national and international banks and microfinance institutions (MFIs) operating in Kenya. The website addresses and email domains of 60 financial institutions were passed to Orpheus Cyber for initial assessment. Results 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



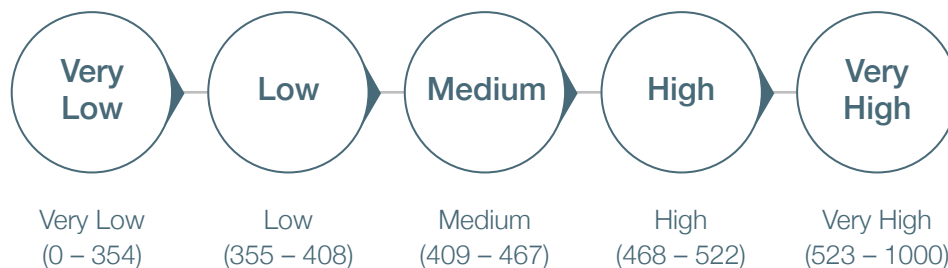
Assessment – Maturity Level 2

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

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

104. 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**:

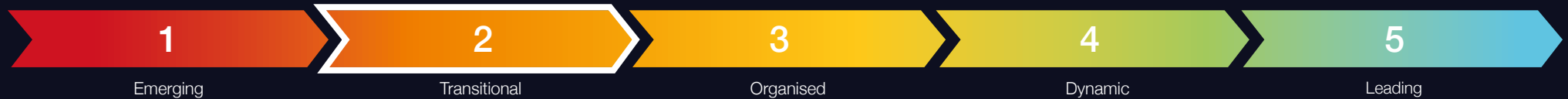


As visible in the scatter diagram on the previous page, assessed financial institutions have been found to have **individual vulnerability scores (X-axis) ranging between 281 and 753**. The **average cyber risk score** for the sample is **420**, which corresponds to a national average risk rating of '**Medium**'.

105. Note that no active (intrusive) assessment was undertaken, nor 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 levels of access required for such an undertaking are far beyond the scope of this report.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile (continued)



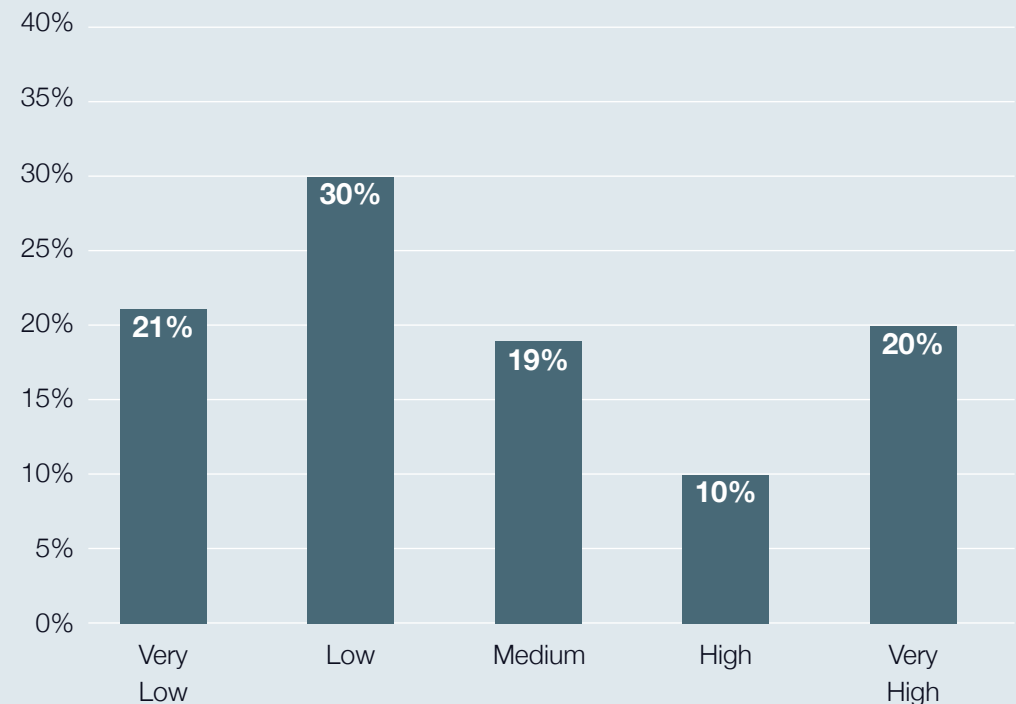
Assessment – Maturity Level 2

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

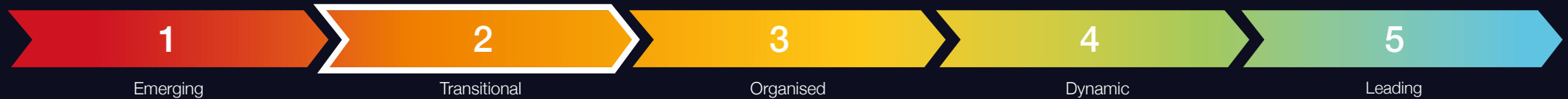
106. A breakdown by category of risk rating of the assessed sample of financial institutions is shown above, once again the results are anonymised. Encouragingly, 51% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'. On the other hand, 30% of the financial institution have an overall cyber risk rating of 'Very High' or 'High'. Institutions in these latter 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.

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



Banking Sector Cyber Security Posture

Indicator 5.2 Infrastructure Vulnerability Risk



Assessment – Maturity Level 2

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

Infrastructure Vulnerability Risk

107. 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.

108. Vulnerabilities, often referred to as CVEs (Common Vulnerabilities and Exposures)⁹⁶, are flaws in software and hardware that cybercriminals seek to exploit when attempting to gain access to the IT infrastructure of a chosen victim. To look for CVEs, they routinely scan portions of the internet. CREST's researchers followed a similar approach, scanning the public-facing IT infrastructure of all 60 of Kenya's 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.

109. **The investigation revealed 41% of Kenya'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.

110. 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 CVS⁹⁷ (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 with which they can be exploited, or the access they provide when successfully exploited. **CREST's research identified 11% of Kenya's assessed financial institutions operate internet-facing IT infrastructure containing 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

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

113. 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 corporate networks.

114.



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**.

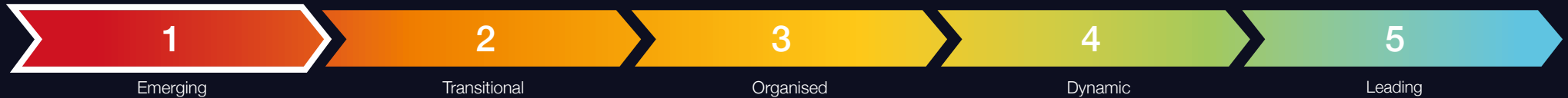
Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk (continued)

115. **CREST's research showed none of the assessed financial institutions maintain any port associated with remote access services open to the internet. This is an excellent finding.**
116. Another set of ports cybercriminals deliberately target are those used by database services. **CREST's research showed that 30% 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.
117. While remote access ports left open to the internet can allow cybercriminals to reach a bank's internal network and steal valuable information, exposed databases place customer data and other sensitive information at an even more direct and imminent risk. This is mostly because database services associated with ports often lack authentication protocols by default, allowing unauthorised third parties to easily access and retrieve their content.
118. Understanding the threat associated with exposed database instances - and reducing the possibility of suffering a data leak also reduces the risk of fines under **Kenya's 2019 Data Protection Act⁹⁸.**

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

119. **Humans have an inherent susceptibility to social engineering and phishing campaigns.** 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.
120. **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.
121. 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 spoofing⁹⁹.
122. 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 sector¹⁰⁰.
123. 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**¹⁰¹.
124. **40%** CREST's research revealed that **40% of the sample of financial institutions had not implemented basic email authentication measures (SPF).**
- 75%** **75% 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 had been identified as having had some employee credentials compromised in recent years by third-party breaches.

Information Leakage Risk

125. **The more sensitive information about an organisation is publicly available, the greater the risk of successful cyber-attacks.** Employees often expose information via social and professional platforms which may be openly viewed by cybercriminals as a starting point for crafting phishing attacks. Alternatively, cybercriminals often gain access to login credentials via the dark web because of third-party website hacks. While the level of information leakage via employee's use of social and professional platforms is hard to quantify, it is easier to spot instances of login credential exposure, and this is often used as a measure of the problem.
126. **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.
127. **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 the corporate accounts of employees. Alternatively, the 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 can 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.
128. It has not been possible to verify how many of the assessed financial institutions follow good hygiene practices and enforce strong password best practices – measures that help mitigate the threat associated with third-party leaked credentials.

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

46%

CREST's research revealed that **46% of the assessed financial institutions had had at least some of their employees' credentials leaked online** after unconnected attacks on third-party website-based service providers.

Banking Sector Cyber Security Posture

Mitigation Measures

129. 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	FIRST	Forum of Incident Response & Security Teams: an international association of CERTs/CSIRTs
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	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
CERT	Computer Emergency Response Team	Information Exchange	A semi-formal mechanism for experts in different organisations to exchange information on observed cyber security threats, vulnerabilities and incidents
CMAGE	Cyber Security Maturity Assessment for Global Ecosystems	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
CSIRT	Computer Security Incident Response Team	IR	Incident Response: a category of cyber security service
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	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
DMARC	Domain-based Message Authentication, Reporting & Conformance: an advanced form of email authentication	Locally registered (service provider)	A cyber security service provider which is registered and headquartered in the country
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	Malware	Malicious software intentionally designed to cause damage to a computer or network
Ethical Hacking	An alternative name for Penetration Testing: see PenTest		

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	Scam	A deceptive scheme or trick used to cheat an organisation or individual out of something, especially money
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	SFP	Sender Policy Framework; a basic form of email authentication
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	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
Port	A physical or virtual connection to a computer server through which different categories of information or instructions are sent and received	Spear-Phishing	A highly targeted attempt at phishing in which the cybercriminal often uses known information to add authenticity to a malicious communication
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	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
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	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. Healthy investment in law enforcement capabilities to counter cybercrime. Awareness of cybercrime within the business community and the public. Some adoption of technical measures. Some investment in cyber defence capabilities. Adoption of some intervention measures to divert potential cybercriminals into cyber security careers (e.g. Cyber Choices).	Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime and some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.	Little evidence of the reporting of cybercrime and its impact. Little evidence of law-enforcement capabilities to tackle cybercrime. Little evidence of public awareness. Little evidence of interest in cyber defence matters.

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1

CERTs & Information Sharing

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

Indicator 3.1

Threat Intelligence Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2

Vulnerability Assessment Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3

Penetration Testing Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4

Security Operation Centre Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5

Incident Response Service providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1

Academia & Higher Education

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

Indicator 4.2

Training Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3

Professional Certifications

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

Indicator 4.4

Professional Cyber Membership Organisations

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5

Specialist Recruitment

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

Indicator 4.6

Events & Exhibitions

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1

Banking Sector Cyber Risk Profile

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

Indicator 5.2

Infrastructure Vulnerability Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3

Architecture & Access Risk

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

Indicator 5.4

Email Authentication Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5

Information Leakage Risk

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

Appendix C

Professional Certifications and Member Organisations

Background

1. Knowledge, skills and experience are factors used by companies when determining who to hire or promote. They are also used by buyers when selecting service providers. Experience is a matter of record, underpinned by endorsements from previous employers or clients. In a mature marketplace, certifications are the common currency used to express an individual's knowledge and skills. Employers can quickly filter potential candidates by certifications they hold, and buyers can use certifications as a benchmark when looking to award a contract. 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, various cyber security certifications have been categorised into a career progression model using a five-tier hierarchy denoting approximate skill level equivalence;
 - Foundation (New Entrant)
 - Practitioner (Intermediate)
 - Senior Practitioner (Subject Matter Expert/Advanced)
 - Principle Advanced (Subject Matter Expert/Senior Management/Chartered)
 - Lead Practitioner (Fellow/Recognised Industry Expert)

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

Certification bodies

3. During CREST's research, fifteen organisations were identified as offering one or more certification of relevance to the cyber security profession. Together, they offer 142 different certifications, including 118 with differing degrees of technical content (grouped as 'Technical Certificates of Relevance') and 24 more focused on security management and other skillsets (grouped as 'Other Certificates of Relevance'). In some cases, certification organisations also act as professional membership organisations, holding events and contributing to through-career development of members.
4. Most certification bodies offer certifications with online exams or through Pearson Vue or PSI test centres. Some certifications requiring practical exams offer this element online, or through connection to a remote network, although some bodies need a physical testing site, which have 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 (also shown in the associated endnote in [Appendix F](#)).

Appendix C

Professional Certifications and Member Organisations (continued)

Certification Body	CERTIFICATION TIER					EXAM DELIVERY				
	Foundation	Practitioner	Senior Practitioner	Principle Advanced	Lead Practitioner	Online	Pearson Vue Centre	PSI Test Centre	Training Classroom	Specialist Test Centre
TECHNICAL CERTIFICATES OF RELEVANCE										
CREST ¹⁰²		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council ¹⁰³	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA ¹⁰⁴		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2 ¹⁰⁵		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS ¹⁰⁶		GSEC GPEN GWAPT GICSP GCIP GCWN GCUX GAWN GPYC GWEB GCIH GCFE GASF GREM GCFA GNFA GSSP-Java GSSP-.Net GICSP GMOB GBFA GCSA	GXPIN GCCC GSED GPPA GMON GCIA GRID GCDA GCTI GCED GPPA GDSA GDAT GEVA GNSA		GSE	✓	✓			
CompTIA ¹⁰⁷	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security ¹⁰⁸		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance ¹⁰⁹		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 ¹¹⁰		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 ¹¹¹		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft ¹¹²	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services ¹¹³	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) ¹¹⁴	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS ¹¹⁵	CSMP	BCM CIAA	CIRM				✓		✓	✓
IET ¹¹⁶	ICTTech									✓

Appendix D

Country Context

Geography

1. Kenya sits in East Africa with a coastline on the Indian Ocean. Its neighbours are Ethiopia in the North, Somalia in the East, Tanzania in the South, Uganda in the West and South Sudan in the North West. It is famous for its spectacular scenery and wildlife reserves. Its capital, Nairobi, sits in the south¹¹⁷.



Natural resources

2. Soda ash - used for glass making - is the most important mineral export for Kenya. Limestone, Vermiculite, gold, rubies, topazes and salt are also important¹¹⁸.

3. Hydroelectricity as a power source has been a focus for Kenya, though the cities tend to consume the bulk of power produced. Access in rural areas can be limited and affected by drought¹¹⁹.

Population

4. In 2019, Kenya's population was ranked 28th highest globally. The estimated population was 48,417,000 in 2020, projected to reach 64,296,000 by 2030. A World Population Review live population tracker estimates Kenya's population to be 54,569,323 in 2021, with a growth rate of 2.8%. This is notably lower than its population growth rate in the early 1980s, when it was 3.94%. Birth and fertility rates are a contributing factor to this drop, with figures falling from an average of 8.1 births per woman in 1977 to an average of 3.4 births per woman¹²⁰.
5. In 2018, population density was 92.6 per square mile with an urban and rural split of 27%:73%¹²¹. As of 2018, 39.1% of the population was under 15 years old, and 27.8% of the population was aged between 15 and 29 years of age. This high number of young people puts pressure on employment opportunities, and the cost of education, health services, food and housing¹²².
6. Kenya's official languages are Swahili and English. The population's literacy rate as of 2015 was 81.1% for males and 75% females. Life expectancy at birth in 2017 was 62.8 years for males and 65.8yrs¹²³ for females¹²⁴.

Economy

7. Kenya's economy was one of the fastest growing in sub-Saharan Africa in 2019, with an average growth rate of 5.7%. In 2020, the economy was hit and slowed down by a plague of locusts as well as COVID-19, and GDP may have contracted to 1.5 or 1% in 2020¹²⁵. The World Bank comments that Kenya has the potential to be one of Africa's success stories because of its growing, youthful population, dynamic private sector, improved infrastructure, a new constitution, and its pivotal role in East Africa. However, the World Bank also states the need to address many challenges, including poverty, inequality, governance, the skills gap between market requirements and the education curriculum¹²⁶. Serianu's Kenya 2018 - Cyber Security Skills Gap Report¹²⁷; also cited education as an issue, along with tackling climate change, low investment, and low firm productivity to achieve rapid, sustained growth rates¹²⁸.
8. Encyclopaedia Britannica suggests tourism and agricultural exports are still a major source of income and foreign exchange. While only contributing a fifth of Kenya's GDP, agriculture still plays a significant role in the economy, as it employs most of the population¹²⁹. In 2017, GNI was US\$71,421 and per capita it was US\$1,440¹³⁰.

Appendix D

Country Context (continued)

9. Serianu's Kenya 2018 - Cyber Security Skills Gap Report reported cybercrime cost Kenya US\$295m in 2018, with 29% of that amount recovered and 71% lost. The most affected industries were:
 - Savings and Credit Co-operative Societies (Saccos)
 - Banking
 - Financial Service Integrators
 - Betting firms, and
 - Government¹³¹.
10. In the Executive Summary of the 2018 Africa Cyber Threat Intelligence Report (ACTIR) it states in 2017 the cost of cybercrime to the African continent was US\$3.7bn, and that 90% of African businesses were operating below the cybersecurity poverty line. The summary cautions that cybercrime will continue to be a problem - because even though the cyber security market would be worth \$2 billion by 2020, there is a lack of viable cybersecurity products or solutions within Africa, and more training and education in computer science and IT security is needed¹³².

Internet connectivity

11. The article "Closing the Internet Connectivity Gap in Kenya (2020)" states in 2000 there were 200,000 internet users, just 7% of the population. Lack of access was most keenly felt by the rurally remote and urban poor. But by 2019, 89.7% of the population were regular internet users, with access to better data, leading to better education opportunities and improved standard of living¹³³. World Internet Stats also quotes 89.7% of the population, which equals 46,870,472 internet users as at Jun 2019¹³⁴.
12. In a January 2021 Communication Authority article, which reports its statistics from July-September 2020, it states seeing increased demand for ICT services, and active mobile subscriptions rose to 59.8million which is up from 57million, with the result that mobile (SIM) penetration is 125.8%¹³⁵.

Cyber crime

13. Serianu's Kenya 2018 - Cyber Security Skills Gap report, suggests an 11% increase of cybercrime incidents being reported to police in 2018, and a 7% increase in successful prosecution¹³⁶.
14. The OSAC Kenya 2020 Crime and Safety Report estimated there are 3000 cybercrime incidents every month¹³⁷.

15. In a 2019 article by the Communication Authority, "Cyber-attacks on the rise in Kenya", it states that its national cyber-security centre had observed a sharp increase in the number of cyber-threats and incidents, rising from 11.3million in the quarter ending on March 30, to 26.6 million between April 1 to June 30, 2019¹³⁸. The article quotes the governor of Embu County as saying: "My government recognises the importance of ICTs as outlined in our ICT roadmap for the period 2015 to 2022. This blue print focuses on increased ICT infrastructure development, staff training and ICT literacy for the residents of this county¹³⁹."
16. An April 2019 article by CIO East Africa, reported that Barclays Bank Kenya had lost KSH11.5 million to suspected criminals believed to have 'hacked' three automated teller machines (ATMs) in different parts of Nairobi over the Easter weekend¹⁴⁰.
17. A 2019 Business Daily Africa article reported E-commerce platform Jumia Kenya had lost at least KSH118 million in the last two years due to consumer cyber fraud and a robbery. In 2017 the firm lost KSH62 million after a group of consumers fraudulently used electronic payment suppliers to acquire goods¹⁴¹.

Appendix D

Country Context (continued)

Cyber Security Professional Development

18. According to a May 2018 Pan African Vision 18 Serianu's Kenya 2018 - Cyber Security Skill Gap states there were 1700 cyber security professionals in Kenya in 2018, with a shortage at senior management levels. The report estimated 60% of companies would face a shortage of cyber security professionals by 2019. Issues with recruiting cyber security professionals include a lack of solid experience and expectations of high remuneration rates¹⁴².

19. The Serianu Kenya 2018 - Cyber Security Skills Gap Report also states that Kenya needs at least 10,000 cyber security professionals to fulfil market needs, but each year, approximately 100 new personnel join the market. The report estimates that by 2023, going by the current rate of technology uptake, the country will need at least 50,000 cyber security professionals. Serianu summarises the skill needs in three categories: understanding, attribution and deterrence¹⁴³.

Other maturity models

20. Oxford University's Global Cyber Security Capacity Centre (GCSCC) has not completed a CMM on Kenya to date¹⁴⁴.
21. The National Cyber Security Index (NCSI) ranks Kenya as 56th of 160 on its national index, and 44th of 160 on its global Index¹⁴⁵.

Appendix E

Bibliography

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

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

Africa CERT (2021)
<https://www.africacert.org/>
(accessed Jul 20 and Mar 21)

Africa Cyber Security Conference (2018). Executive Summary: 2018 Africa Cyber Threat Intelligence Report (ACTIR). *Jighi (online)*.
<https://www.africacybersecurityconference.com/document/Summary-ACTIR-2018.pdf>
(accessed Jul 20 and Mar 21)

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

Business Daily Africa, (2019). How Jumia lost millions in cyber fraud, robbery. Kenya: *Author*. (online)
<https://www.businessdailyafrica.com/corporate/companies/Jumia-lost-millions-in-cyber-fraud/4003102-5023944-89xnyoz/index.html>
(accessed Jul 20 and Mar 21)

Career Point Kenya, (2021). Search Results for Cyber jobs. Kenya: (online)
<https://www.careerpointkenya.co.ke/?s=cyber>
(accessed Mar 21)

Central Bank of Kenya (CBK) (2019). Guidelines on Cyber Security for Payment Service Providers 2019. Kenya: *Author*. (online)
<https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf> (accessed Jul 20 and Mar 21)

Central Bank of Kenya (CBK) (2017). CBK Guidance Note on Cybersecurity for Banking Sector (2017). Kenya: *Author* (online)
https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf
(accessed Jul 20 and Mar 21)

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

Collaboration on International ICT Policy in East and Southern Africa (CIPESA) (2021). Assessing the Barriers to Accessing ICT by People with Disability in Kenya – January 2021. Uganda: *Author* (online)
https://cipesa.org/?wpfb_dl=429 (accessed Feb 21)

Communications Authority of Kenya.
<https://ca.go.ke/>
(accessed Jul 20 and Mar 21)

Communication Authority (2019). Cyber Attacks on the rise in Kenya. Kenya: *Author* (online)
<https://ca.go.ke/cyber-attacks-on-the-rise-in-kenya/>
(accessed Mar 21)

Communications Authority (CA) (2021). Cyber Threats on the Rise with Increased Reliance on ICTs in the Mitigation of Covid-19 Pandemic'. Kenya: *Author* (online)
<https://ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic/> (accessed Mar 21)

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

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

Appendix E

Bibliography (continued)

Cummings, Celeb (2020). Closing the Internet Connectivity Gap in Kenya.
USA: *The Borgen Project* (online)
<https://borgenproject.org/internet-connectivity-gap-in-kenya/> (accessed Feb 21)

Cybersecurity Alliance for Mutual Progress (CAMP). (2021)
<https://www.cybersec-alliance.org/camp/index.do>
(accessed Jan 20 and Mar 21)

Cyber Security Intelligence (2018). Kenya is 3rd in Africa for Cybercrimes Readiness.
UK: *Author* (online)
<https://www.cybersecurityintelligence.com/blog/kenya-is-3rd-in-africa-for-cybercrime-readiness-2677.html> (Accessed Mar 21)

Directorate of Criminal Investigation, (2020) Banking Fraud Investigation Unit.
Kenya: *Author*. (online)
<https://www.cid.go.ke/index.php/sections/investigationunits/banking-fraud-investigation-unit-bfiu.html> (accessed Jul 20 and Mar 21)

Directorate of Criminal Investigations (2020). Digital Forensics Laboratory (DFL).
Kenya: *Author* (online)
<https://cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html>
(accessed Jul 20 and Mar 21)

Directorate of Criminal Investigations (2020). Serious Crime Unit.
Kenya: *Author*. (online)
<https://www.cid.go.ke/index.php/sections/investigationunits/serious-crime-unit.html>
(accessed Mar 21)

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

Forum of Incident Response and Security Teams (FIRST) (2015-2020). USA.
<https://www.first.org/> (accessed Jul 20 and Mar 21)

Global Cyber Security Capacity Centre, (2021). CMM Reviews Around the World. Oxford: *Author*,
<https://gcscc.ox.ac.uk/cmm-reviews>
(accessed Feb 2021)

Government of Kenya (2019). Data Protection Act 2019. Kenya: Kenya Gazette Supplement No. 181 (Acts No. 24).
http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf
(accessed Jul 20 and Feb 21)

ISACA (2016). ISACA-Kenya Chapter.
<https://www.isaca.or.ke/>
(accessed Jul 20 and Mar 21)

(ISC)2, (2019). Kenya Chapter.
<https://www.isc2chapter-kenya.or.ke/>
(accessed Aug 20 and Mar 21)

Information and Communications Technology Authority (ICT-A). Kenya.
<https://icta.go.ke/>
(accessed Jul 20 and Mar 21)

Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040. Kenya: *Author* (online) Ch4 pp24.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf>
(accessed Mar 21)

Internet World Stats, (2019) Kenya Internet Usage Stats and Market Reports (online)
<https://www.internetworldstats.com/af/ke.html>
(accessed Feb 21)

IST-Africa. (2002-2017). Dublin.
<http://www.ist-africa.org/home/default.asp>
(accessed Jul 20 and Mar 21)

IST-Africa (2002-2017). National ICT Research Capacity and Priorities for Cooperation – Republic of Kenya. Dublin: *Author*.
<http://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=6990>
(accessed Jul 20 and Feb 21)

Kenyan Bankers Association. (2021)
<https://www.kba.co.ke/>
(accessed July 20 and Mar 21)

Appendix E

Bibliography (continued)

Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), *Author*, <http://mefmi.org/> (Accessed Oct 2020)

Ministry of Education, (2016). Kenya. <https://education.go.ke/> (accessed Mar 21)

Ministry of Information, Communications and Technology. <https://ict.go.ke/> (accessed Jul 20 and Mar 21)

Ministry of Information, Communications and Technology (2018). Computer Misuse & Cyber Crimes Act 2018. Kenya: *Kenya Gazette Supplement No 60 (Acts No5)* (online). <http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> (accessed Jul 20 and Feb 21)

Ministry of Information, Communications and Technology - National Cyber Security Strategy (2014). Kenya: *Author*. (online) <https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf> (accessed Jul 20 and Mar 21)

Ministry of Information, Communications and Technology (MoICT) (2016). National Information and Communications Technology (ICT) Policy 2016. Kenya: *Author* (online) <http://icta.go.ke/national-ict-policy/> (accessed Mar 21)

Ministry of Information, Communications and Technology Kenya (2019). National Information, Communications and Technology (ICT) Policy 2019. Kenya: *Author* (online) <https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf> (accessed Jul 20 and Feb 21)

Ministry of Information, Communications and Technology (2014-2017). The Kenya National ICT Masterplan 2014 – 2017. Kenya: *Author* (online) <http://icta.go.ke/national-ict-masterplan/> (accessed Jul 20 and Mar 21)

Mwale Litwaji, C (2017). The Phenomenal Adequacy and Efficiency of Cybercrimes in Kenya. Kenya: *MOI University – School of Law (Ch 3.3.1.3 National Intelligence Services) (NIS)* https://www.academia.edu/36412418/THE_PHENOMENAL_ADEQUACY_AND_EFFICIENCY_OF_CYBER_CRIME_LAWS_IN_KENYA (Accessed Feb 21)

National Computer Security Incident Response Team (KE-CIRT/CC) (2020). Kenya. <https://ke-cirt.go.ke/> (accessed Jul 20 and Mar 21)

National Council for Law Reporting (2011). The Kenya Information and Communications Act, Ch 411A, Revised Edition 2011. Kenya: *Author* (online) <https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf> (accessed Jul 20 and Feb 21)

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

National Cyber Security Index (2021). *Estonia, e-Governance Academy*, (online), <https://ncsi.ega.ee/ncsi-index/> (accessed Feb 21)

National Intelligence Services (NIS) (2021) Kenya. <https://www.nis.go.ke/index.html> (accessed Mar 21)

National Police Service (NPS), (2021). Kenya. <https://www.nationalpolice.go.ke/> (accessed Jul 20 and Mar 21)

National Police Service (2013). Strategic Plan 2013/14-2017/18. Kenya: *Author* (online). <https://nationalpolice.go.ke/downloads/category/14-nps-strategic-plan.html> (accessed Mar 21)

Odlambo, Humphrey (2019). ‘Hackers’ steal 11.5million from Barclays Bank teller machines in Nairobi. Kenya: *CIO East Africa* (online) <https://www.cio.co.ke/hackers-steal-11-5-million-from-barclays-bank-teller-machines-in-nairobi/> (accessed Jul 20 and Mar 21)

Okoth Jackson (2019). Banker's Plot to Combat the Threat of Cybercrime. Kenya: *The Kenyan Wall Street*. <https://kenyanwallstreet.com/bankers-plot-to-combat-the-threat-of-cybercrime/> (accessed Mar 21)

Appendix E

Bibliography (continued)

OSAC (2020). Kenya 2020 Crime and Safety Report. *Author* (online)

<https://www.osac.gov/Content/Report/50c57c03-c161-4f9c-8942-182082896065> (Accessed Mar 21)

Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020).

Kenya. *Encyclopedia Britannica*,

<https://www.britannica.com/place/Kenya>

(Accessed 25 February 2021).

Parliament of Kenya (2013). The Kenya Information and Communications (Amendment) Act 2013.

Kenya: *Kenya Gazette Supplement No. 169A (Acts No. 41 A) para 2c and 24c*

<https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-and-Communication-Amendment-Act-2013.pdf> (accessed Jul 20 and Mar 21)

Parliament of Kenya (2018). The Computer Misuse and Cybercrimes Act 2018.

Kenya: *Kenya Gazette Supplement (No 60 Acts No5)*

<http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> (accessed Jul 20 and Mar 21)

Sacco Societies Regulatory Authority (SASRA), (2021).

<https://www.sasra.go.ke/>

(accessed Jul 20 and Feb 21)

Sambuli N, Maina J and Kamau T, (2016). Mapping the Cyber Policy Landscape: Kenya.

London: *Global Partners Digital*. (online), pp8-10.

<https://www.gp-digital.org/wp-content/uploads/2016/12/Kenya-Cyber-Policy-Mapping-final-i-1.pdf> (accessed Jul 20 and Mar 21)

Sentinel Africa (2020). Sentinel Talent Shield Program.

Kenya: *Author* (online)

<https://sentinel africa.co.ke/talent-shield/>

(accessed Jul 20 and Mar 21)

Serianu. (2021) Africa Cyber Immersion Centre (ACIC).

Kenya: *Author*. (online)

<https://www.serianu.com/acic.html>

(accessed Jul 20 and Mar 21)

Serianu, 'Africa Cyber Security Report 2017 - Demystifying Africa's Cyber Security Poverty Line' Kenya, *Author*, 2017,

<https://www.serianu.com/downloads/AfricaCyberSecurityReport2017.pdf>

Accessed July 2020)

Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap.

Kenya: *Author* (online)

<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>

(accessed Feb 21)

Serianu (2020). Africa Cyber Security Report – Kenya 2019/ 2020, Local Perspective on Data Protection and Privacy Laws, Insights from African SMEs.

Kenya: *Author* (online)

<https://www.serianu.com/downloads/KenyaCyberSecurityReport2020.pdf>

(accessed Feb 21)

Serianu (2018). Sacco Cybersecurity Report 2018 – Demystifying Cybersecurity for Saccos.

Kenya: *Author*.

<https://www.serianu.com/downloads/SaccoCyberSecurityReport2018.pdf>

(accessed Mar 21)

SheHacks Kenya, (2021).

<https://www.shehackske.com/>

(accessed Aug 20 and Mar 21)

Suri, Tavneet (2018), The Impact of Internet Connectivity in Kenya. *Innovations for Poverty Action (IPA)* (online)

<https://www.poverty-action.org/study/impact-internet-connectivity-kenya#:~:text=The%20Impact%20of%20Internet%20Connectivity%20in%20Kenya%20The,and%20the%20spread%20of%20low-cost%20smartphones%20and%20tablets.>

(accessed Feb 21)

TESPOK (2015) iCSIRT (online)

https://www.tespok.co.ke/?page_id=11674

(accessed Mar 21)

Appendix E

Bibliography (continued)

The African Network Information Centre (AFRINIC),
<https://afrinic.net/about>
(accessed July 2020)

The World Bank, (2021). The World Bank in Kenya –
Economic Overview, *Author*, (online)
<https://www.worldbank.org/en/country/kenya>
(accessed Feb 21)

The Sacco Societies Regulatory Authority (SASRA)
(2015). Guidelines on Risk Management Practices for
Deposit Taking SACCO Societies.
Kenya: *Author* (Pdf available to download)
Ch 5 pp44-49.
[https://www.sasra.go.ke/index.php?option=com_](https://www.sasra.go.ke/index.php?option=com_phocadownload&view=category&id=1&Itemid=194#YEFAQ-k5xdPY)
[phocadownload&view=category&id=1&Itemid=194#.](https://www.sasra.go.ke/index.php?option=com_phocadownload&view=category&id=1&Itemid=194#YEFAQ-k5xdPY)
[YEFAQ-k5xdPY](https://www.sasra.go.ke/index.php?option=com_phocadownload&view=category&id=1&Itemid=194#YEFAQ-k5xdPY)

UN, (2020). UNDIR Cyber Security Portal – Kenya.
Author (online)
<https://undir.org/cpp/en/states/kenya>
(accessed Feb 21)

Women in Cyber Security (WiCyS), (2021). Affiliate and
Industry - Worldwide Affiliates – Africa.
USA: *Author*.
[https://www.wicys.org/initiatives/affiliate-and-](https://www.wicys.org/initiatives/affiliate-and-industry/)
[industry/](https://www.wicys.org/initiatives/affiliate-and-industry/) (accessed Aug 20 and Mar21)

World Population Review, (2021). Kenya Population 2021.
USA: *Author* (online)
[https://worldpopulationreview.com/countries/kenya-](https://worldpopulationreview.com/countries/kenya-population)
[population](https://worldpopulationreview.com/countries/kenya-population) (accessed Feb 21)

Appendix F

Endnotes

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

1. Further information available on the Bill & Melinda Gates Foundation, Financial Services for the Poor programme website, <https://www.gatesfoundation.org/What-We-Do/Global-Growth-and-Opportunity/Financial-Services-for-the-Poor> (accessed 29 Oct 2020)
2. Further information available on the CREST International website, <https://crest-approved.org/> (accessed 29 Oct 2020)
3. Further information available on the Orpheus Cyber website, <https://orpheus-cyber.com/> (accessed 29 Oct 2020)
4. Ministry of Information, Communications and Technology. <https://ict.go.ke/> (accessed Jul 20 and Mar 21)
5. Ministry of Information, Communications and Technology - National Cyber Security Strategy (2014). Kenya: *Author*. (online) <https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf> (accessed Jul 20 and Mar 21)
6. Ministry of Information, Communications and Technology (2014-2017). The Kenya National ICT Masterplan 2014 – 2017. Kenya: *Author* (online) <http://icta.go.ke/national-ict-masterplan/> (accessed Jul 20 and Mar 21)
7. Ministry of Information, Communications and Technology (MoICT) (2016). National Information and Communications Technology (ICT) Policy 2016. Kenya: *Author* (online) <http://icta.go.ke/national-ict-policy/> (accessed Mar 21)
8. Ministry of Information, Communications and Technology Kenya (2019). National Information, Communications and Technology (ICT) Policy 2019. Kenya: *Author* (online) <https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf> (accessed Jul 20 and Feb 21)
9. Ministry of Information, Communications and Technology. <https://ict.go.ke/> (accessed Jul 20 and Mar 21)
10. Information and Communications Technology Authority (ICT-A). Kenya. <https://icta.go.ke/> (accessed Jul 20 and Mar 21)
11. Information and Communications Technology Authority (ICT-A). Kenya. <https://icta.go.ke/> (accessed Jul 20 and Mar 21)
12. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040. Kenya: *Author* (online) pp12. <https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
13. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040. Kenya: *Author* (online) Ch4 pp24. <https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
14. Communications Authority of Kenya (2021). <https://ca.go.ke/> (accessed Jul 20 and Mar 21)
15. The Ministry of Information, Communications and Technology (2019). State Corporations Under Ministry of ICT. Kenya: *Author*. (Online) <https://ict.go.ke/state-corporations-under-mict/> (accessed Mar 21)
16. Communications Authority of Kenya (2021). Who We Are. Kenya: *Author* (online) <https://ca.go.ke/about-us/who-we-are/> (accessed Mar 21)
17. Communications Authority of Kenya, (2021). Statutes and Regulations. Kenya: *Author*. (online) <https://ca.go.ke/about-us/statutes-regulations/overview/> (accessed Mar 21)

Appendix F

Endnotes (continued)

18. Communications Authority of Kenya, (2021). Search results for Cyber. Kenya: *Author* (online)
<https://ca.go.ke/?s=cyber>
(accessed Mar 21)
19. Communications Authority of Kenya (2021). About KE-CIRT.
Kenya: *Author*. (online)
<https://ca.go.ke/industry/cyber-security/about-ke-cirt/> (accessed Mar 21)
20. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch4 pp24.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
21. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch4 pp24.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
22. Ministry of Information, Communications and Technology Kenya (2019). National Information, Communications and Technology (ICT) Policy.
Kenya: *Author* (online)
<https://www.ict.go.ke/wp-content/uploads/2019/12/NATIONAL-ICT-POLICY-2019.pdf>
(accessed Jul 20 and Feb 21)
23. Government of Kenya (2019). Data Protection Act 2019.
Kenya: *Kenya Gazette Supplement No. 181* (Acts No. 24).
http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct_No24of2019.pdf (accessed Jul 20 and Feb 21)
24. Parliament of Kenya (2018). The computer Misuse and Cybercrimes Act 2018.
Kenya: *Kenya Gazette Supplement* (No 60 Acts No5)
<http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/ComputerMisuseandCybercrimesActNo5of2018.pdf> (accessed Jul 20 and Mar 21)
25. Ministry of Information, Communications and Technology (2014-2017). The Kenya National ICT Masterplan 2014 – 2017.
Kenya: *Author* (online)
<http://icta.go.ke/national-ict-masterplan/> (accessed Jul 20 and Mar 21)
26. Ministry of Information, Communications and Technology (2014-2017). The Kenya National ICT Masterplan 2014 – 2017.
Kenya: *Author* (online) Ch4.2.4 pp50-54.
<http://icta.go.ke/national-ict-masterplan/> (accessed Jul 20 and Mar 21)
27. Ministry of Information, Communications and Technology (2014-2017). The Kenya National ICT Masterplan 2014 – 2017.
Kenya: *Author* (online) Ch6.6.3 pp96.97.
<http://icta.go.ke/national-ict-masterplan/> (accessed Jul 20 and Mar 21)
28. The Ministry of Information, Communications and Technology - National Cyber Security Strategy (2014).
Kenya: *Author*. (online) pp6-8
<https://icta.go.ke/pdf/NATIONAL%20CYBERSECURITY%20STRATEGY.pdf>
(accessed Jul 20 and Mar 21)
29. National Council for Law Reporting (2011). The Kenya Information and Communications Act, Ch 411A, Revised Edition 2011.
Kenya: *Author* (online)
<https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-Communications-Act-1.pdf>
(accessed Jul 20 and Feb 21)
30. Parliament of Kenya (2013). The Kenya Information and Communications (Amendment) Act 2013, No 41A of 2013. para 2c and 24c
<https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-and-Communication-Amendment-Act-2013.pdf>
(accessed Jul 20 and Mar 21)

Appendix F

Endnotes (continued)

31. Parliament of Kenya (2013). The Kenya Information and Communications (Amendment) Act 2013. Kenya: *Kenya Gazette Supplement* No. 169A (Acts No. 41 A) para 2c and 24c
<https://ca.go.ke/wp-content/uploads/2018/02/Kenya-Information-and-Communication-Amendment-Act-2013.pdf>
(accessed Jul 20 and Mar 21)
32. Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), Author, <http://mefmi.org/> (Accessed Oct 2020)
33. Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), Author, <http://mefmi.org/> (Accessed Oct 2020)
34. Kenyan Bankers Association. (2021)
<https://www.kba.co.ke/>
(accessed July 20 and Mar 21)
35. Okoth Jackson (2019). Banker's Plot to Combat the Threat of Cybercrime.
Kenya: *The Kenyan Wall Street*.
<https://kenyanwallstreet.com/bankers-plot-to-combat-the-threat-of-cybercrime/>
(accessed Mar 21)
36. Central Bank of Kenya (CBK) (2017). CBK Guidance Note on Cybersecurity for Banking Sector (2017). Kenya: Author (online)
https://www.centralbank.go.ke/uploads/banking_circulars/634077191_GUIDANCE%20NOTE%20ON%20CYBERSECURITY%20FOR%20THE%20BANKING%20SECTOR.pdf
(accessed Jul 20 and Mar 21)
37. Central Bank of Kenya (CBK) (2019). Guidelines on Cyber Security for Payment Service Providers 2019. Kenya: Author. (online)
<https://www.centralbank.go.ke/wp-content/uploads/2019/07/GuidelinesonCybersecurityforPSPs.pdf>
(accessed Jul 20 and Mar 21)
38. Sacco Societies Regulatory Authority (SASRA). (2021)
<https://www.sasra.go.ke/>
(accessed Jul 20 and Feb 21)
39. Serianu (2018). Sacco Cybersecurity Report 2018 – Demystifying Cybersecurity for Saccos.
Kenya: Author.
<https://www.serianu.com/downloads/SaccoCyberSecurityReport2018.pdf>
(accessed Mar 21)
40. The Sacco Societies Regulatory Authority (SASRA) (2015). Guidelines on Risk Management Practices for Deposit Taking SACCO Societies.
Kenya: Author (Pdf available to download) Ch 5 pp44-49.
https://www.sasra.go.ke/index.php?option=com_cadownload&view=categor&id=1&Itemid=194#.YEFQ-k5xdPY
41. Communications Authority (CA) (2021). Cyber Threats on the Rise with Increased Reliance on ICTs in the Mitigation of Covid-19 Pandemic'.
Kenya: Author (online)
<https://ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic/> (accessed Mar 21)
42. Communications Authority (CA) (2021). Cyber Threats on the Rise with Increased Reliance on ICTs in the Mitigation of Covid-19 Pandemic'.
Kenya: Author (online)
<https://ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic/> (accessed Mar 21)
43. National Police Service (NPS), (2021). Kenya.
<https://www.nationalpolice.go.ke/>
(accessed Jul 20 and Mar 21)

Appendix F

Endnotes (continued)

44. National Police Service (2013). Strategic Plan 2013/14-2017/18.
Kenya: *Author* (online). pp12-17.
<https://nationalpolice.go.ke/downloads/category/14-nps-strategic-plan.html>
(accessed Mar 21)
45. National Police Service (2013). Strategic Plan 2013/14-2017/18.
Kenya: *Author* (online). pp60-62
<https://nationalpolice.go.ke/downloads/category/14-nps-strategic-plan.html>
(accessed Mar 21)
46. Directorate of Criminal Investigations (2020). Digital Forensics Laboratory (DFL).
Kenya: *Author* (online)
<https://cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html>
(accessed Jul 20 and Mar 21)
47. Directorate of Criminal Investigations (2020). Serious Crime Unit.
Kenya: *Author*. (online)
<https://www.cid.go.ke/index.php/sections/investigationunits/serious-crime-unit.html>
(accessed Mar 21)
48. Directorate of Criminal Investigations (2020). Digital Forensics Laboratory (DFL).
Kenya: *Author* (online)
<https://cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html>
(accessed Jul 20 and Mar 21)
49. National Computer Security Incident Response Team (KE-CIRT/CC) (2020). National KE-CIRT/CC Partners. Kenya. *Author*. (online)
<https://ke-cirt.go.ke/partners/> (accessed Mar 21)
50. Directorate of Criminal Investigation, (2020) Banking Fraud Investigation Unit.
Kenya: *Author*.
<https://www.cid.go.ke/index.php/sections/investigationunits/banking-fraud-investigation-unit-bfiu.html> (accessed Jul 20 and Mar 21)
51. National Computer Security Incident Response Team (KE-CIRT/CC) (2020). Kenya.
<https://ke-cirt.go.ke/> (accessed Jul 20 and Mar 21)
52. National Computer Security Incident Response Team (KE-CIRT/CC) (2020). National KE-CIRT/CC Partners. Kenya. *Author*. (online)
<https://ke-cirt.go.ke/partners/> (accessed Mar 21)
53. Africa CERT (2021)
<https://www.africacert.org/>
(accessed Jul 20 and Mar 21)
54. Forum of Incident Response and Security Teams (FIRST) (2015-2020). USA.
<https://www.first.org/>
(accessed Jul 20 and Mar 21).
55. 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)
56. Kenya Education Network CERT (KENET-CERT) (2018).
Kenya: *Author*
<https://cert.kenet.or.ke/>
(accessed Jul 20 and Mar 21)
57. Directorate of Criminal Investigations (2020). Digital Forensics Laboratory (DFL).
Kenya: *Author* (online)
<https://cid.go.ke/index.php/sections/forensic-sections/cyber-crime.html>
(accessed Jul 20 and Mar 21)
58. TESPOK (2015). About TESPOK. (online)
<https://www.tespok.co.ke>
(accessed Mar 21)
59. TESPOK (2015). iCSIRT (online)
https://www.tespok.co.ke/?page_id=11674
(accessed Mar 21)
60. Africa CERT (2021)
<https://www.africacert.org/>
(accessed Jul 20 and Mar 21)
61. Cybersecurity Alliance for Mutual Progress (CAMP). (2021)
<https://www.cybersec-alliance.org/camp/index.do>
(accessed Jan 20 and Mar 21)
62. Cybersecurity Alliance for Mutual Progress (CAMP). (2021) About CAMP.
Korea: *Author*
<https://www.cybersec-alliance.org/camp/index.do>
(accessed Jan 20 and Mar 21)

Appendix F

Endnotes (continued)

63. Ministry of Education, (2016). Kenya.
<https://education.go.ke/> (accessed Mar 21)
64. IST-Africa. (2002-2017). Dublin.
<http://www.ist-africa.org/home/default.asp>
(accessed Jul 20 and Mar 21)
65. IST-Africa. (2002-2017). Dublin.
<http://www.ist-africa.org/home/default.asp>
(accessed Jul 20 and Mar 21)
66. IST-Africa (2002-2017). National ICT Research Capacity and Priorities for Cooperation – Republic of Kenya. Dublin: *Author*.
<http://www.ist-africa.org/home/default.asp?page=doc-by-id&docid=6990>
(accessed Jul 20 and Feb 21)
67. 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)
68. Forum of Incident Response and Security Teams (FIRST) (2015-2020). USA.
<https://www.first.org/>
(accessed Jul 20 and Mar 21)
69. CREST, 'Accredited Companies Providing Vulnerability Assessment Services', 2020,
https://service-selection-platform.crest-approved.org/accredited_companies/vulnerability_assessment/ (accessed Nov 2020)
70. National Cyber Security Centre (NCSC), "Penetration Testing", UK, *Author*, 8 Aug 2017,
<https://www.ncsc.gov.uk/guidance/penetration-testing> (accessed Nov 2020)
71. CREST, 'Accredited Companies providing Security Operations Centres (SOC)' 2020, *Author*,
https://service-selection-platform.crest-approved.org/accredited_companies/soc/
(accessed Nov 2020)
72. 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)
73. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch. 4.2.3 & 4.2.4, pp28-30
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
74. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch.4.2.4, pp28.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
75. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch.4.2.4, pp28.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
76. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch.4.2.4, pp29.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
77. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch.4.2.4, pp30.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
78. Information and Communication Technology Authority (ICT-A). (2020). ICT Authority Strategic Plan 2020-2040.
Kenya: *Author* (online) Ch.4.2.4, pp30.
<https://icta.go.ke/pdf/ICT%20Strategic%20Plan.pdf> (accessed Mar 21)
79. Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. *Author* (online) pp11.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)

Appendix F

Endnotes (continued)

80. Serianu. (2021) Africa Cyber Immersion Centre (ACIC). Kenya: *Author*. (online)
<https://www.serianu.com/acic.html>
(accessed Jul 20 and Mar 21)
81. Sentinel Africa (2020). Sentinel Talent Shield Program. Kenya: *Author* (online)
<https://sentinelafrica.co.ke/talent-shield/>
(accessed Jul 20 and Mar 21)
82. CREST International,
<https://www.crest-approved.org/>
(accessed Aug 20)
83. Cisco,
<https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html>
(accessed Aug 20)
84. ISACA. ISACA-Kenya Chapter.
<https://www.isaca.or.ke/>
(accessed Jul 20 and Mar 21)
85. (ISC)2, (2019). Kenya Chapter.
<https://www.isc2chapter-kenya.or.ke/>
(accessed Aug 20 and Mar 21)
86. ISACA,
<https://www.isaca.org/>
(accessed Aug 20)
87. EC Council,
<https://www.eccouncil.org/>
(accessed Aug 20)
88. (ISC)2,
<https://www.isc2.org/>
(accessed Aug 20)
89. IRCA(ISMS),
<https://www.quality.org/>
(accessed Aug 20)
90. Women in Cyber Security (WiCyS), (2021). Affiliate and Industry - Worldwide Affiliates – Africa. USA: *Author*.
<https://www.wicys.org/initiatives/affiliate-and-industry/> (accessed Aug 20 and Mar21)
91. SheHacks Kenya, (2021).
<https://www.shehackske.com/>
(accessed Aug 20 and Mr 21)
92. Career Point Kenya, (2021). Search Results for Cyber jobs.
<https://www.careerpointkenya.co.ke/?s=cyber>
(accessed Mar 21)
93. Central Bank of Kenya, Supervised Banks,
<https://www.centralbank.go.ke/bank-supervision/>
(accessed 26 May 2020)
94. Kenya Bankers Association,
<https://www.kba.co.ke/>
(accessed 26 May 2020)
95. Wikipedia, List of Banks in Kenya,
https://en.wikipedia.org/wiki/List_of_banks_in_Kenya (accessed 26 May 2020)
96. 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)
97. Further information on CVSS available on Wikipedia,
https://en.wikipedia.org/wiki/Common_Vulnerability_Scoring_System
(accessed on 29 Oct 2020)
98. Kenya Law, Data Protection Act, 2019,
http://kenyalaw.org/kl/fileadmin/pdfdownloads/Acts/2019/TheDataProtectionAct__No24of2019.pdf (accessed 22 Dec 20)
99. Valimail report on DMARC, 2019,
<https://www.valimail.com/resources/domain-spoofing-declines-as-protective-measures-grow/>
(accessed 30 Oct 2020)
100. Finance Digest Report, 2019,
<https://www.financedigest.com/rise-sophisticated-bec-scams-finance-industry>
(accessed 30 Oct 2020)
101. FBI Internet Crime Report, 2019,
<https://www.ic3.gov/Media/Y2019/PSA190910>
(accessed 31 Oct 2020)
102. CREST International,
<https://www.crest-approved.org/>
(accessed Aug 20)
103. EC Council,
<https://www.eccouncil.org/>
(accessed Aug 20)
104. ISACA,
<https://www.isaca.org/>
(accessed Aug 20)

Appendix F

Endnotes (continued)

105. (ISC)2,
<https://www.isc2.org/>
(accessed Aug 20)
106. SANS,
<https://www.sans.org/>
(accessed Aug 20)
107. CompTIA,
<https://www.comptia.org/>
(accessed Aug 20)
108. Offensive Security,
<https://www.offensive-security.com/>
(accessed Aug 20)
109. Cloud Security Alliance,
<https://cloudsecurityalliance.org/education/>
(accessed Aug 20)
110. PCI,
https://www.pcisecuritystandards.org/program_training_and_qualification/
(accessed Aug 20)
111. Cisco,
<https://www.cisco.com/c/en/us/training-events/training-certifications/certifications/security.html>
(accessed Aug 20)
112. Microsoft,
<https://www.microsoft.com/en-us/learning/browse-all-certifications.aspx> (accessed Aug 20)
113. Amazon Web Services,
https://aws.amazon.com/training/path-security/?nc2=sb_lp_se (accessed Aug 20)
114. IRCA(ISMS),
<https://www.quality.org/> (accessed Aug 20)
115. BCS,
<https://www.bcs.org/get-qualified/certifications-for-professionals/information-security-and-ccp-scheme-certifications/> (accessed Aug 20)
116. IET,
<https://www.theiet.org/career/professional-registration/ict-technician/> (accessed Aug 20)
117. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Introduction and Quick facts. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
118. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Resources and Power. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
119. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Resources and Power. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
120. World Population Review, (2021). Kenya Population 2021. USA: *Author* (online)
<https://worldpopulationreview.com/countries/kenya-population> (accessed Feb 21)
121. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Introduction and Quick facts. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
122. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Demographic Trends. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
123. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Introduction and Quick facts. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
124. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Introduction and Quick facts. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
125. The World Bank, (2021). The World Bank in Kenya – Economic Overview, *Author*, (online)
<https://www.worldbank.org/en/country/kenya>
(accessed Feb 21)
126. The World Bank, (2021). The World Bank in Kenya – Economic Overview, *Author*, (online)
<https://www.worldbank.org/en/country/kenya>
(accessed Feb 21)

Appendix F

Endnotes (continued)

127. Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. Kenya: *Author* (online) pp11.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)
128. The World Bank, (2021). The World Bank in Kenya – Economic Overview, *Author*, (online)
<https://www.worldbank.org/en/country/kenya>
(accessed Feb 21)
129. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Economy, Agriculture, Forestry and Fishing. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
130. Ominde, Simeon Hongo, Ingham, Kenneth and Ntarangwi, Mwenda. (2020). Kenya – Introduction and Quick facts. *Encyclopedia Britannica*, (online)
<https://www.britannica.com/place/Kenya>
(Accessed 25 February 2021).
131. Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. Kenya: *Author* (online) pp12 & pp31.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)
132. Africa Cyber Security Conference (2018). Executive Summary: 2018 Africa Cyber Threat Intelligence Report (ACTIR). *Jighi* (online).
<https://www.africacybersecurityconference.com/document/Summary-ACTIR-2018.pdf>
(accessed Jul 20 and Mar 21)
133. Cummings, Celeb (2020). Closing the Internet Connectivity Gap in Kenya. USA: *The Borgen Project* (online)
<https://borgenproject.org/internet-connectivity-gap-in-kenya/> (accessed Feb 21)
134. Internet World Stats, (2019) Kenya Internet Usage Stats and Market Reports (online)
<https://www.internetworldstats.com/af/ke.html>
(accessed Feb 21)
135. Communications Authority (CA) (2021). Cyber Threats on the Rise with Increased Reliance on ICTs in the Mitigation of Covid-19 Pandemic'. Kenya: *Author* (online)
<https://ca.go.ke/cyber-threats-on-the-rise-with-increased-reliance-on-icts-in-the-mitigation-of-covid-19-pandemic/> (accessed Mar 21)
136. Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. Kenya: *Author* (online) pp12.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)
137. OSAC (2020). Kenya 2020 Crime and Safety Report. *Author* (online)
<https://www.osac.gov/Content/Report/50c57c03-c161-4f9c-8942-182082896065>
(Accessed Mar 21)
138. Communication Authority (2019). Cyber Attacks on the rise in Kenya. Kenya: *Author* (online)
<https://ca.go.ke/cyber-attacks-on-the-rise-in-kenya/> (accessed Mar 21)
139. Communication Authority (2019). Cyber Attacks on the rise in Kenya. Kenya: *Author* (online)
<https://ca.go.ke/cyber-attacks-on-the-rise-in-kenya/> (accessed Mar 21)
140. Odlambo, Humphrey (2019). 'Hackers' steal 11.5million from Barclays Bank teller machines in Nairobi. Kenya: *CIO East Africa* (online)
<https://www.cio.co.ke/hackers-steal-11-5-million-from-barclays-bank-teller-machines-in-nairobi/>
(accessed Jul 20 and Mar 21)
141. Business Daily Africa, (2019). How Jumia lost millions in cyber fraud, robbery. Kenya: *Author*. (online)
<https://www.businessdailyafrica.com/corporate/companies/Jumia-lost-millions-in-cyber-fraud/4003102-5023944-89xnyoz/index.html>
(accessed Jul 20 and Mar 21)

Appendix F

Endnotes (continued)

^{142.} Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. Kenya: *Author* (online) pp12.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)

^{143.} Serianu (2018). Africa Cyber Security Report - Kenya 2018, Cyber Security Skills Gap. *Author* (online) pp11.
<https://www.serianu.com/downloads/KenyaCyberSecurityReport2018.pdf>
(accessed Feb 21)

^{144.} Global Cyber Security Capacity Centre, (2021). CMM Reviews Around the World. Oxford: *Author*,
<https://gcsc.ox.ac.uk/cmm-reviews>
(accessed Feb 2021)

^{145.} National Cyber Security Index (2021). Estonia, *e-Governance Academy*, (online),
<https://ncsi.ega.ee/ncsi-index/>
(accessed Feb 21)