CMAGE

Cyber Security Maturity Assessment Global Ecosystem

Uganda Report

Maturity Model Assessment

2021

Report Structure

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

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

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

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

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

A short commentary to support the maturity level assessment is also found in the corresponding section.

The report contains six appendices:

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

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

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

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

Navigation Key

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

Contents

Foreword from Ian Glover, President, CREST International

While organisations and individuals can take steps to maintain and improve their own cyber security, most of us live in a highly connected world.

We rely on the actions of others to play their part in sustaining our collective cyber security.

Knowingly or unknowingly, we are all part of a complex cyber security ecosystem which reaches far beyond the technology itself.

At the organisational level, the cyber security ecosystem comprises:

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

In this Cyber security Maturity Assessment of the Global Ecosystem (CMAGE), we have gathered evidence against twenty indicators across five specific dimensions of the Ugandan Cyber Security Ecosystem.

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

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

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

The relational database containing the CMAGE model has helped facilitate consistent application of the assessment and allows for ease of update and maintenance of 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 collaborative journey between CREST and national and international stakeholders with the shared interest of improving Uganda's overall cyber security posture.

Unashamedly, the endpoint from a CREST perspective is that every financial services institution in Uganda 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 Uganda 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 we are all now undertaking.

Ian Glover
President
CREST International

Highlights Report

Background

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

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

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

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

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

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

Maturity Model Assessment Summary

Overall 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'.

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

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

Dimensions and Indicators

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

Qualitative Assessments	1-4
Qualitative Assessments	5

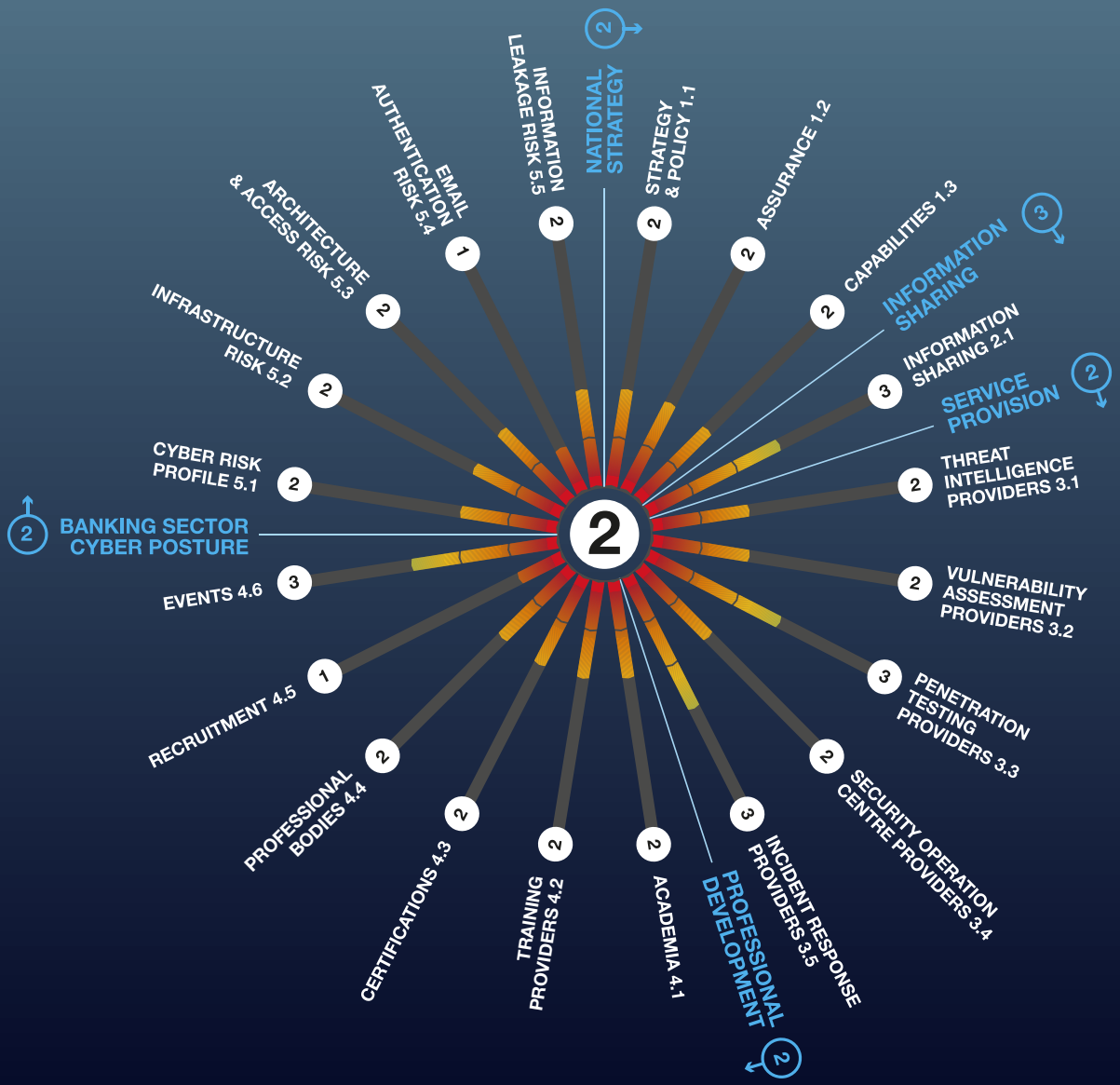
Maturity Scores

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

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

Highlights Report

Summary of Observations (continued)



Maturity Levels

1 Emerging
2 Transitional
3 Organised
4 Dynamic
5 Leading

Summary Assessment

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

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

Uganda's National Information Security Strategy was published in 2011.

Without an up-to-date national cyber security strategy, it is difficult to know where to focus activities.

The de facto government lead for cyber security is the **National Information Technology Authority (NITA-U)**. Hopefully, it can utilise this **CMAGE** assessment to focus activities and use the good practice guidance to provide practical support.

The Bank of Uganda's most recent annual supervision report acknowledges increased cyber risk across the banking sector.

However, as with other countries in the region, it does not appear to have effective tools to supervise cyber risk across the sector.

Uganda's 2011 Computer Misuse Act and 2019 Data Protection and Privacy Act are useful tools when it comes to tackling cyber crime.

The establishment of the **Ugandan Police Force's Electronic Crime Counter Measure Unit** is also positive news, but scale of investment in investigation or prevention of cybercrimes is unclear.

In Practice

There was no evidence of an intervention programme to divert young people with talent away from involvement in cybercrime. Good practice from other countries could help speed the development and effectiveness of this unit.

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 2

Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

CERTs & Information Sharing

Research identified two Ugandan Computer Emergency Response Teams (CERTs), **CERT-UG and Ug-CERT. This is encouraging.**

CERT-UG is the national CERT, sitting within the **National Information Technology Authority (NITA-U)**. **Ug-CERT is part of the Uganda Communications Commission**, with a primary focus on the telecommunications sector.

Both CERTs already have some cross-border links but would undoubtedly benefit from increased international collaboration. Apart from the telecommunications sector, a lack of focus on information sharing in other critical sectors, such as financial services, is apparent.

Dimension 2

Cyber Security Information Sharing

Maturity Level 3

Highlights Report

Key Observations - Dimension 3 - Cyber Security Service Provision

Uganda has a good mix of local, regional and international providers of cyber security services across most of the five disciplines.

Provision of Threat Intelligence and Security Operations Centre services are the least developed sectors.

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

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

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

Opportunity

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

Dimension 3

Cyber Security Service Provision

Maturity Level 2

Highlights Report

Key Observations - Dimension 4 - Cyber Security Professional Development

While many Ugandan universities and colleges provide computer science and ICT courses, very few offer specific cyber security qualifications.

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

Utilising international good practice, Uganda could build upon its currently available range of computer science and ICT courses to support creating more specific cyber security courses and qualifications.

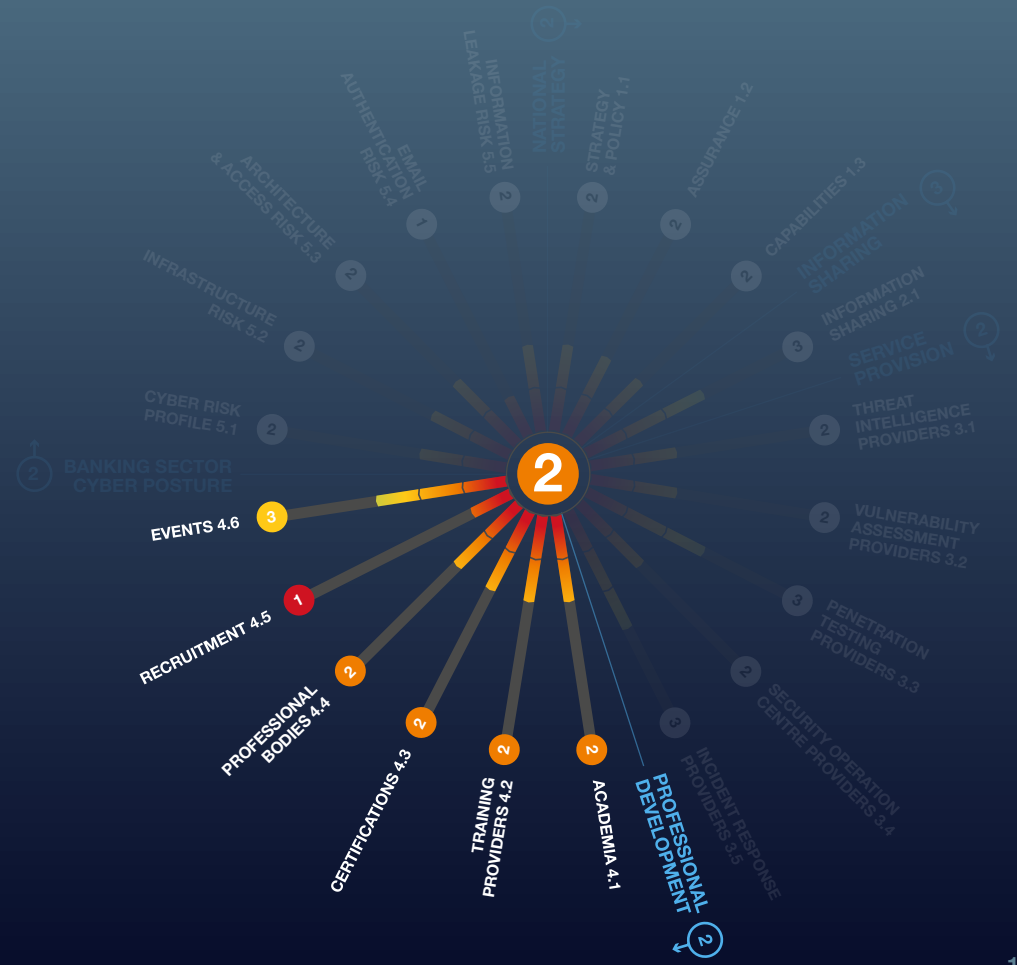
There are opportunities for developing an academic cyber security research capability in Uganda, increasing the country's capacity for forward thinking in this important field.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 2



Highlights Report

Key Observations - Dimension 4 (continued)

A good mix of in-country and international cyber security training providers were identified.

More local cyber security training providers would expand opportunities for people to train at affordable cost and help develop the professional cyber security community.

It is unclear how many existing training courses lead to internationally recognised qualifications.

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

CREST's research reveals a lack of importance attached to using certifications to encourage and retain the most talented people into the industry.

The cost of some professional certificates may be prohibitive.

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

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

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

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

The number of in-country and regional cyber-related events that took place in 2019 and early 2020 is very encouraging evidence of a developing community of interest in cyber security matters.

There is little evidence of any in-country cyber security specialist recruitment.

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

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

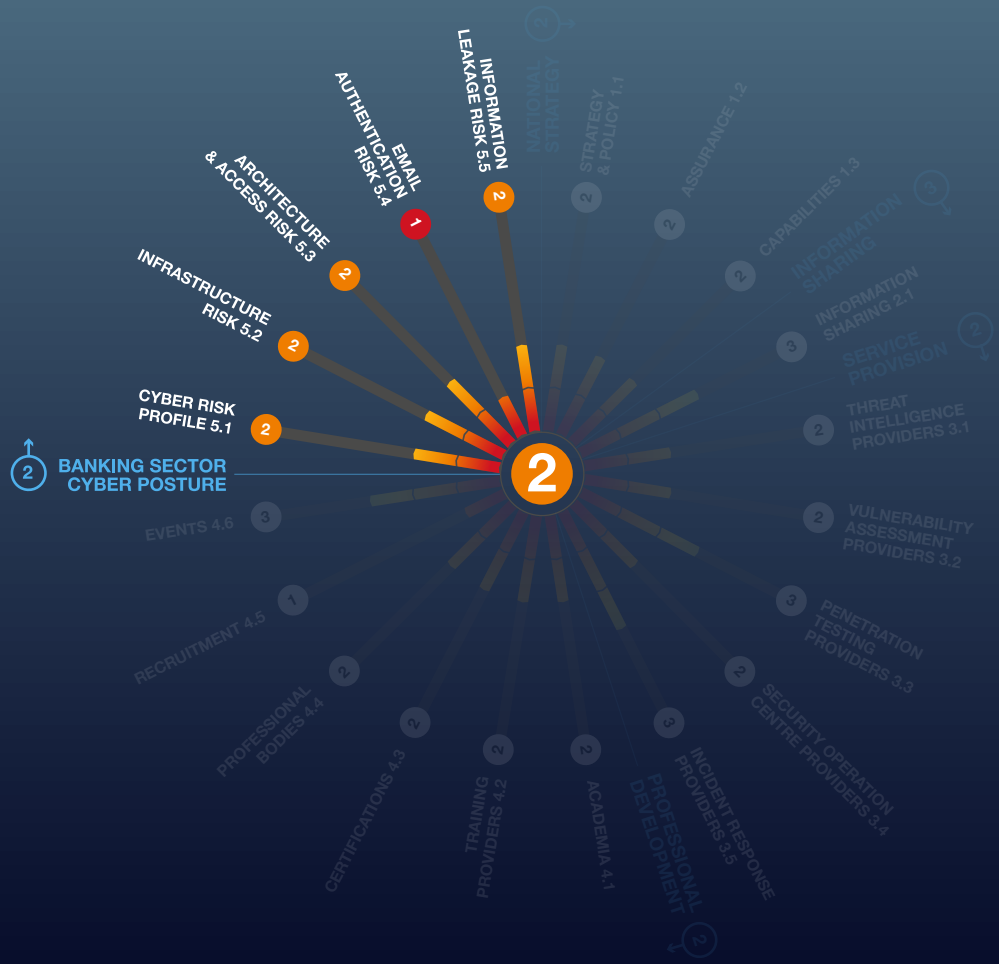
Uganda's regulators can utilise this assessment to focus attention and highlight areas for review, provide access to the supporting guidance being developed and, where appropriate, encourage take up of technical security measures to improve cyber resilience.

Continued on next page...

Dimension 5

Banking Sector Cyber Security Posture

Maturity Level 2



Highlights Report

Key Observation - Dimension 5 (continued)

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

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

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

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

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

Passive external assessments were conducted on the public-facing IT infrastructure of a sample of 34 financial institutions. For obvious reasons, all results were anonymised.

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

CREST assessed the general threat to Uganda's financial institutions is lower than for larger institutions in more advanced economies. Yet some of Uganda's financial institutions still attract a significant threat score.

35% Overall, **35%** were awarded a risk rating of 'Very High' or 'High', indicating Maturity Level 2 for Risk Profile.

5% Just **5%** of the sample had evidence of critical vulnerabilities within their infrastructure.

47% A further **47%** appeared to be carrying non-critical vulnerabilities. This indicates Maturity Level 2 for Infrastructure Vulnerability Risk.

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

32% Some **32%** appeared to have one or more database ports open, leading to the award of Maturity Level 2 for this risk category.

45% Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **45%** of the sample.

53% Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **53%** of the sample. Our research indicates Maturity Level 1 for Email Authentication Risk.

73% In **73%** of sampled institutions, at least some staff data was available online because of third-party data breaches, indicating Maturity Level 2 for Information Leakage Risk.

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

Highlights Report

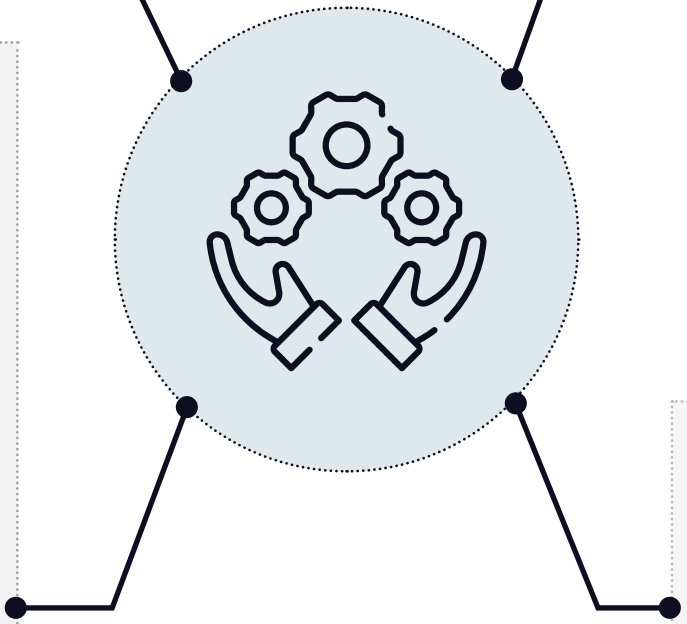
2021 Good Practices Guides and Tools

Goverment Strategy Policy

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

Service Suppliers

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



Training and Academia

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

Security Postures

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

Introduction

Introduction

Background

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

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

CREST International

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

Introduction

Research Methodology

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

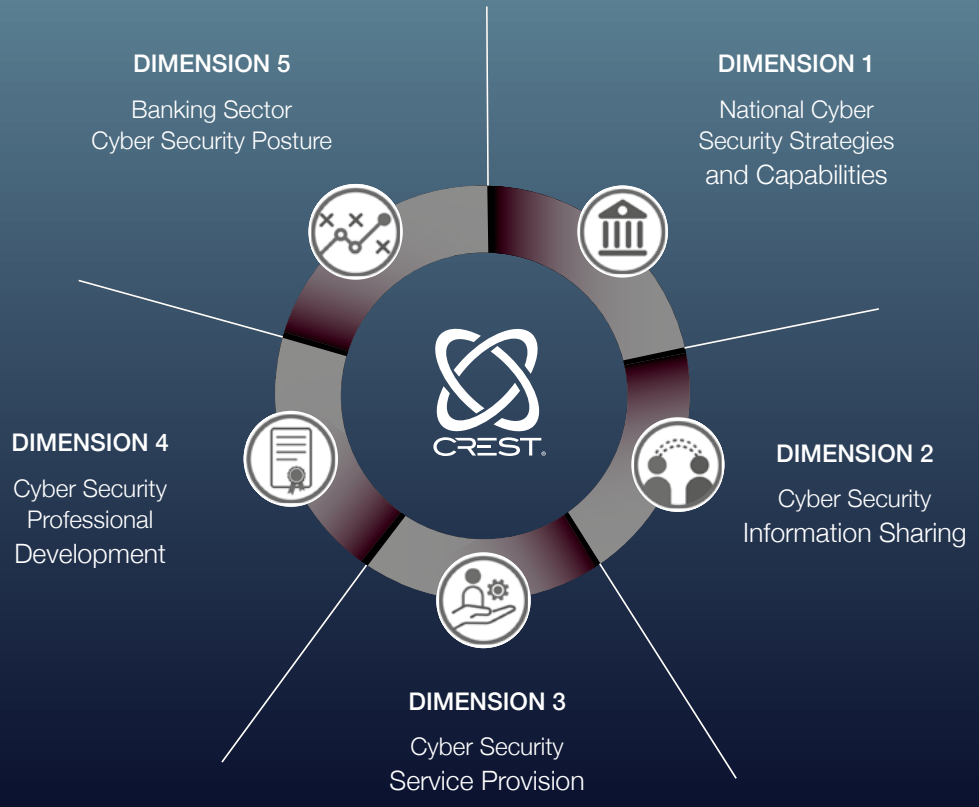
10. In terms of banking sector cyber security posture, CREST worked with **Orpheus Cyber**[3], a leading cyber threat intelligence service provider, to carry out a passive (non-intrusive) external assessment of the public-facing IT infrastructure from a sample of the country's financial institutions.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

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

CMAGE Structure

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

The CMAGE is based on assessment of twenty separate Indicators across five Dimensions. The five Dimensions are depicted diagrammatically in the image below.



Introduction

Maturity Level Definitions

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

16. The complete listing of the Dimensions and their associated Indicators is shown in the table, right. A full listing of the five maturity level definitions for each indicator can be found at **Appendix B.**

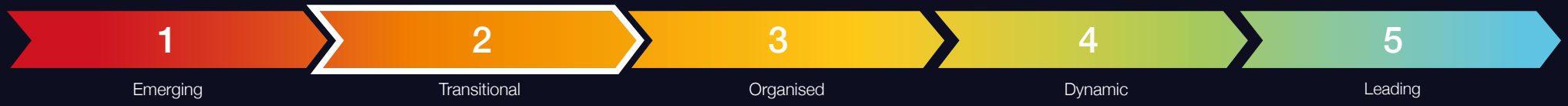
DIMENSION		INDICATOR	
QUALITATIVE ASSESSMENT			
1	National Cyber Security Strategy & Capabilities	1.1	Government Strategy & Policy
		1.2	Regulator/Government Operated Assurance Schemes
		1.3	Law Enforcement & Cyber Defence Capabilities
2	Cyber Security Information Sharing	2.1	Computer Emergency Response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

Dimension 1

National Cyber Security Strategy & Capabilities

National Cyber Security Strategy & Capabilities

Overall Dimension Assessment: *Maturity Level 2*



National strategy is of vital importance.

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

18. Academia and professional training providers would struggle to know what courses to provide; and potential students would face difficulty in understanding career options. It would also be tough to justify and target research.

19. Public and private sectors would have no guidance or framework to base their cyber security policies on, and ultimately, a lack of national strategy would undermine economic growth. Examining a country's **National Cyber Security Strategy** provides good insight into its willingness to implement cyber security measures and tackle cybercrime. In short, a national cyber security strategy sets standards for all other sectors to follow.

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

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

21. **The Ugandan Government's National Electronic Government Policy Framework** provides an overarching legal and regulatory framework that all member institutions must comply with[4]. The two primary institutions named in this framework are the **Ministry of Information and Communications Technology (ICT)** and the **National Information Technology Authority Uganda (NITA-U)**.

22. The Ministry of ICT's responsibilities include providing strategic and technical leadership for the ICT sector, ICT legal and regulatory environment, and secure ICT access and usage[5].

23. NITA-U, established in 2009, is responsible for coordination and regulation of ICT services in Uganda[6]. The National Information Security Advisory Group (NISAG), established in 2014, sits within NITA-U; it advises the government on information security governance matters[7], and in 2014 mandated the creation of a National Computer Emergency Response Team (CERT UG)[8] under NITA-U. NITA-U develope NISF) and has subsequently pr 2014[9].

24. **The Global Cyb Capacity Review of the Republic** ber security strategy in Ugan ity Policy is being used. As there is budget, each ministry must all y[11].

[11] Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Review of the Republic of Uganda', Oxford, Author, 2016, p8, **https://gcscc.web.ox.ac.uk/files/ugandacmmpdf** (accessed July 2020)

National Cyber Security Strategy & Capabilities

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

Both the Ministry of ICT and NITA-U are key to providing national cyber and information security.

25. Five other institutions are also listed in the National Electronic Government Policy Framework:

Together, the seven institutions enable a comprehensive electronic governance regime. However, there does not appear to be one overarching National Cyber Security Strategy or policy, and little evidence found of other organisations having their own cyber security policies.

26. The Uganda Communications Commission[12], one of the agencies of the Ministry of ICT, has a mandate which covers The Ugandan Institute of Communications & Technology (UICT), an agency of the Ministry of ICT, and the only government institution specializing in skills-based middle-level ICT training[13].

27. In addition, the Ugandan Communications Commission (UCC), together with The Rural Communications Fund (RCDF) and in partnership with the Ministry of Education and Sport, implemented a programme for integrating ICT into education in Uganda[14].

28. The programme's 2014 report indicated a substantial number of ICT laboratories had been established in schools, colleges and universities[15], with more pending. A more recent update did not appear to be available.

29. This is a positive move to improve ICT education throughout the education systems and in civil society, as it will lead to more qualified ICT and cyber security professionals in future. More information on cyber security professional development can be found in **Dimension 4**.

Overall Assessment

30. The Computer Misuse Act 2011, The Electronic Signatures Act 2011 and The Electronic Transactions Act 2011, (classed as Uganda's National Cyber Laws), combined with the establishment of the National Information Technology Authority (NITA-U) and CERT-UG, are useful legislative tools to tackle cybercrime.

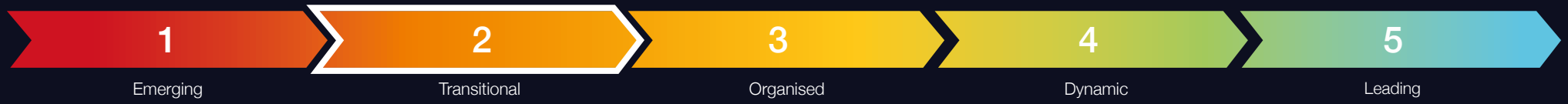
31. However, as part of the research, there was no evidence of a specific national cyber security strategy or policy. Nor did the research identify any of the organisations, such as the Bank of Uganda or the Ugandan Police, having their own cyber security strategy or policy publicly available. Most activity in bringing in new legislation and establishing organisations to focus on cyber/information security seems to have been between 2011 and 2014. The most recent policy found which links to cyber and information security is the **2019 Data Protection and Privacy Act**[16].

32. A review of cybercrime is covered in the Ugandan Police Annual Crime Report 2019 and more general detail on cybercrime can be found in Appendix D of this report. Some resources are clearly being committed to tackling cybercrime and improving Uganda's national cyber security posture, but the facts and figures could not be identified during research. Nor were plans identified to establish government/regulator-operated assurance schemes to underpin security standards in the financial services sector or other critical areas of national infrastructure.

33. Development approach: Enhancements to law enforcement and cyber defence capabilities should be considered a priority. This should include measures to enlarge the pool of cyber talent available to the government and private sector.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy



Assessment – *Maturity Level 2*
Some evidence of up-to-date strategies and policies aimed at improving the country's cyber security posture and/or capabilities.

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

34. The research sought information on publicly available strategic level policy and legislation relating to national cyber/information security, how up to date it is, and which agencies were empowered to uphold it

35. **The legal and regulatory framework of the National Electronic Government Policy Framework is as follows**[18]: The Computer Misuse Act 2011[19], which provides for the safety and security of electronic transactions and information systems; The Electronic Signatures Act 2011[20], which legalises the use of electronic signatures, and The Electronic Transactions Act 2011[21], which provides for the use, security, facilitation and regulation of electronic communications and transactions. These three acts are described as the national cyber security laws by the Ministry of ICT and quoted by the Bank of Uganda in March 2013 as being the cyber laws it needed to comply with[22]. While all three acts are important, the Computer Misuse Act and Electronic Transactions Act are more aligned with cyber security than the Electronic Signatures Act.

36. Additionally, The National Information Technology Authority Act 2009[23] is the establishment act of the National Information Technology Authority (NITA-U) that sits within the Ministry of ICT. It is also is the parent body for the Ugandan National Computer Emergency Response Team (CERT-UG) and part of the National Electronic Government Policy Framework.

37. The information security page[24] on the government of Uganda's Ministry of ICT and National Guidance website reflects the National Electronic Government Policy Framework.
It lists the Computer Misuse Act 2011, the Electronic Signatures Act 2011 and the Electronic Transactions Act 2011 in its suite of cyber laws and legal frameworks which deal with cybercrime. The National Information Security Framework (NISF)[25] and The Ugandan National Computer Emergency Response Team (CERT-UG) are also mentioned as part of the legal framework.

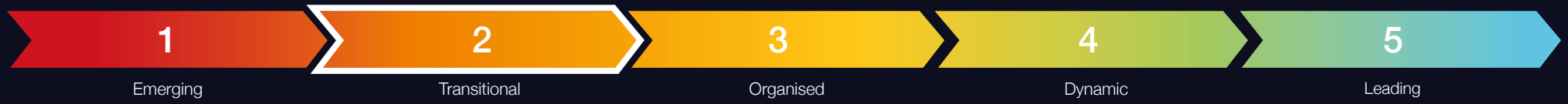
38. CERT-UG does not operate in isolation. Although not mentioned in any of the national frameworks or policies above, there is also a Ugandan Communications Sector Computer Emergency Response Team UG-CERT[26]. There is more detail on both CERTS in Dimension 2 – Cyber Security Information Sharing.

39. The most recent act, mentioned by both the Ministry of ICT and NITA-U on their websites, which adds to the suite of laws available to deal with cybercrime, is the Data Protection and Privacy Act 2019. This act aims to protect the privacy of the individual and of personal data[27].

40. Despite various legislative acts, published policies and organisations established, which all add value to national cyber security, no one specific national cyber strategy or law could be identified. Much of the activity in establishing some degree of national cybersecurity strategy took place between 2011 and 2014, except for the Data Protection and Privacy Act in 2019.

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



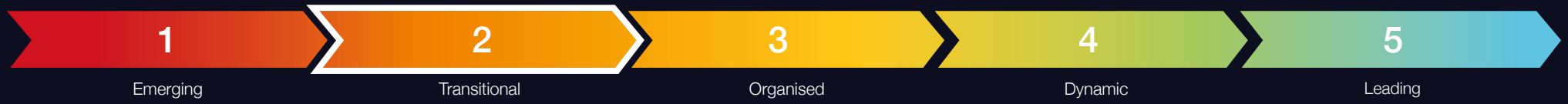
Assessment – *Maturity Level 2*
Central Bank (and/or other financial services regulators) maintain accurate records. Some evidence of good regulation of financial services sector. Little evidence of regulators operating in other sectors.

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

41. The research focused on looking for any publicly available policies and laws which support and uphold financial ethics, integrity and cyber security.
42. The Ministry of Finance, Planning and Economic Development (MoFPED) of the Republic of Uganda, affiliated with the Bank of Uganda, has several policies for financial regulation and management, though non-specific to cyber security[28]. The MoFPED has five directorates. One is the Directorate of Internal Audit, which includes an Information Technology and Performance Audit Department that reviews and reports on actual and potential security threats affecting the national IT system[29].
43. No specific Bank of Uganda policy on cyber security was found during the research. However, evidence of the Bank of Uganda seeking consultancy services[30] in 2013 to assess the Bank's compliance to Ugandan cyber laws, as mentioned previously, was found. The Bank co-hosted a workshop on Cyber Security in the Financial Sector with the Macro-economic and Financial Management Institute of Eastern and Southern Africa (MEFMI)[31] in March 2020.
44. Uganda's Ministry of Finance and the Bank of Uganda are both members of the MEFMI[32], one of 14 member States. The MEFMI has cyber security information on its website[33], mostly relating to various cyber workshops.
45. The Financial Intelligence Authority (FIA)[34] was established in 2013 by the Anti-Money Laundering Act 2013[35], to identify and combat money laundering activities and crime. It oversees compliance with numerous government Acts as listed in its publications page[36]. The Anti-Money Laundering Act 2013 does not mention cybercrime, though it covers electronic funds transfers[37], which, if illegal, could constitute a cybercrime. Of note, as a strategic level organisation, the FIA has no specific cyber security policy or reference to cyber security in relation to the financial sector on its website.

National Cyber Security Strategy & Capabilities

Indicator 1.3 Law Enforcement & Cyber Defence Capabilities



Assessment – *Maturity Level 2*
Some reporting of cybercrime and its impact. Evidence of investment in law enforcement capabilities to tackle cybercrime. Evidence of some strategy/policy/legal support for tackling cybercrime. Some public awareness. Evidence of some government and military interest in cyber defence matters. Little evidence of specific measures within the financial services sector to tackle cybercrime.

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

47. **Serianu's Africa – Cyber Security Report 2016**[38] and its **Africa Cyber Security Report - Uganda - Cyber Security Skills Gap 2018**[39] both give detail of the economic size and effects of cybercrime in Uganda, as does an article by the Forensic Institute and ICT Security[40], although these reports are most likely to only be read by cyber professionals.

48. The Daily Monitor[41] news site has published a few articles on cybercrime. An article dated March 2014 is no longer accessible online via the Daily Monitor but can be found via Unwanted Witness[42]. Other articles publicly reporting cybercrime were also found online in The Observer[43], New Vision[44] and on the websites of the African Centre for Media Excellence[45], a not-for-profit organisation, and Unwanted Witness[46], a civil society organisation, both Kampala-based.

49. **The Ugandan Police Annual Crime Report 2019**[47], available publicly, reports activities in relation to cybercrime and what cybercrime has been reported to the police. It also reports the activities of its Directorate of Forensics Services and Department of Cybercrime and Digital Forensics[48]. More detail on cybercrime statistics can be seen in **Appendix D Country Context.**

50. The Ugandan Police has taken several initiatives towards tackling cybercrime. Around 2008, it formed the Directorate of ICT[49] , to ensure the Police adhere with national policy. It is believed[50] to have established a Cybercrime Unit in 2015, and an Electronic Counter Measure Unit[51]. The only evidence of the latter is from other media sources, not via publicly available information from the Ugandan Police.

51. However, a Ugandan Police Cybercrime[52] Barometer was launched in 2017 and is publicly available. It has a few articles, aimed at the general public, providing information about internet and information security. While the Ugandan Police is dealing with cybercrime, it does not have a Cyber Security Strategy and Policy available.

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.

52. There is no commercial advantage to be gained by not sharing information. The open publication of academic research and the use of sector-specific information exchanges are two mechanisms for sharing information on cyber security risks, threats and vulnerabilities. There is not much evidence of either of these mechanisms being currently well-established in Uganda.

53. Information sharing enables the spread of best practice. CREST research focused on looking for expert groups such as **Computer Emergency Response Teams (CERTs)**, which, as a team of information/cyber security experts, handle protection against and detection and response to cyber security incidents. They provide cyber security services, as well as running cyber security awareness campaigns or events for organisations and the 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.

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

Overall Assessment

55. Uganda has two CERTS, the Ugandan National Computer Emergency Response Team (CERT-UG)[53] established by the National Information Technology Authority - Uganda (NITA-U) in 2014[54], and the Uganda Communication Sector Computer Emergency Response Team (Ug-CERT), established in 2013 by the Ugandan Communications Commission, in partnership with the International Telecommunications Union (ITU)[55]. Both CERT-UG and Ug-CERT appear to be well established with respective international and regional links.

Development Approach

56. The establishment of a CERT focused on the financial sector would help strengthen information sharing between banks and other financial instructions.

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.

57. **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)

58. Of Uganda's two CERTs, Ug-CERT is partnered with the Forum of Incident Response and Security Teams (FIRST) which has an international membership of CERTs[56]. FIRST provides global collaboration for its member teams and ensures no team operates in isolation. Because Ug-CERT is a member of FIRST, it meets the ENISA Maturity Model Tier 2 requirements[57].

59. Both Ug-CERT and CERT-UG are members of the Africa CERT[58] which helps and encourages cooperation and collaboration between its members. Establishing CERTs with regional and international links, which enable collaboration and continued growth, is a positive step for cyber security in Uganda.

60. The Global Cyber Security Capacity Centre's 'Cybersecurity Capacity Review of the Republic of Uganda 2016' mentions that Uganda has a military CERT, though no further publicly available evidence of this CERT was identified during research[59].

61. It was encouraging to see that Ugandan regulators and service providers are members of the six-country East Africa Communications Organisation (EACO). One of EACO's objectives is to develop guidance on addressing cyber security issues and to produce an annual report on cyber security, although none appear to have been produced to date.

62. **Six organisations** that could be classed as information sharers were identified during research.

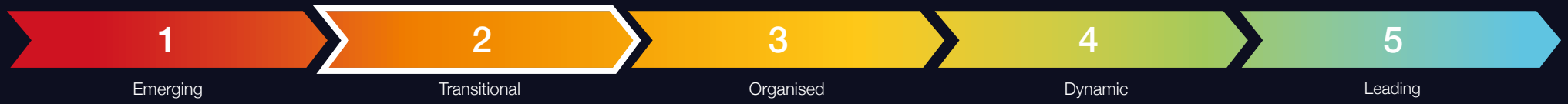
63. **Four were international organisations, one was a regional think-tank, one was based in Kampala.** This is positive for cyber security professionals and good in terms of raising awareness of cyber security within Uganda.

Dimension 3

Cyber Security Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 2*



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

64. Research into how cyber security services are currently provided in Uganda quantified cyber security service providers, examined what services they offered, what accreditations they held, and what accredited services and certifications they provided.

65. The location of company offices and customer reach were also recorded

CREST asked:

- Are they local companies, registered and only based in Uganda?
- Are they regional, registered in another African country, but with offices and the ability to reach regional customers?
- Or are they a large international organisation, with multiple global office locations which may be located in-country?
- If not, can they deliver services in Uganda without having a permanent physical presence there, or anywhere in Africa?

When examined together, all of these factors combined give an idea of the maturity of the cyber security industry.

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

Overall Assessment

67. There are some locally-registered companies in each service category except Security Operations Centres (SOC). While provision of Penetration Testing and Incident Response Services in Uganda is judged to be at Level 3; the availability of Vulnerability Assessment, SOC and Threat Intelligence service providers is much more scarce. Currently, there are **three CREST International accredited member companies** with local offices in Kampala, but there are no local CREST member companies.

Development Approach

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

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers

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

Assessment – *Maturity Level 2*

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

Cyber Threat Intelligence

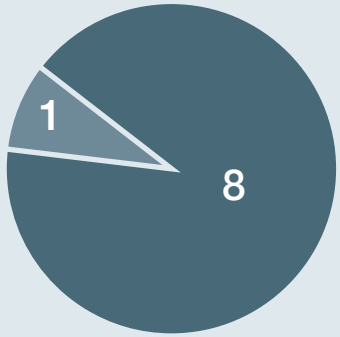
69. Cyber threat intelligence is information about current and future cyber threats and actors that adversly affect a nation's or individual organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks[60]. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark-side sources.

70. The research looked for companies providing cyber threat intelligence services to Ugandan organisations and where these services were provided from. For the purposes of a robust cyber security environment, the ideal is a host of Uganda-based threat intelligence service providers. Evidence of quality, through any accreditions or partnerships these companies may have, was also sought.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	1	2	3
Regional	1	0	1
International	1	8	9
Total	**3**	**10**	**13**

71. There are **13 companies offering threat intelligence services** in Uganda. **Three are based in Uganda, two are CREST-accredited international companies** with offices in Kampala, and one is headquartered in Kenya. There is one international company based in Africa which provides its services to Kampala, Gulu, Lira, and Mbarara.

72.



Of the **nine international organisations** that provide services into Uganda, **eight are CREST-accredited**.

It is not confirmed how frequently the threat intelligence services of these international organisations are being used.

73. One of the international organisations providing support into Uganda is the Forum of Incident Response Teams (FIRST), which has the Ugandan Computer Emergency Response Team (Ug-CERT) among its members.

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment Providers

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

Assessment – *Maturity Level 2*

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

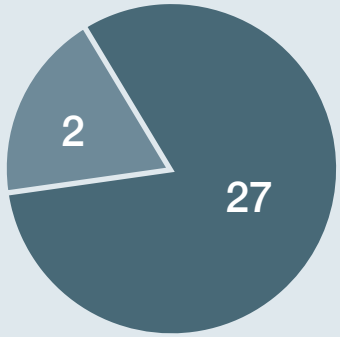
Vulnerability Assessment (VA)

74. Vulnerability Assessment (VA) is defined by CREST as: "the examination of an information system or product to determine the adequacy of security measures. 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 implementation[61]".

75. 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	5	2	7
Regional	4	0	4
International	2	27	29
Total	**11**	**29**	**40**

76. CREST's research found **40 companies providing Vulnerability Assessment (VA)** services into Uganda. **Seven companies operate in-country, two of which are CREST-accredited**. Regionally, there are **four non-CREST-accredited companies offering VA services into Uganda**.



There are **29 international companies offering VA services** into Uganda from international offices elsewhere, **27 of which are CREST accredited members**.

Cyber Security Service Provision

Indicator 3.3 Penetration Testing Providers

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

Assessment – *Maturity Level 3*

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

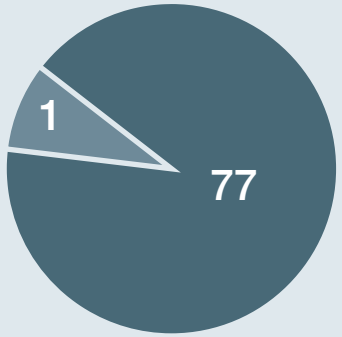
Penetration Testing

77. 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 [an] organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities[62]."

78. CREST's research found significantly more companies providing penetration testing than any other cyber security service, although many service providers provide more than one cyber security service. In assessing the maturity of the cyber industry, efforts focused on looking for Uganda-based service providers.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	4	3	7
Regional	2	2	4
International	1	77	78
Total	**7**	**82**	**89**

79. The research identified **89 companies providing Penetration Testing services into Uganda**. **Seven companies operate in-country**, of which **three are CREST-accredited**. Regionally, there are **four companies providing services into Uganda, two of which are CREST-accredited**.



There are **78 international organisations providing penetration services into Uganda** from international offices, **77 of which are CREST-accredited**.

Cyber Security Service Provision

Indicator 3.4 Security Operation Centre Providers

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

Assessment – *Maturity Level 2*

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

Security Operations Centres

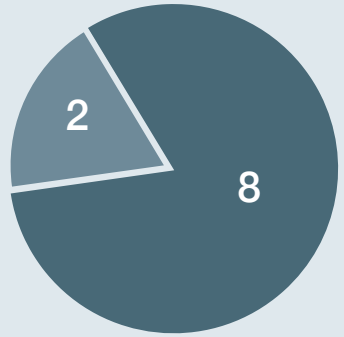
80. **CREST provides a detailed definition of Security Operations Centres:** "An Information Security Operations Centre (SOC) is a facility where enterprise information systems (web sites, applications, databases, data centres and servers, networks, desktops and other endpoints) are monitored, assessed, and defended. Depending on the nature of the SOC, organisations may offer a variety of services including monitoring, detection, threat hunting, log analysis, incident management, forensic imaging, malware analysis, reverse engineering, mitigation advice and general good practice guidance.

"A range of response options may be available, from telephone or email triage through to onsite assistance as required. Where such services are not available within the organisation, the SOC will know where and how to procure appropriate services from third parties[63]."

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	0	1	1
Regional	1	1	2
International	2	8	10
Total	**3**	**10**	**13**

81. 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.

82. There are **13 companies that can provide Security Operations Centre services into Uganda.** Only **one operates in-country,** and it is a CREST-accredited international company. **There are two regionally-based companies.**



Of **10 international companies**, **8 are CREST-accredited companies** which offer their services into Uganda at clients' request.

Cyber Security Service Provision

Indicator 3.5 Incident Response Providers

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

Assessment – *Maturity Level 2*

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

Incident Response Providers

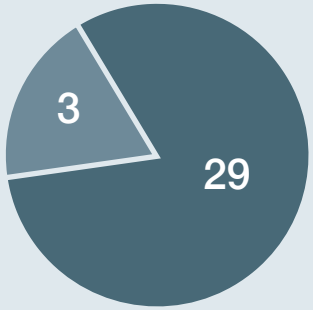
83. Incident response to a cyber security issue is defined by CREST as: "an information (or IT) security incident ...ranging from serious cyber security attacks on critical national infrastructure and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction[64]."

84. 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 in-house. Companies providing incident response services are a vital component of the cyber industry and the fight against cybercrime.

85. The number of incident response service providers based in-country is critical to the overall cyber maturity of the cyber industry in that country. There are **42 companies providing incident response services into Uganda**. Of the **eight companies that operate in-country**, **two are the Ugandan Communications sector's Ug-CERT run by the UCC**, and the **National CERT-UG run by NITA-U**. **A further two are CREST-accredited international organisations.**

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	6	2	8
Regional	2	0	2
International	3	29	32
Total	**11**	**31**	**42**

86.



There are **32 international organisations providing Incident Response Services into Uganda, 29 of which are CREST-accredited.** It is unknown how often these services are used by Ugandan clients.

Dimension 4

Cyber Security Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2*

88. Education and professional development are both critical in providing students, from school age to adulthood, with the skills and knowledge to thrive in the modern workplace.

89. Without ICT and cyber security being taught in the national education system and then available as part of professional development, it is difficult to attract young people into the cyber security industry and to train as professionals.

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

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

92. CREST looked at what professional membership organisations were doing to improve the cyber profession. CREST studied recruitment channels to identify cyber security roles advertised and cyber security freelancers promoting themselves, to ascertain the vibrancy of the cyber security job market.

93. The Ugandan Communications Commission and The Ministry of Education and Sports have a programme for integrating ICT into education in Uganda[65]. A 2014 report on the programme claimed that Uganda is the only African country to have declared computer studies a compulsory subject. At the time, the country had rolled out **ICT Laboratories to 1027 government secondary schools, 43 tertiary institutions - including all National Teachers' Colleges, nine universities, and more to the civil community and health centres**, although not all had an internet connection[66].

94. During the literature review on the cyber security profession in Uganda, several articles and reports provided deeper context to education and professional development in Uganda. Details of this can be found in **Appendix D**.

Overall Assessment

95. The number of computer science courses offered by academia is encouraging, however the security content of most appears to be minimal. With some exceptions, there is also a general lack of specialist in-country training and certification opportunities.

96. Little cyber-specific recruitment activity was identified during the research - not a good indicator of vibrance in Uganda's cyber security industry. But the variety of cyber security-related events that took place in 2019 is very encouraging and points to a real appetite for knowledge and community. The existence of local chapters of the Information Systems Audit and Control Association (ISACA) and The International Information System Security Certification Consortium (ISC)2 is also a positive sign.

Development Approach

97. Partnerships between local universities and renowned institutions elsewhere could improve cyber security education opportunities. Increasing reachout to the school aged population and university students to educate them about the benefits of cyber security courses and following a career in cyber security would reap benefits. Investment certifications would also improve matters considerably.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education

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

Assessment – *Maturity Level 2*

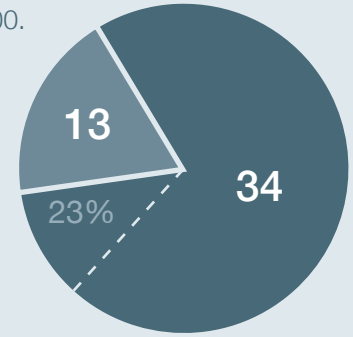
In addition to computer science degrees, evidence of some cyber security degrees (BSc, MSc, and PhD) and some research.

Academia and Higher Education

98. 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.

99. CREST's research sought to identify the universities and colleges offering ICT or cyber courses and modules to their students, and what level the courses were at – diploma, degree or masters, for example. The more students graduating with ICT or cyber-related degrees, potentially result in more people following an ICT-related career.

100.



Of the **47 universities in Uganda**, **34 offer ICT-related courses**, of which **23% offered cyber security courses**, or some cyber security content.

One university was found to have published a research paper on cyber security.

	Cert	Diploma	BA/ BSc	Pg Dip	MSc	PhD	Total
ICT Courses	12	23	59	7	17	2	120
Cyber Cources	10	0	2	1	2	0	15
Total	**22**	**23**	**61**	**8**	**19**	**2**	**135**

101. The table above shows approximate numbers of courses offered from the 34 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.

Cyber Security Professional Development

Indicator 4.2 Training Providers

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

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

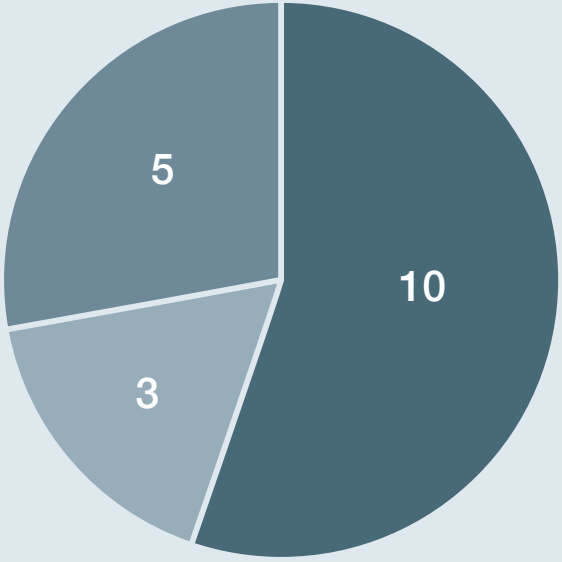
102. Training providers are qualified to provide training via an established course to clients in a particular subject matter area. CREST's research sought to identify the number of training providers, where they were located and what cyber courses they were providing.

103. Eighteen training providers were identified during CREST's research:

- 10 Ten are **based in Uganda**
- 3 Three are **regionally based**
- 5 Five are **international training providers**

There is a good mix of physical and online courses being offered to Ugandans and the level of cyber-related courses ranges from professional certifications to Higher National Diplomas. The majority offer courses to adults, except for Cyber School Technology Solutions Ltd, which offers online tutorials for children and schools. The ACIC outreach programme offer of education and training to high schools, university campuses and corporate clients is a promising initiative.

Ugandan Training Providers by location



Cyber Security Professional Development

Indicator 4.3 Professional Certifications

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

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

104. 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**.

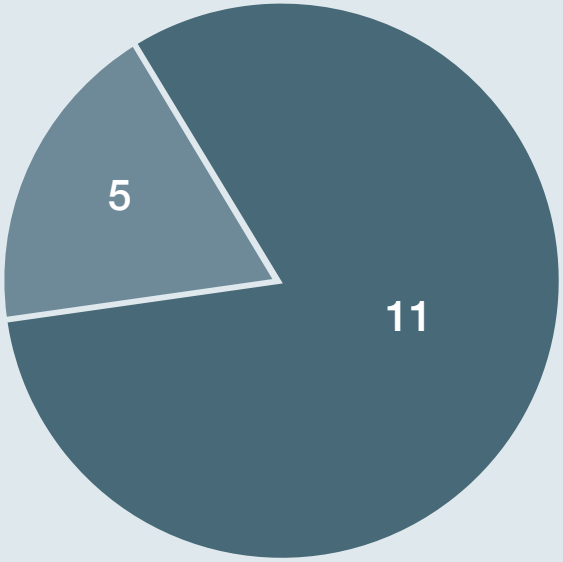
105. Of the 15 training providers offering professional certifications in Uganda:

- 11 Eleven are **internationally based**
- 5 Five have **regional offices**

Candidates can take physical exams at either of the two Pearson Vue centres in Kampala, or at a PSI test centre in either Kenya, Rwanda or online. There did not appear to be a PSI test centre in Uganda.

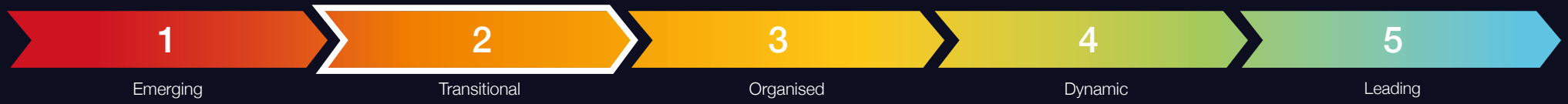
106. Other opportunities for online examinations exist. Most training providers did not offer statistics on the number of students successfully trained and certified, though from those that did, there seems to be low take up for certifications.

Professional Certification Training Providers



Cyber Security Professional Development

Indicator 4.4 Professional Cyber Membership Organisations



Assessment – *Maturity Level 2*
Some evidence of international cyber security membership bodies representing individuals and/or companies having local chapters/branches.

Professional Cyber Membership Organisations or Associations

107. Professional membership organisations or associations are usually focused on furthering the profession they represent. They provide membership by subscription and membership benefits include gaining access to further professional development and training, access to discounted products and events, networking and collaboration with like-minded people and increasing professional credibility because of membership.

    These organisations can frequently be not-for-profit organisations.

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

109.

There are **two international cyber security membership bodies operating in Uganda, ISACA and (ISC)2**, both in Kampala, with active chapters, hosting monthly meetings, training events and webinars, for example.

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment

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

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

Specialist Cyber Recruitment

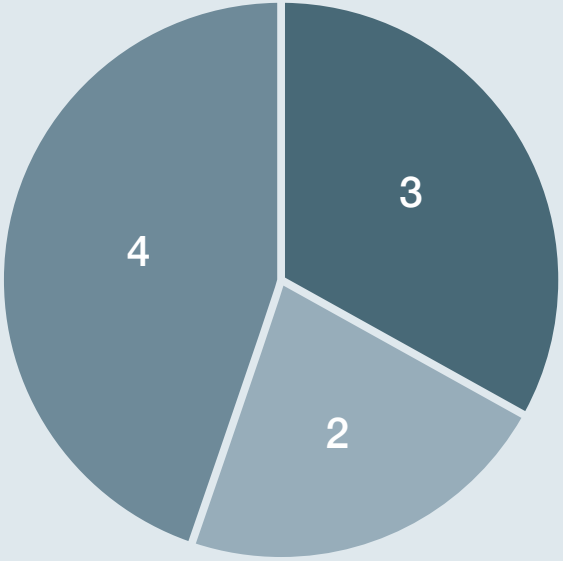
110. The presence and activity levels of recruitment companies and platforms provide evidence of how vibrant the job market is in a particular geographical area and/or industry sector. CREST's research looked for companies, online or with a physical in-country presence, that were either recruiting specifically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

111. No specific cyber-security recruitment companies were found during online research conducted. Nine generic recruiting companies were found, some with cyber security freelancers listed.

- 3 Three were **based in Uganda**
- 2 Two were **regionally based**
- 4 Four were **international organisations**

The overall impression is that the recruitment market for cyber professionals is not particularly vibrant.

Generic recruitment companies in Uganda



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

112. 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.
113. CREST's research looked for any cyber or information security events recently held in Uganda, what level of event they were and how frequently they were held. This provides evidence of an appetite for both cyber security knowledge and services.
114. The impact of these events can be far-reaching as they are effective hubs for networking, collaboration and information sharing, which helps to sow the seeds of cyber security inspiration.
115. CREST's research found **seven cyber security or information security events** between the summer of 2019 and 2020.

5 **All the events** took place in **Kampala** and **five were annual**

5 **Five** of those events were organised by **Ugandan cyber security organisations**

2 **Two** of those events were organised by **international organisations**

Of note, **The ITU Africa Regional Cyber Drill 2019** in Kampala was a high-level event, with teams representing 14 African countries, including Uganda. The participants were from government organisations, regulators, telecommunications operators, CERTs and other stakeholders.

Dimension 5

Banking Sector Cyber Security Posture

Banking Sector Cyber Security Posture

Overall Dimension Assessment: *Maturity Level 2*

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

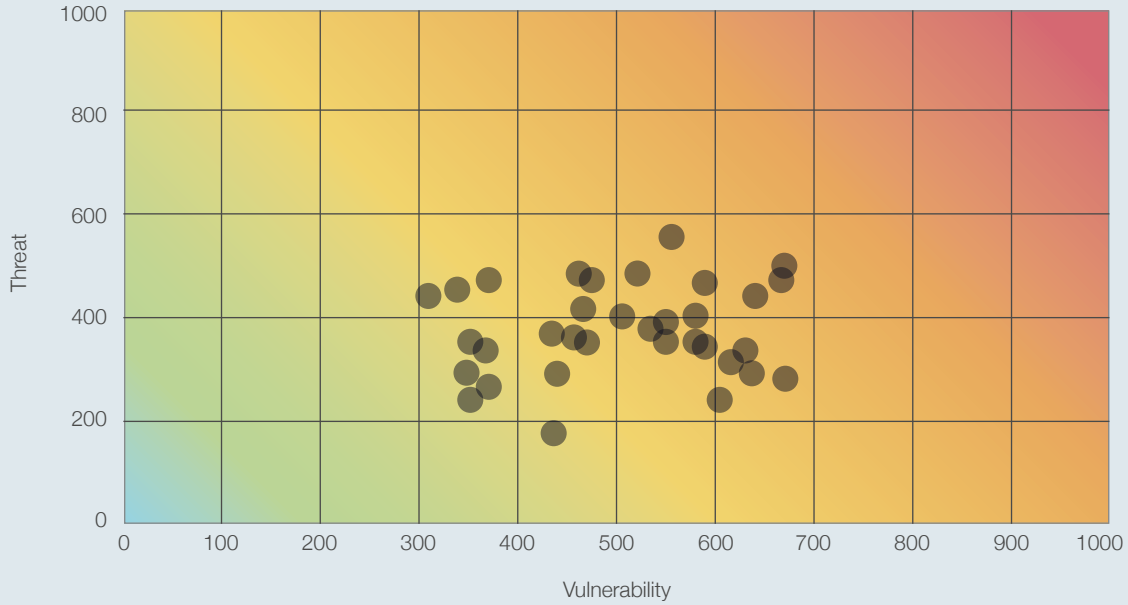
116. To assess the current cyber security posture of the Ugandan banking sector, CREST commissioned a leading cyber threat intelligence service provider, Orpheus Cyber, to undertake passive (non-intrusive) external assessments of the public-facing IT infrastructure from a sample of financial institutions.

117. 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.

118. 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.**

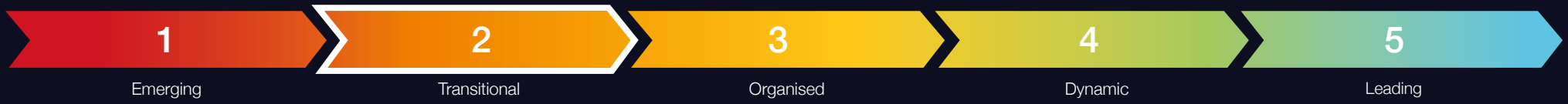
Comparative Risk Rating

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



Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile

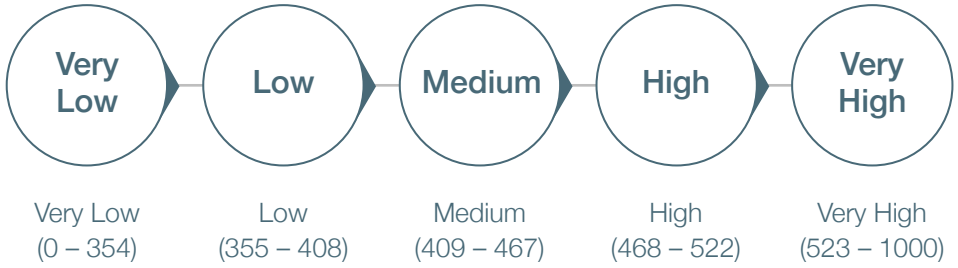


Assessment – *Maturity Level 2*
Banking sector cyber risk profile is assessed as poor; 30% or fewer of the surveyed financial institutions received a cyber risk rating of Very High and 55% or fewer received a rating of High or Very High.

Banking Sector Cyber Risk Profile

119. 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.

120. 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 310 and 672**. The **average cyber risk score** for the sample is **440**, which corresponds to a national average risk rating of '**Medium**'.

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

However, the levels of access that would have been required for such an undertaking are far beyond the scope of this report.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile (continued)

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

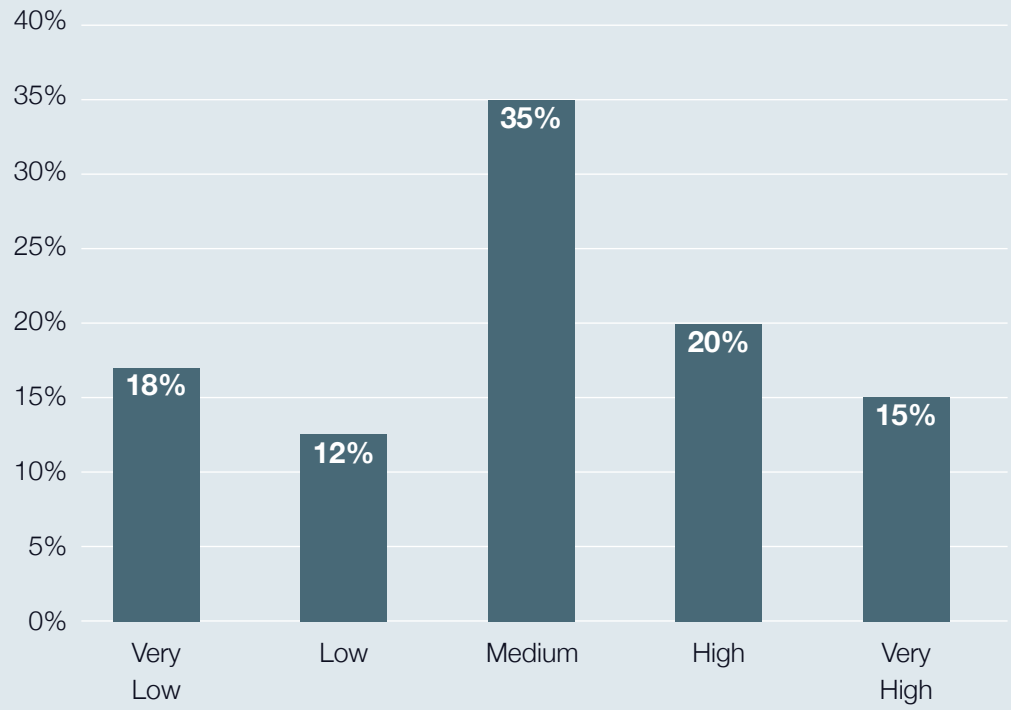
Assessment – *Maturity Level 2*

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

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

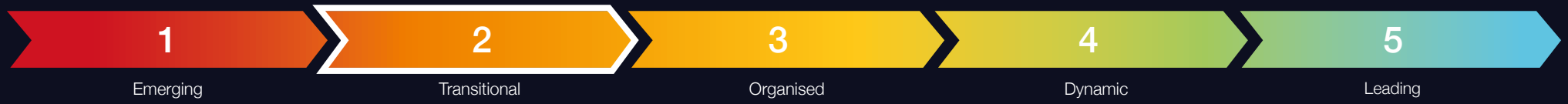
123. A breakdown by category of risk rating of the assessed sample of financial institutions is shown here, and the results anonymised. Encouragingly, 30% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'. But 35% have an overall cyber risk rating of 'Very High' or 'High'. Institutions in these latter two categories are not implementing good cyber hygiene practices and/or operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.

Breakdown of Uganda'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

124. Software patching and other routine housekeeping activities are essential tasks which must be carried out frequently and methodically to reduce opportunities for attackers. They are a good indicator of an organisation's enduring commitment to security. Ethically, research was limited to carrying out non-intrusive examinations of infrastructure elements directly connected to the internet. Formally, the results are similarly constrained, but it is reasonable to assume the research results are typical of the state of patching across each financial institution's complete IT infrastructure.

125. Vulnerabilities, often referred to as CVEs[68], (Common Vulnerabilities and Exposures) are flaws in software and hardware that cybercriminals constantly seek to exploit when attempting to gain access to the IT infrastructure of a chosen victim. To look for CVEs, they routinely scan portions of the internet.

    CREST's researchers followed a similar approach, scanning the public-facing IT infrastructure of all 34 of the Ugandan financial institutions being assessed. By restricting themselves to passive reconnaissance only, CREST's researchers were unable to confirm if the vulnerabilities they detected existed; there is a possibility that in some cases they were false positives.

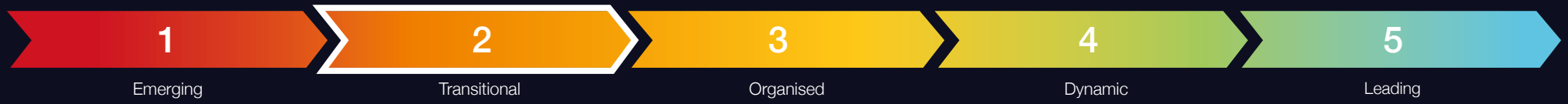
126. **The investigation revealed that 52% of Ugandan financial institutions appear to operate an unsecure internet-facing infrastructure that features at least one known vulnerability.** The vulnerabilities detected mostly have patches available. Their presence on an internet-facing infrastructure suggests lax patching practices.

127. Each CVE is analysed and assigned a severity score ranging from 0 to 10, with 10 being the most severe. This score is known by the acronym CVSS[69] (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.

128. **CREST's research identified that only 5% of the assessed Ugandan financial institutions were operating internet-facing IT infrastructure with at least one critical vulnerability.** In those financial institutions with critical vulnerabilities, these results are indicative of a failure to adopt an 'attacker's eye perspective' and prioritise critical CVEs for remediation.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk



Assessment – *Maturity Level 2*
Architecture & Access risk is poor; 20% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 40% or fewer were identified as having potential database vulnerabilities.

Architecture & Access Risk

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

130. In the context of computer infrastructure, ports are the 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 it is closed, it cannot. Certain ports need to be configured as 'open' to allow the server to perform. Traffic [data] going in and out of these ports can be guarded by mechanisms such as firewalls.

131. 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.

132.

Cybercriminals frequently look to **scan ports associated with remote access services** – hardware and software that allow authorised users to remotely access a computer or a network from a distinct network connection.

Cybercriminals favour **targeting remote access services** because, once compromised, they can easily move within a network and gain access to systems containing valuable information they can steal and/or encrypt.

Certain specialised cybercriminals also look to target remote access services and **gain access to bank networks**, with a view to **selling-on this access in online criminal forums and marketplaces**.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk (continued)

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

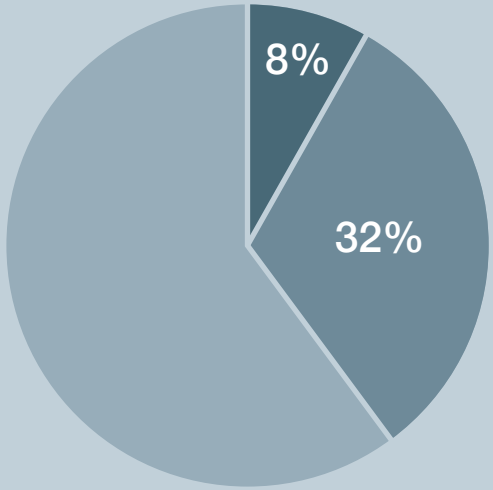
133. In most cases these ports will have been configured to accept incoming data packets from the internet for a valid business requirement and will have adequate security measures in place. Although those banks that have open remote access ports on their IT infrastructure remain susceptible to a potential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

134. Another set of ports on computer servers that cybercriminals often deliberately target are those used by database services. **CREST's research showed that 32% of the assessed financial institutions have at least one database-related port open on their public-facing infrastructure.** As above, although some of these internet-accessible database services are in place to meet valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.

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

136. Understanding the threat associated with exposed database instances - and reducing the possibility of suffering a data leak - would also reduce the risk of fines under **Uganda's Data Protection and Privacy Act 2019**[70].

Uganda's financial institution Access risk - open ports



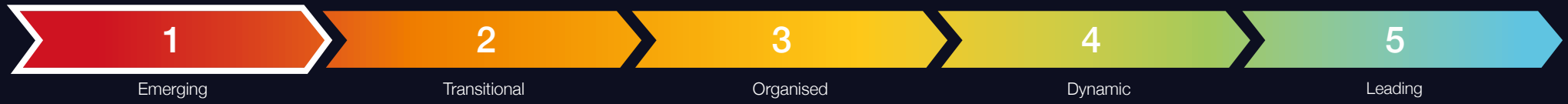
Key

8% - have remote access services open to the internet

32% - have at least one database-related port open to the internet

Banking Sector Cyber Security Posture

Indicator 5.4 Email Authentication Risk



Assessment – *Maturity Level 1*
Email authentication risk is assessed as very poor; more than 15% of the surveyed financial institutions had not correctly enabled basic email authentication measures (SPF) and/or more than 70% had not correctly enabled advanced email authentication measures (DMARC).

Email Authentication Risk

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

138. **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.

139. SPF is regarded as the minimum (basic) standard to safeguard against spoofing and impersonation. DMARC is a more advanced security mechanism that, when correctly enabled, signals a strong cybersecurity posture. While it is still not as commonly implemented as SPF, recent global statistics confirm DMARC implementation rates are growing, with a corresponding decline in domain spoofing[71].

140. Having SPF and DMARC correctly enabled does not entirely negate the threat from phishing. However, it reduces the chance of falling victim to impersonation attempts and **business email compromise (BEC) scams**. Both are common threats in the financial services sector[72].

141. 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**[73].

142.

45%

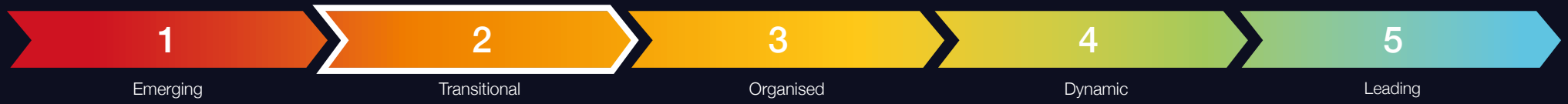
CREST's research revealed that **45% of the sample of financial institutions had not implemented basic email authentication measures (SPF)**.

53%

53% of the sample had not implemented advanced email authentication measures (DMARC). These results suggest there is still significant room for improving the financial service sector's defences against phishing and similar threats.

Banking Sector Cyber Security Posture

Indicator 5.5 Information Leakage Risk



Assessment – *Maturity Level 2*

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

Information Leakage Risk

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

144. **Employees often use their work email address to sign-up for third-party websites** – not only professional platforms but also leisure-oriented services. However, these platforms and services can expose users' sensitive information in data breaches caused by either a malicious external compromise or internal negligence.

> **73%** CREST's research revealed that **73% of the assessed financial institutions in Uganda** had had at least some of their **employees' credentials leaked online** after unconnected attacks on third-party website-based service providers.

145. 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 can potentially allow cybercriminals to directly hijack employee's corporate accounts. Alternatively, leaked credentials may allow for more tailored and enhanced brute force attacks, providing adversaries with patterns and common combinations employees might follow when choosing passwords. Third party breaches may also lead to more sophisticated phishing efforts, with cybercriminals using the exposed information to craft highly convincing malicious messages, seeking to lure recipients into providing access or revealing additional data.

146. It has not been possible to verify how many financial institutions assessed in the research follow good information leakage hygiene practices and enforce strong password best practices. These measures help mitigate the threat associated with third-party leaked credentials.

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

Banking Sector Cyber Security Posture

Mitigation Measures

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

Infrastructure Vulnerability

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

Architecture & Access

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

Email Authentication

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

Information Leakage

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

Appendices

Appendix A

Glossary

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

Appendix A

Glossary (continued)

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

Appendix B

Summary of Maturity Level Definitions

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

Indicator 1.1
Government Strategy & Policy

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

Indicator 1.2
Regulator/Government Operated Assurance Schemes

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 1.3
Law Enforcement & Cyber Defence Capabilities

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1
CERTs & Information Sharing

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

Indicator 3.1
Threat Intelligence Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2
Vulnerability Assessment Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3
Penetration Testing Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4
Security Operation Centre Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5
Incident Response Service providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1
Academia & Higher Education

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

Indicator 4.2
Training Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3
Professional Certifications

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

Indicator 4.4
Professional Cyber Membership Organisations

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5
Specialist Recruitment

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

Indicator 4.6
Events & Exhibitions

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1
Banking Sector Cyber Risk Profile

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

Indicator 5.2
Infrastructure Vulnerability Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3
Architecture & Access Risk

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

Indicator 5.4
Email Authentication Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5
Information Leakage Risk

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

Appendix C

Professional Certifications and Member Organisations

Background

1. Knowledge, skills and experience are three factors used by companies when determining who to hire or promote. These factors are also used by a buyer when selecting which service provider to award a contract to. Experience is a matter of record and can be underpinned by endorsements from former 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. Buyers can also 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 at '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[74]		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council[75]	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA[76]		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2[77]		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS[78]		GSEC GPEN GWAPT GICSP GCIP GCWN GCUX GAWN GPYC GWEB GCIH GCFE GASF GREM GCFA GNFA GSSP-Java GSSP-.Net GICSP GMOB GBFA GCSA	GXPN GCCC GSED GPPA GMON GCIA GRID GCDA GCTI GCED GPPA GDSA GDAT GEVA GNSA		GSE	✓	✓			
CompTIA[79]	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security[80]		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance[81]		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[82]		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[83]		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft[84]	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services[85]	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)[86]	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS[87]	CiSMP	BCM CIAA	CIRM				✓		✓	✓
IET[88]	ICTTech									✓

Appendix D

Country Context

Geography

1. Uganda is a land-locked country in east Africa whose neighbours are: South Sudan to the north, Kenya to the west, Lake Victoria is south west, with Tanzania and Rwanda to the south and the Democratic Republic of Congo to the east[89]. The capital and largest city of Uganda is Kampala, with a population of 3,298,364. Other major cities include Jinja, Mbale and Entebbe in the south and Gulu in the north[90].
2. Some 20% of the country comprises lakes and rivers - as a result the soil is generally fertile and productive, especially near Lake Victoria[91]. The lakes and rivers mean the majority of the country's power is provided by the Nalubaale and Kiira hydroelectric stations on the Victoria Nile river[92]. Even so, only 18% of households in Uganda have electricity connected, and there is an urban-rural electricity gap of 85%[93].

Natural resources

3. Uganda has the natural resources of petroleum, copper tungsten, cobalt, columbite-tantalite, gold, phosphate, iron ore and limestone.[94]

Population

4. The population of Uganda is ranked 35th largest in the world and as of 2019 was 40,367,000[95]. Uganda has one of the highest population growth rates in the world at 3%. It is the largest host for refugees in Africa and the third largest refugee host in the world[96]. Encyclopaedia Britannica shows that as of 2017, 48.4% of the population was under 15 years old and 28.9% was aged between 15 and 29 years, with a life expectancy at birth of 54.5 yea[97]. The population is split 23.8% urban and 76.2% rural. Some 50% of the population does not have access to medical facilities[98].
5. 32 different languages are spoken. As of 2017-18, male literacy in Uganda is 77.5% versus female literacy of 69.9%[99].

Economy

6. The Ugandan economy has slowed down due to COVID-19 and a locust invasion, so GDP 2020 is expected to be 0.4-1.7% compared to 5.6% in 2019[100]. As of 2016, Gross Domestic Product (GDP) was US$26,369bn[101] and in 2017 Gross National Income (GNI) was $600 USD per capita[102].
7. As of 2018, 90% of Ugandan organisations operate below the poverty line[103]. An article entitled "*A market systems approach to financial inclusion: Going beyond supply and demand*" stated that: "most of the Ugandan economy is comprised of informal and unregistered MSMEs, [Micro, Small & Medium Enterprises] which employ up to 90% of Uganda's workforce"[104].
8. 70% of Ugandans are still employed in agriculture, with most farmers working on less than three acres. Interestingly, a substantial proportion of women own the land on which they work[105] [106] and agriculture and agricultural products represent a large share of the Gross Domestic Product.
9. In terms of digital financial inclusion, there are several inhibitors including poor internet penetration rates and the effects of the 2018 introduction of a Government tax on social media and mobile money. There is a daily social media levy of US$0.005 per day, chargeable on 60 apps (including Facebook, etc) and mobile money withdrawals are taxed at 0.5% of the value of withdrawal[107]. Only 2% of the population has bank accounts[108].

Internet connectivity

10. Serianu's Africa-Cyber Security Report 2016 suggests 14,564,620 people (38% of the population) use the internet[109], though an article by Research ICT Africa entitled "The State of ICT in Uganda" from May 2019 states internet penetration in the country is only at 14%, with 65% of the population receiving 3G coverage, 17% receiving LTE/4G, and the number of mobile smart phone users comprising 16% of the population[110]. Uganda is ranked 152 of 176 on the International Telecommunication Union's Development Index[111].

Appendix D

Country Context (continued)

Cyber crime

11. Uganda was one of five countries studied in Serianu's Africa Cyber Security Report 2016. The report's results for malicious activity during the period studied are not positive for Uganda: IP Statistics – 40% of all malicious activity in Africa came from Uganda, 67% of top 10 spam servers used for spamming emails came from Uganda, and 66% of the top 10 dictionary attackers (a malicious attack based on trying all the strings in a pre-arranged listing)[112].

12. Serianu's 2016 report also revealed the cost of cybercrime to Uganda - US$35m[113]. In 2017, the Forensic Institute reported cybercrime cost Uganda the equivalent of US$42m, with 95.6% of cyber security incidents going unreported and only 4.4% of reported cases being successfully prosecuted[114].

13. In the Serianu Africa Cyber Security Report - Uganda Cyber Security Skills Gap 2018 "Cost of Cyber Crime" section, it states cybercrime in Uganda cost the equivalent of US$52m.

    The most affected industries were:

    - Banking
    - Financial services integrators
    - Microfinance schemes
    - Financial institutions and service providers, and
    - Government[115].

    The 2018 highlights stated a 15% increase in cybercrime incidents reported to police and a 5% increase in successfully prosecuted cybercrime[116]. Of crimes reported, the report states engineered malware attacks were on the rise, as were targeted ATM attacks and targeted phishing attacks[117].

14. In its 2019 annual crime report, Uganda's Police Force reports an increase in reported cybercrimes from 198 cases in 2018 to 284 cases in 2019, a loss of UGX11,446,603,500 in 2019, (just over US$3m), with UGX51,890,000, (approximately US$14,000) of that amount being recovered[118]. In 2019, the Ugandan Police's Directorate of Forensics Services and Department of Cybercrime and Digital Forensics received 237 requests for digital forensics, 23 of which were for computer forensics[119]. Ugandan Police also reported two major categories of cybercrime in 2019 - fradulent SIM card registration and swapping, and (virtual) impersonation of celebrities and well-known people.[120]

Cyber Security Professional Development

15. According to a May 2018 Pan African Vision magazine article, there were 1421 Ugandan graduates[121] with degrees, diplomas or certificates in ICT that year, from the ICT University in collaboration with Makerere University Business School (MUBS).

16. Serianu's Africa Cyber Security Report 2016 stated there were only 300 cyber security professionals in 2016[122]. And in the Serianu Africa Cyber Security Report - Uganda Cyber Security Skills Gap 2018 report, it recorded 400 cyber professionals, an increase of 100 people in two years. The report estimated at the date of publication (2018), Uganda needed 3,000 cyber professionals and that in five years' time (2023) the country would need 30,000.[123-124]

17. In the Serianu Africa Cyber Security Report - Uganda Cyber Security Skills Gap 2018, a skills shortage at senior management was identified The report suggested that 70% of companies faced a talent shortage of cybersecurity professionals in 2019. The report suggests a constraint when recruiting cybersecurity professionals is a lack of solid experience and low remuneration rates. It noted an increase in organisational spend in cybersecurity in 2017 to 2018, with 25% of respondents suggesting expenditure on cybersecurity measures of above US$10,000. It also noted a 50% increase in involvement of Board members on cybersecurity matters[125].

Other maturity models

18. Oxford University's Global Cyber Security Capacity Centre (GCSCC) and the Commonwealth Telecommunications Organisation (CTO) jointly authored a cyber security maturity model assessment on Uganda in 2015[126]. The International Telecommunications Union (ITU) has also produced a 'cyberwellness' report on Uganda.[127]

Appendix E

Bibliography

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

Africa CERT, 2020,
https://www.africacert.org/about-us/
(accessed July and 27 Oct 2020)

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

Anena Harriet,
'Social Media Crime Crackdown. There's more to this story,' 22 Jun 2015,
African Centre for Media Excellence, 22 June 2015
https://acme-ug.org/2015/06/22/social-media-crime-crackdown-theres-more-to-this-story/
(accessed July 2020)

Asiimwe, Dicta,
'ICT University Graduates more than over 1000 in Uganda', *Pan African Visions,* 27 May 2018,
https://panafricanvisions.com/2018/05/ict-university-graduates-1000-uganda/
(accessed 26 Oct 2020)

Bagala Andrew,
'Activists Cry Foul as Police Set up Cybercrime Unit,'
Unwanted Witness, 19 Mar 2014,
https://www.unwantedwitness.org/activists-cry-foul-as-police-set-up-cyber-crime-unit/
(accessed Oct 2020)

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)

Bank of Uganda,
'Expression of Interest for Provision of Consultancy Services for Assessment of Bank of Uganda's Compliance to Uganda Cyber Laws'.
Author, March 2013,
https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/MediaCenter/press_releases/2013/Mar/Expressions-of-Interest-for-Provision-of-Consultancy-Services-for-Assesment-of-BOU-Complaince-to-Uganda-cyber-laws.pdf
(accessed Oct 2020)

Bank of Uganda and MEFMI, Workshop in Cyber Security in the Financial Sector, *Author,* 2020,
https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/MediaCenter/misc/Cyber-Financial-Crimes-FlierRegistration-Form_1.pdf
(accessed Oct 2020)

Courses Eye,
https://www.courseseye.com
(accessed July 2020)

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

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)

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,
https://www.first.org/about/mission
(accessed 26 Oct 2020)

Appendix E

Bibliography (continued)

Gilibrays G, Gilbert M, Karume SM, Matovu D, 'State of Cyber Security: the Ugandan perspective', International Journal of Scientific & Engineering Research Volume 10, Issue 4, April-2019, 713 ISSN 2229-5518 *(PDF) State of cyber security: the Ugandan perspective.* Available from: **https://www.researchgate.net/publication/333759204_State_of_cyber_security_the_Ugandan_perspective** (accessed 26 Oct 2020)

Gillwald, A., Mothobi, O., Tusubira, F., & Ndiwalana, A. (2019). 'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'. *Research ICT Africa*. **https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf** (Accessed 25 Oct 2020)

Global Cyber Security Capacity Centre, 'Cybersecurity Capacity Review of the Republic of Uganda', *Oxford,* Author, 2016, **https://gcscc.web.ox.ac.uk/files/ugandacmmpdf** (accessed July 2020)

Government of Uganda, 'Anti-Money Laundering Act 2013', *The Financial Intelligence Authority (FIA),* July 2013, **https://www.fia.go.ug/sites/default/files/2020-06/Anti-Money%20Laundering%20ACT%2C2013_0.pdf** (accessed Oct 2020)

Government of Uganda, The Ministry of Finance, Planning and Economic Development (MoFPED), *Author,* **https://finance.go.ug/** (accessed October 2020)

Government of Uganda, Ministry of ICT and National Guidance, 'About us', 2018, **https://ict.go.ug/about-us/** (accessed Oct 2020)

Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'Blog - Press Release 5th Mar 2019', *Author,* 2019, **https://ict.go.ug/2019/03/06/press-release-5th-march-2019/** (accessed Oct 2020)

Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'Computer Misuse Act 2011', *The Ugandan Gazette. No 10, Vol CIV, Act 2,* 14 February 2011, **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Computer-Misuse-Act-No.-2-of-2011-1.pdf** (accessed July and Oct 2020)

Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'Data Protection and Privacy Act 2019' *Author,* 2019, **https://ict.go.ug/2019/03/01/data-protection-and-privacy-act-2019/** (accessed July 2020)

Government of Uganda, Ministry of Information and Communication Technology (ICT) and National Guidance, 'Electronic Signature Act 2011', *Ugandan Gazette. No 19, Vol CIV, Act 7,* 18 March 2011, **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Electronic-Signatures-Act-No.-7-of-2011.pdf** (accessed July and Oct 2020)

Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'The Electronic Transactions Act 2011', *The Ugandan Gazette. No 19, Vol CIV, Act 8,* 18 March 2011, **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Electronic-Transactions-Act-No.-8-of-2011.pdf** (accessed July and Oct 2020)

Government of Uganda, Ministry of Information and Communication Technology (ICT) and National Guidance, 'Information Security', *Author,* 2018, **https://ict.go.ug/initiatives/information-security/** (accessed July and Oct 2020)

Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, "National Electronic Government Policy Framework 2011" *Author,* June 2011, **https://ict.go.ug/wp-content/uploads/2019/12/National_E-Government_Policy_Framework_2011-2.pdf** (accessed Oct 2020)

Appendix E

Bibliography (continued)

Government of Uganda,
Ministry of Information and Communications Technology (ICT) and National Guidance,
'National Information Security Strategy (NISS Final Draft) March 2011', *CERT-UG,* 2011,
https://www.cert.ug/sites/default/files/National%20Information%20Security%20Strategy%202011.pdf
(accessed July and Oct 2020)

Government of Uganda,
The National Information Technology Authority Act 2009,
The Ugandan Gazette, No36, Vol CII, Act 4,
Dated 32 July 2009,
https://www.nita.go.ug/sites/default/files/publications/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf
(accessed July and Oct 2020)

Ingham, Kenneth, 'Uganda', Britannica, UK, 8 Sep 2020,
https://www.britanica.com/place/Uganda
(accessed 23 Oct 2020)

International Telecoms Union (ITU), 'Uganda', *Author,*
https://www.itu.int/ITU-D/ict/cs/uganda/uganda.html
(accessed July 2020 and 28 Oct 2020)

K, Paul, 'Cybercrime in Uganda',
Forensic Institute and ICT Security, 2018?,
https://www.forensicsinstitute.org/cybercrime-in-uganda/ (accessed 26 Oct 2020)

Kamoga, Jonathon,
'Uganda Loses Shs 122bn Annually to Cyber Attacks, Says Report'. *The Observer – Uganda,* 18 August 2017.
https://observer.ug/news/headlines/54458-uganda-loses-shs-122bn-annually-to-cyber-attacks-says-report.html
(accessed 25 Oct 2020)

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

Muhumza Joel,
"A market systems approach to financial inclusion: Going beyond supply and demand"
Uganda, *Centre for Development Alternatives,*
24 Jan 2020,
https://cda.co.ug/2080/a-market-systems-approach-to-financial-inclusion-going-beyond-supply-and-demand/ (accessed Nov 2020)

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

National Cyber Security Index,
"National Cyber Security Index 2018", *Estonia, e-Governance Academy,* 2018,
https://ega.ee/wp-content/uploads/2018/05/ncsi_digital_smaller.pdf
(accessed Oct 2020)

National Information Technology Authority – Uganda (NITAU),
https://www.nita.go.ug/
(accessed July 2020)

National Information Technical Authority (NITA-U),
'The National Information Security Framework, The National Information Security Policy',
Author, February 2014,
https://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf
(accessed Oct 2020)

National Information Technology Authority -Uganda,
'NITA-U Launches the National Computer Emergency Response Team/Coordination Centre'
Author, 1 May 2014,
https://www.nita.go.ug/media/nita-u-launches-national-computer-emergency-response-teamcoordination-centre
(accessed 27 October 2020)

New Vision,
'Uganda Still Regarded a High-Risk Nation for Cyber-attacks', *Author,* Nov 2017,
https://www.newvision.co.ug/news/1466266/uganda-regarded-risk-nation-cyber-attacks
(accessed 23 Oct 2020)

Appendix E

Bibliography (continued)

Sekyewa Edward Ronald,
'Digital Surveillance',
Development and Cooperation, 8 Oct 2019,
https://www.dandc.eu/en/article/what-ugandan-authorities-are-doing-limit-impact-online-opposition-voices (accessed July 2020)

Serianu,
'Africa – Cyber Security Report 2016',
Kenya, *Author,* 2016,
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

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,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap',
Kenya, *Author,* 2018,
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

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

The Financial Intelligence Authority (FIA), 2014,
https://www.fia.go.ug/
(accessed Oct 2020)

The Ugandan Institute of Communications & Technology (UICT), 2020,
https://www.uict.ac.ug/
(accessed Oct 2020)

The World Bank,
'The World Bank in Uganda – Economic Overview',
Author, 12 Aug 2020,
https://www.worldbank.org/en/country/uganda/overview (accessed 24 Oct 2020)

Ugandan Communications Commission, 2020,
https://www.ucc.co.ug/
(accessed July and Oct 2020)

Ugandan Communications Commission,
'Integrating ICT into Education in Uganda ',
Author July 2014,
https://www.ucc.co.ug/files/downloads/ICT%20Integration%20into%20teaching%20and%20learning%20booklet%202014.pdf
(accessed Oct 2020)

Ugandan Computer Emergency Response Team,
Ug-CERT,
https://www.ug-cert.ug/
(accessed July 2020)

Ugandan National Computer Emergency Response Team/Coordination Centre,
CERT-Ug,
https://cert.ug/
(accessed 27 Oct 2020)

Ugandan Police Force,
'Cybercrime Barometer',
https://www.upf.go.ug/cyber-barometer/
(accessed July 2020)

Ugandan Police,
'Directorates',
https://www.upf.go.ug/directorate/
(accessed July 2020)

Ugandan Police,
Annual Crime Report 2019,
Author, 2019,
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

UN,
'UNDIR Cyber Security Portal – Uganda'
Author, Sep 2020,
https://cyberpolicyportal.org/en/states/uganda
(accessed 23 Oct 2020)

Appendix E

Bibliography (continued)

Unwanted Witness,
'Ugandan Police Force, The Electronic Counter Measures Unit, What is it and What does it do? Seeking Clarity of its role in policing in Uganda',
Author, Mar 2018,
https://www.unwantedwitness.org/wp-content/uploads/2017/03/Electronic-Counter-Measure-Unit.pdf (accessed July and Oct 2020)

Unwanted Witness,
'Cybercrime'
https://www.unwantedwitness.org/?s=cyber+crime&tztc=1
(accessed Oct 2020)

Walter Max,
"What Is Uganda's Employment Challenge?"
Uganda, *Centre for Development Alternatives*,
23 May 2019.
https://cda.co.ug/1572/reframing-ugandas-employment-challenge/
(accessed Nov 2020)

Waswa, Sam,
'Uganda Tops African Nations in Cyber Security',
Chimp Reports, 24 Sep 2018,
https://chimpreports.com/uganda-tops-african-nations-in-cyber-security/
(accessed 25 Oct 2020)

World Population Review,
'Kampala Population 2020', *Author*, 2020,
https://worldpopulationreview.com/world-cities/kampala-population
(accessed 26 Oct 2020)

Appendix F

Endnotes

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

[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] Government of Uganda, National Electronic Government Policy Framework 2011
'Institutional Framework', *Author,* June 2011,
Para 2.5.1 p20-23
https://ict.go.ug/wp-content/uploads/2019/12/National_E-Government_Policy_Framework_2011-2.pdf (accessed Oct 2020)

[5] Government of Uganda, Ministry of ICT and National Guidance, 'About us', 2018,
https://ict.go.ug/about-us/ (accessed Oct 2020)

[6] National Information Technology Authority Uganda (NITA-U),
https://www.nita.go.ug/
(accessed July 2020)

[7] NITA-U,
'National Information Security Advisory Group (NISAG) Inauguration Ceremony', *Author,* 28 Oct 2014,
https://www.nita.go.ug/media/national-information-security-advisory-group-nisag-inauguration-ceremony (accessed October 2020)

[8] Ugandan National Computer Emergency Response Team/Coordination Centre, (CERT-UG),
https://cert.ug/ (accessed 27 Oct 2020)

[9] National Information Technical Authority (NITA-U),
'The National Information Security Framework, The National Information Security Policy', *Author,* February 2014, para 2.1, p8,
https://www.nita.go.ug/sites/default/files/publications/National%20Information%20Security%20Policy%20v1.0_0.pdf
(accessed Oct 2020)

[10] Global Cyber Security Capacity Centre,
'Cybersecurity Capacity Review of the Republic of Uganda', Oxford, *Author,* 2016,
https://gcscc.web.ox.ac.uk/files/ugandacmmpdf
(accessed July 2020)

[11] Global Cyber Security Capacity Centre,
'Cybersecurity Capacity Review of the Republic of Uganda', Oxford, Author, 2016, p8,
https://gcscc.web.ox.ac.uk/files/ugandacmmpdf
(accessed July 2020)

[12] Ugandan Communications Commission,
"About-UCC" *Author,* 2020,
https://www.ucc.co.ug/about-ucc/
(accessed July and Oct 2020)

[13] The Ugandan Institute of Communications & Technology (UICT),
https://www.uict.ac.ug/ (accessed Oct 2020)

[14] Ugandan Communications Commission,
'Integrating ICT into Education in Uganda',
Author, July 2014,
https://www.ucc.co.ug/files/downloads/ICT%20Integration%20into%20teaching%20and%20learning%20booklet%202014.pdf
(accessed Oct 2020)

[15] Ugandan Communications Commission,
'Integrating ICT into Education in Uganda',
Author, July 2014, Para 1.1
https://www.ucc.co.ug/files/downloads/ICT%20Integration%20into%20teaching%20and%20learning%20booklet%202014.pdf
(accessed Oct 2020)

[16] Ministry of Information and Communications Technology (ICT),
'Data Protection and Privacy Act 2019' *Author,* 2019,
https://ict.go.ug/2019/03/01/data-protection-and-privacy-act-2019/
(accessed July 2020)

Appendix F

Endnotes (continued)

[17] Ugandan Police, Annual Crime Report 2019, *Author,* 2019, **https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801** (accessed 26 Oct 2019)

[18] Government of Uganda, National Electronic Government Policy Framework 2011 'Legal and Regulatory Framework', *Author,* June 2011, Para 2.1.3 p15 and Para 2.5.3 p23 **https://ict.go.ug/wp-content/uploads/2019/12/National_E-Government_Policy_Framework_2011-2.pdf** (accessed Oct 2020)

[19] Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'Computer Misuse Act 2011', *The Ugandan Gazette.* No 10, Vol civ, 14 February 2011, **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Computer-Misuse-Act-No.-2-of-2011-1.pdf** (Accessed July and Oct 2020)

[20] Government of Uganda, Ministry of Information and Communication Technology (ICT) and National Guidance, 'Electronic Signature Act 2011', *The Ugandan Gazette. No 19,* Vol CIV, Act 7, 18 March 2011 **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Electronic-Signatures-Act-No.-7-of-2011.pdf** (Accessed July and Oct 2020)

[21] Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'The Electronic Transactions Act 2011', *The Ugandan Gazette. No 19, Vol CIV, Act 8,* 18 March 2011, **https://ict.go.ug/wp-content/uploads/2019/12/UGANDA-Electronic-Transactions-Act-No.-8-of-2011.pdf** (Accessed July and Oct 2020)

[22] Bank of Uganda, 'Expression of Interest For Provision of Consultancy Services For Assessment of Bank of Uganda's Compliance to Uganda Cyber Laws'. *Author,* March 2013, para 1, **https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/MediaCenter/press_releases/2013/Mar/Expressions-of-Interest-for-Provision-of-Consultancy-Services-for-Assesment-of-BOU-Complaince-to-Uganda-cyber-laws.pdf** (accessed Oct 2020)

[23] Government of Uganda, The National Information Technology Authority Act 2009, *The Ugandan Gazette, No36, Vol CII, Act 4,* dated 32 July 2009, **https://www.nita.go.ug/sites/default/files/publications/NITA-U%20Act%20%28Act%20No.%204%20of%202009%29.pdf** (accessed July and Oct 2020)

[24] Government of Uganda, Ministry of ICT and National Guidance, 'Information Security', *Author, 2018*, **https://ict.go.ug/initiatives/information-security/** (accessed July and Oct 2020)

[25] Government of Uganda, Ministry of Information and Communications Technology (ICT) and National Guidance, 'National Information Security Strategy (NISS Final Draft) March 2011', *CERT-UG,* 2011, **https://www.cert.ug/sites/default/files/National%20Information%20Security%20Strategy%202011.pdf** (accessed July and Oct 2020)

[26] Ugandan Computer Emergency Response Team, Ug-CERT, **https://www.ug-cert.ug/** (accessed July 2020)

[27] Ministry of Information and Communications Technology (ICT), 'Data Protection and Privacy Act 2019' *Author,* 2019, **https://ict.go.ug/2019/03/01/data-protection-and-privacy-act-2019/** (accessed July 2020)

[28] Government of Uganda, The Ministry of Finance, Planning and Economic Development (MoFPED), 'Policies and Legislation', *Author,* **https://finance.go.ug/mofped/policies** (accessed October 2020)

Appendix F

Endnotes (continued)

[29] Government of Uganda, The Ministry of Finance, Planning and Economic Development (MoFPED),'Ministry Structure', *Author,* Sect 2-A-v, **https://finance.go.ug/mofped/ministry-structure** (accessed October 2020)

[30] Bank of Uganda, 'Expression of Interest For Provision of Consultancy Services For Assessment of Bank of Uganda's Compliance to Uganda Cyber Laws'. *Author,* March 2013, **https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/MediaCenter/press_releases/2013/Mar/Expressions-of-Interest-for-Provision-of-Consultancy-Services-for-Assesment-of-BOU-Complaince-to-Uganda-cyber-laws.pdf** (accessed Oct 2020)

[31] Bank of Uganda and MEFMI, Workshop in Cyber Security in the Financial Sector, *Author,* 2020, **https://www.bou.or.ug/bou/bouwebsite/bouwebsitecontent/MediaCenter/misc/Cyber-Financial-Crimes-FlierRegistration-Form_1.pdf** (accessed Oct 2020)

[32] Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), 'Member States', *Author,* **http://mefmi.org/about-mefmi/member-states/** (Accessed Oct 2020)

[33] Macroeconomic and Financial Management Institute of Eastern and Southern Africa (MEFMI), 'Cyber Security', *Author,* **http://mefmi.org/?s=cyber+security+** (Accessed Oct 2020)

[34] The Financial Intelligence Authority (FIA), 2014, **https://www.fia.go.ug/** (accessed Oct 2020)

[35] Ugandan Government, 'Anti-Money Laundering Act 2013', *The Financial Intelligence Authority (FIA),* July 2013, **https://www.fia.go.ug/sites/default/files/2020-06/Anti-Money%20Laundering%20ACT%2C2013_0.pdf** (accessed Oct 2020)

[36] The Financial Intelligence Authority (FIA), 'Legal – Publications' 2014, **https://www.fia.go.ug/index.php/publications** (accessed Oct 2020)

[37] Ugandan Government, 'Anti-Money Laundering Act 2013', *The Financial Intelligence Authority (FIA),* July 2013, Part III, para 13, p19, **https://www.fia.go.ug/sites/default/files/2020-06/Anti-Money%20Laundering%20ACT%2C2013_0.pdf** (accessed Oct 2020)

[38] Serianu, 'Africa – Cyber Security Report 2016', Kenya, *Author,* 2016, p11. **https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf** (Accessed 26 Oct 2020)

[39] Serianu, 'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap', Kenya, *Author,* 2018, **https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf** (accessed Oct 2020)

[40] K, Paul, 'Cybercrime in Uganda', *Forensic Institute and ICT Security,* 2018?, **https://www.forensicsinstitute.org/cybercrime-in-uganda/** (accessed 26 Oct 2020)

[41] Daily Monitor - Business-Technology, 'Cyber Criminals now targeting SMEs- report', *Author* 2014 and 2020, **https://www.monitor.co.ug/uganda/business/technology/cyber-criminals-now-targeting-smes-report-2731402** (accessed July and Oct 2020)

[42] Bagala Andrew, 'Activists Cry Foul as Police Set up Cybercrime Unit', *Unwanted Witness* 19 Mar 2014, **https://www.unwantedwitness.org/activists-cry-foul-as-police-set-up-cyber-crime-unit/** (accessed Oct 2020)

Appendix F

Endnotes (continued)

[43] Kamoga, Jonathon,
'Uganda Loses Shs 122bn Annually to Cyber Attacks, Says Report'. *The Observer – Uganda,* 18 August 2017.
https://observer.ug/news/headlines/54458-uganda-loses-shs-122bn-annually-to-cyber-attacks-says-report.html (accessed 25 Oct 2020)

[44] New Vision,
'Uganda Still Regarded a High-Risk Nation for Cyber-attacks', *Author,* Nov 2017,
https://www.newvision.co.ug/news/1466266/uganda-regarded-risk-nation-cyber-attacks
(accessed 23 Oct 2020)

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

[46] Unwanted Witness, 'Cybercrime'
https://www.unwantedwitness.org/?s=cyber+crime&tztc=1 (accessed Oct 2020)

[47] Ugandan Police,
Annual Crime Report 2019, *Author,* 2019, p-xxvii,
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

[48] Ugandan Police,
Annual Crime Report 2019, *Author,* 2019,
para 4.3, p89-90
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

[49] Ugandan Police Force,
Directorate of Information & Communications Technology,
https://www.upf.go.ug/directorate/
(Accessed July 2020)

[50] Anena Harriet,
'Social Media Crime Crackdown. There's more to this story', *African Centre for Media Excellence,* 22 Jun 2015,
https://acme-ug.org/2015/06/22/social-media-crime-crackdown-theres-more-to-this-story/
(accessed July 2020)

[51] Unwanted Witness,
'Ugandan Police Force, The Electronic Counter Measures Unit, What is it and What does it do? Seeking Clarity of its role in policing in Uganda ',
Author, Mar 2018,
https://www.unwantedwitness.org/wp-content/uploads/2017/03/Electronic-Counter-Measure-Unit.pdf (accessed Oct 2020)

[52] Ugandan Police Force,
Cybercrime Barometer,
https://www.upf.go.ug/cyber-barometer/
(accessed July 2020)

[53] Ugandan National Emergency Response Team,
CERT-Ug,
https://cert.ug/ (accessed 27Oct2020)

[54] NITA-Uganda,
'NITA-U Launched the National Computer Emergency Response Team/Coordination Centre'
01May2014,
https://www.nita.go.ug/media/nita-u-launches-national-computer-emergency-response-teamcoordination-centre (accessed 27 October 2020)

[55] Ugandan Computer Emergency Response Team, Ug-CERT, 'Roles and Functions'
https://www.ug-cert.ug/data/smenu/17/Roles-and-Functions.html (accessed July 2020)

[56] Forum of Incident Response and Security Teams (FIRST), 2015-2020,
https://www.first.org/about/mission
(accessed 26 Oct 2020)

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

[58] Africa CERT, 2020
https://www.africacert.org/about-us/
(accessed 27 Oct 2020)

[59] Global Cyber Security Capacity Centre,
'Cybersecurity Capacity Review of the Republic of Uganda', Oxford, *Author,* 2016, p16,
https://gcscc.web.ox.ac.uk/files/ugandacmmpdf
(accessed July 2020)

Appendix F

Endnotes (continued)

[60] 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)

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

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

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

[64] 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)

[65] Ugandan Communications Commission,
'Integrating ICT into Education in Uganda',
Author, July 2014,
https://www.ucc.co.ug/files/downloads/ICT%20Integration%20into%20teaching%20and%20learning%20booklet%202014.pdf
(accessed Oct 2020)

[66] Ugandan Communications Commission,
'Integrating ICT into Education in Uganda',
Author, July 2014, Para 1.1
https://www.ucc.co.ug/files/downloads/ICT%20Integration%20into%20teaching%20and%20learning%20booklet%202014.pdf
(accessed Oct 2020)

[67] Africa Cyber Immersion Centre outreach training and education programme,
https://www.serianu.com/acic.html
(accessed Oct 20)

[68] 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)

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

[70] Uganda Legal Information Institute, Data Protection and Privacy Act, 2019,
https://ulii.org/ug/legislation/act/2019/1
(accessed 29 Oct 20)

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

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

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

[74] CREST International,
https://www.crest-approved.org/
(accessed Aug 20)

[75] EC Council,
https://www.eccouncil.org/
(accessed Aug 20)

[76] ISACA,
https://www.isaca.org/
(accessed Aug 20)

[77] (ISC)2,
https://www.isc2.org/
(accessed Aug 20)

[78] SANS,
https://www.sans.org/
(accessed Aug 20)

[79] CompTIA,
https://www.comptia.org/
(accessed Aug 20)

Appendix F

Endnotes (continued)

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

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

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

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

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

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

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

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

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

[89] Ingham, Kenneth, 'Uganda-Land,' *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[90] World Population Review, 'Kampala Population 2020', *Author,* 2020, **https://worldpopulationreview.com/world-cities/kampala-population** (accessed 26 Oct 2020)

[91] Ingham, Kenneth, 'Uganda-Economy, Britannica, UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[92] Ingham, Kenneth, 'Uganda–Resources and Power,' *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[93] Gillwald, A., Mothobi, O., Tusubira, F., & Ndiwalana, A. (2019). 'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'. *Research ICT Africa,* May 2019, pIV. **https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf** (Accessed 25 Oct 2020)

[94] Ingham, Kenneth, 'Uganda–Resources and Power,' *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[95] Ingham, Kenneth, 'Uganda–Quick Facts', *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[96] The World Bank, The World Bank in Uganda – Economic Overview, *Author,* 12 Aug 2020, **https://www.worldbank.org/en/country/uganda/overview** (accessed 24 Oct 2020)

[97] Ingham, Kenneth, 'Uganda–Quick Facts', *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[98] Ingham, Kenneth, 'Uganda–Demographic Trends', *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

[99] Ingham, Kenneth, 'Uganda-Quick Facts', *Britannica,* UK, 8 Sep 2020, **https://www.britannica.com/place/Uganda** (accessed 23 Oct 2020)

Appendix F

Endnotes (continued)

[100] The World Bank,
'The World Bank in Uganda – Economic Overview', *Author,* 12 Aug 2020,
https://www.worldbank.org/en/country/uganda/overview (accessed 24 Oct 2020)

[101] Serianu,
'Africa – Cyber Security Report 2016', Kenya, *Author,* 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

[102] Ingham, Kenneth,
'Uganda–Quick Facts', *Britannica,* UK, 8 Sep 2020,
https://www.britannica.com/place/Uganda
(accessed 23 Oct 2020)

[103] K, Paul,
'Cybercrime in Uganda', *Forensic Institute and ICT Security,* 2018,
https://www.forensicsinstitute.org/cybercrime-in-uganda/ (accessed 26 Oct 2020)

[104] Muhumza Joel,
"A market systems approach to financial inclusion: Going beyond supply and demand" Uganda, *Centre for Development Alternatives,* 24 Jan 2020,
https://cda.co.ug/2080/a-market-systems-approach-to-financial-inclusion-going-beyond-supply-and-demand/ (accessed Nov 2020)

[105] Ingham, Kenneth,
'Uganda–Agriculture, Forestry and Fishing', *Britannica,* UK, 8 Sep 2020,
https://www.britannica.com/place/Uganda
(accessed 23 Oct 2020)

[106] The World Bank,
'The World Bank in Uganda – Economic Overview', *Author,* 12 Aug 2020,
https://www.worldbank.org/en/country/uganda/overview (accessed 24 Oct 2020)

[107] Gillwald, A., Mothobi, O., Tusubira, F.,
& Ndiwalana, A. (2019).
'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'.
Research ICT Africa, May 2019, pIII.
https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf
(Accessed 25 Oct 2020)

[108] Gillwald, A., Mothobi, O., Tusubira, F.,
& Ndiwalana, A. (2019).
'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'.
Research ICT Africa, May 2019, p14 Fig10.
https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf (Accessed 25 Oct 2020)

[109] Serianu,
'Africa – Cyber Security Report 2016',
Kenya, *Author,* 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

[110] Gillwald, A., Mothobi, O., Tusubira, F.,
& Ndiwalana, A. (2019).
'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'.
Research ICT Africa, May 2019, pIII, pVI, p12 Fig7.
https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf
(Accessed 25 Oct 2020)

[111] Gillwald, A., Mothobi, O., Tusubira, F.,
& Ndiwalana, A. (2019).
'The State of ICT in Uganda (Policy Paper No. 8; Series 5: After Access – Assessing Digital Inequality in Africa)'.
Research ICT Africa, May 2019, pV.
https://researchictafrica.net/wp/wp-content/uploads/2019/05/2019_After-Access-The-State-of-ICT-in-Uganda.pdf
(Accessed 25 Oct 2020)

[112] Serianu,
'Africa – Cyber Security Report 2016',
Kenya, *Author,* 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

Appendix F

Endnotes (continued)

[113] Serianu,
'Africa – Cyber Security Report 2016', Kenya, *Author,* 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

[114] K, Paul,
'Cybercrime in Uganda', *Forensic Institute and ICT Security,* 2018,
https://www.forensicsinstitute.org/cybercrime-in-uganda/ (accessed 26 Oct 2020)

[115] Serianu,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap', Kenya, *Author,* 2018, p32
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

[116] Serianu,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap', Kenya, *Author,* 2018, p13
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

[117] Serianu,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap', Kenya, *Author,* 2018, p13
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

[118] Ugandan Police,
Annual Crime Report 2019, *Author,* 2019, p-xxvii,
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

[119] Ugandan Police,
Annual Crime Report 2019, *Author,* 2019,
para 4.3, p89-90
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

[120] Ugandan Police,
Annual Crime Report 2019, Author, 2019, p-xxvii,
https://www.upf.go.ug/wp-content/uploads/2020/04/Annual-Crime-Report-2019-Public.pdf?x45801
(accessed 26 Oct 2019)

[121] Asiimwe, Dicta,
'ICT University Graduates more than over 1000 in Uganda', *Pan African Visions,* 27 May 2018,
https://panafricanvisions.com/2018/05/ict-university-graduates-1000-uganda/
(accessed 26 Oct 2020)

[122] 'Africa – Cyber Security Report 2016', Kenya, Author, 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf

[123] Serianu,
'Africa – Cyber Security Report 2016', Kenya, *Author,* 2016, p11.
https://www.serianu.com/downloads/AfricaCyberSecurityReport2016.pdf
(Accessed 26 Oct 2020)

[124] Serianu,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap',
Kenya, *Author,* 2018, pp12-13,
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

[125] Serianu,
'Africa Cyber Security Report - Uganda - Cyber Security Skills Gap', Kenya, Author, 2018, p13
https://www.serianu.com/downloads/UgandaCyberSecurityReport2018.pdf
(accessed Oct 2020)

[126] GCSCC/CTO cyber security maturity model report,
https://gcscc.ox.ac.uk/cmm-reviews
(accessed Oct 2020)

[127] ITU Cyberwellness Report on Uganda,
https://www.itu.int/en/ITU-D/Cybersecurity/Documents/Country_Profiles/Uganda.pdf
(accessed Oct 2020)