CMAGE

Cyber Security Maturity Assessment Global Ecosystem

Indonesia 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 Indonesia's cyber security ecosystem. CREST has made both quantitative and qualitative assessments to arrive at an overall judgment as to the country's level of cyber security.

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

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

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

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

Unashamedly, the endpoint – at least from a CREST perspective - is that every financial services institution in Indonesia 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 Indonesia 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 Indonesia's cyber security ecosystem. The underlying aim is that every financial institution in Indonesia will become more resilient to cyber-attacks to better protect everyone in society.

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

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

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

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

The results are complex. Inevitably, there are areas of good practice and areas where investments of time, effort and money are needed.

The ecosystem is interconnected and interdependent. Making improvements in one part will bring benefits to other areas of the ecosystem as well.

Maturity Model Assessment Summary

Overall Indonesia Ecosystem

Maturity Level 2

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

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

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

Highlights Report

Summary of Observations

The overall maturity assessment for Indonesia'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

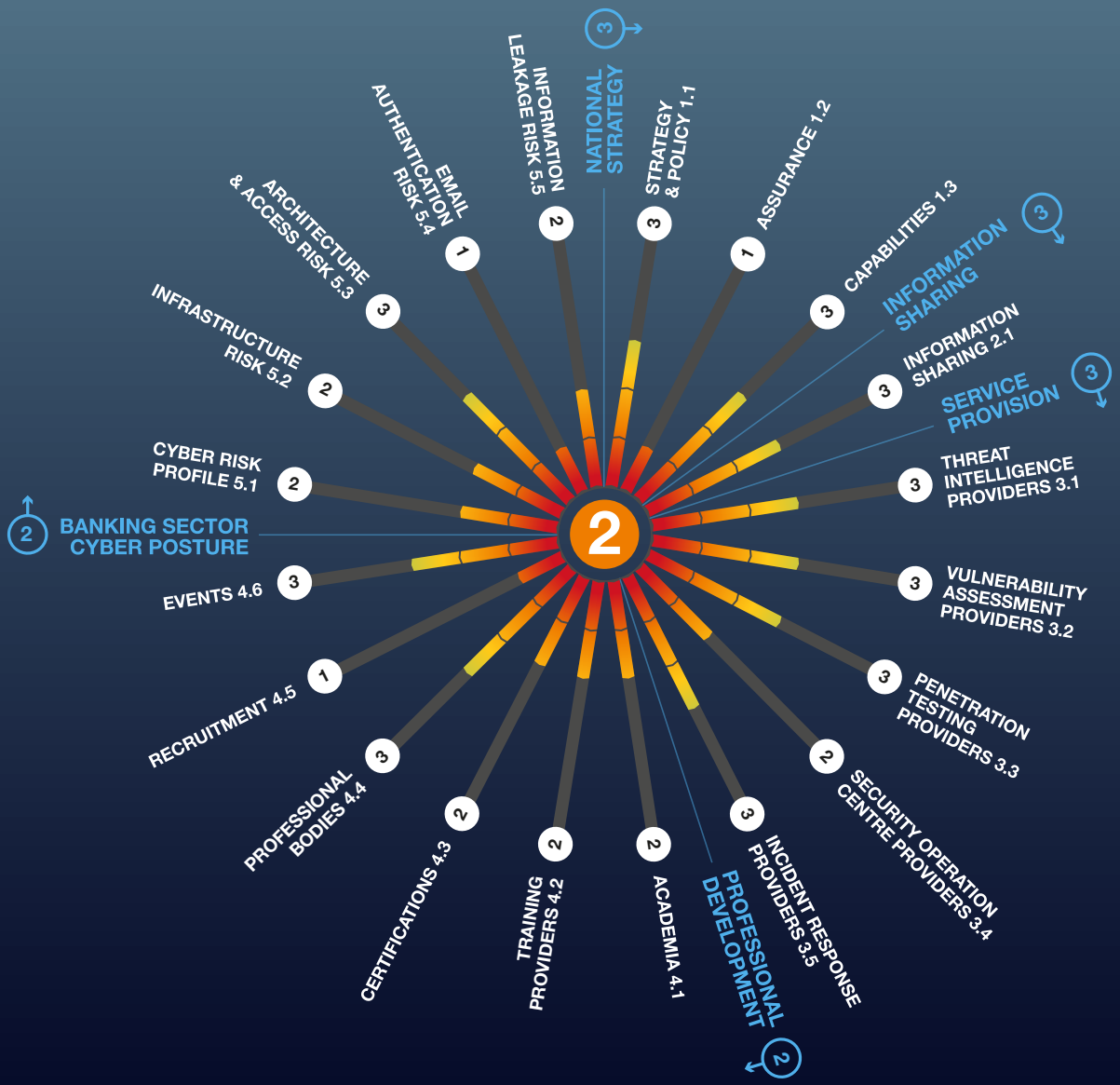
Maturity Scores

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 Indonesia’s cyber security ecosystem.

Highlights Report

Key Observations - Dimension 1 - National Cyber Security & Capabilities

Indonesia has a twenty-year track record of embracing the benefits and managing the risks of the internet age.

This journey has accelerated in the last few years. A 2015 Indonesian Defence white paper, identifying cybercrime and cyber warfare as significant threats, was a major milestone.

A new legal framework for dealing with cybercrime was established in 2016, and in 2017 **the State Cyber & Crypto Agency (BSSN)** was formed. Although still being refined, the 2018 National Cyber Security Strategy is another key milestone.

Responsibility for regulation of banks and other financial institutions lies with the **Indonesian Financial Conduct Authority (OJK)** rather than the Central Bank. There was no immediate evidence of any strong regulatory measures in respect of cyber risk or information security risk. As with some other countries in the region, Indonesia does not currently have the tools to effectively supervise cyber risk across the sector.

There appears to be healthy investment in capabilities to tackle cybercrime and to provide cyber defence. This matches the priority placed on such matters within the strategy and policy domain. There is some evidence of awareness of cybercrime threats within the general population but the addition of intervention measures to channel the skills of young people away from cybercrime should be considered.

Dimension 1

National Cyber Security Strategy & Capabilities

Maturity Level 3

Highlights Report

Key Observations - Dimension 2 - Cyber Security Information Sharing

CERTs & Information Sharing

Indonesia has two active Computer Emergency Response Teams (CERTs), **ID-SIRTII/CC and ID-CERT.**

They were established in 2007 and 1998 respectively, and both have regional links. **ID-SIRTII/CC is the official national CERT.** It is hosted by BSSN and a member of FIRST, and also plays a role in law enforcement.

A third CERT, covering academia, appears to be inactive. The last update on its website was in 2013.

There appears to be a lack of focus on information sharing in other critical sectors, such as financial services.

Dimension 2

Cyber Security Information Sharing

Maturity Level 3

Highlights Report

Key Observations - Dimension 3 - Cyber Security Service Provision

There is a good mix of local, regional, and international providers of cyber security services across four of the five disciplines examined. But provision of security operation centre services appears to be lagging slightly.

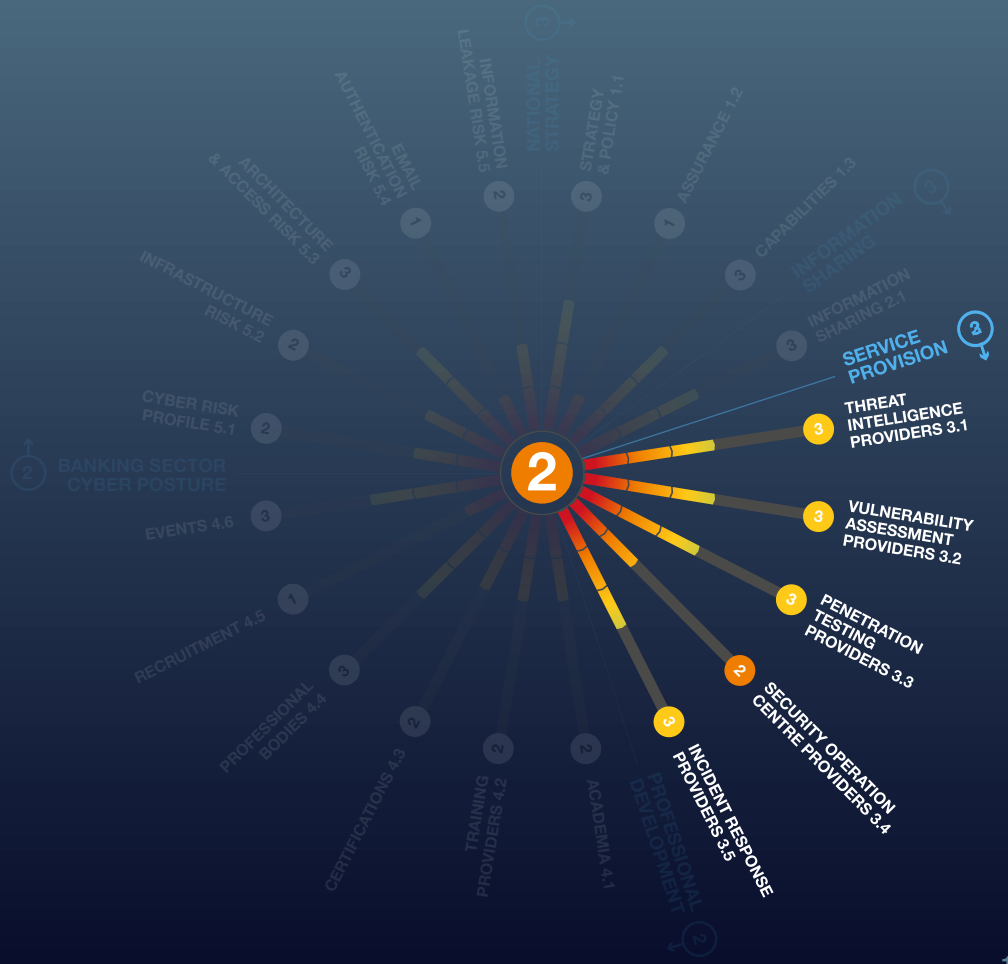
There are no local CREST member companies in Indonesia, but twelve international member companies already have local offices. There are local service providers across most disciplines, but their services have not been benchmarked. Several CREST and non-CREST companies offer cyber security services to clients in Indonesia from regional offices in nearby countries.

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

Dimension 3

Cyber Security Service Provision

Maturity Level 3



Highlights Report

Key Observations - Dimension 4 - Cyber Security Professional Development

CREST could only identify one university (Binus University) offering a dedicated cyber security degree. This appears to be at odds with the government's focus on improving cyber security across the country.

While many universities offer computer science and similar degrees, the security content of these courses is not known. It is noteworthy that a team from University Indonesia won the 2019 National Hacking Competition (Cyber Jawara). Cyber skills may be more widely taught than expected.

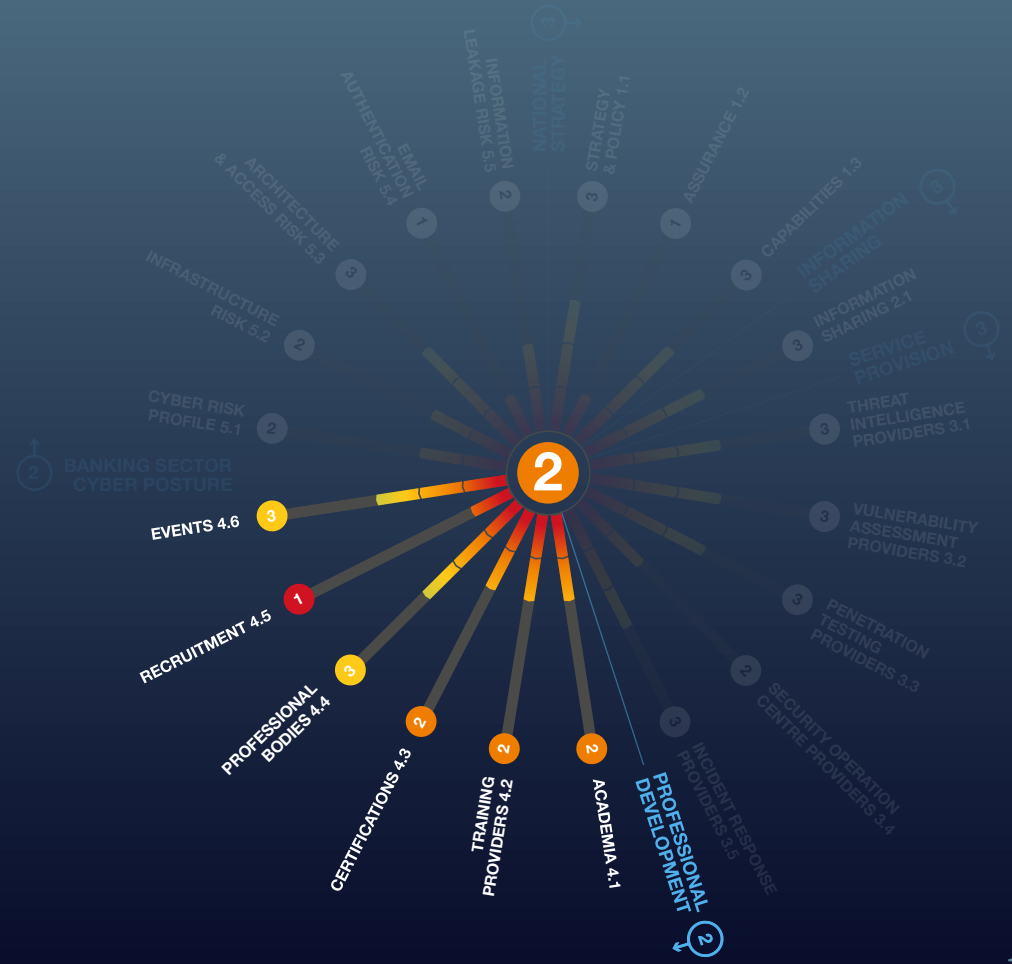
A first-class cyber security industry needs to be underpinned by an expansion in cyber security education. By utilising international good practice, Indonesia could build on its existing ICT courses to support creation of more specific cyber security courses and qualifications.

Continued on next page...

Dimension 4

Cyber Security Professional Development

Maturity Level 2



Highlights Report

Key Observations - Dimension 4 (continued)

Opportunities exist to develop an academic research capability in Indonesia, increasing the country's capacity for forward thinking in this important field.

There is a mixed picture with regards to training providers. Many providers are locally based and offer courses in Indonesian and English, both instructor-led and online, but there is little evidence there these training courses result in recognised certifications.

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

While examinations for many international professional certifications are readily accessible in Indonesia, take-up appears to be relatively low given the size of the Indonesian market.

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

It may be that cost of some professional certificates is prohibitive to many.

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

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

Recent steps to increase the number of local chapters of global membership organisations are encouraging. Of note is the Indonesia Network Security Association (IdNSA) which was formed in 2011.

There is little immediately available evidence of in-country cyber security specialist recruitment. This appears to contrast with the country's performance in other professional development indicators, the health of the local community of cyber security service providers and the national vision for tackling cybercrime and improving cyber defences.

Highlights Report

Key Observation - Dimension 5 - Banking Sector Cyber Security Posture

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

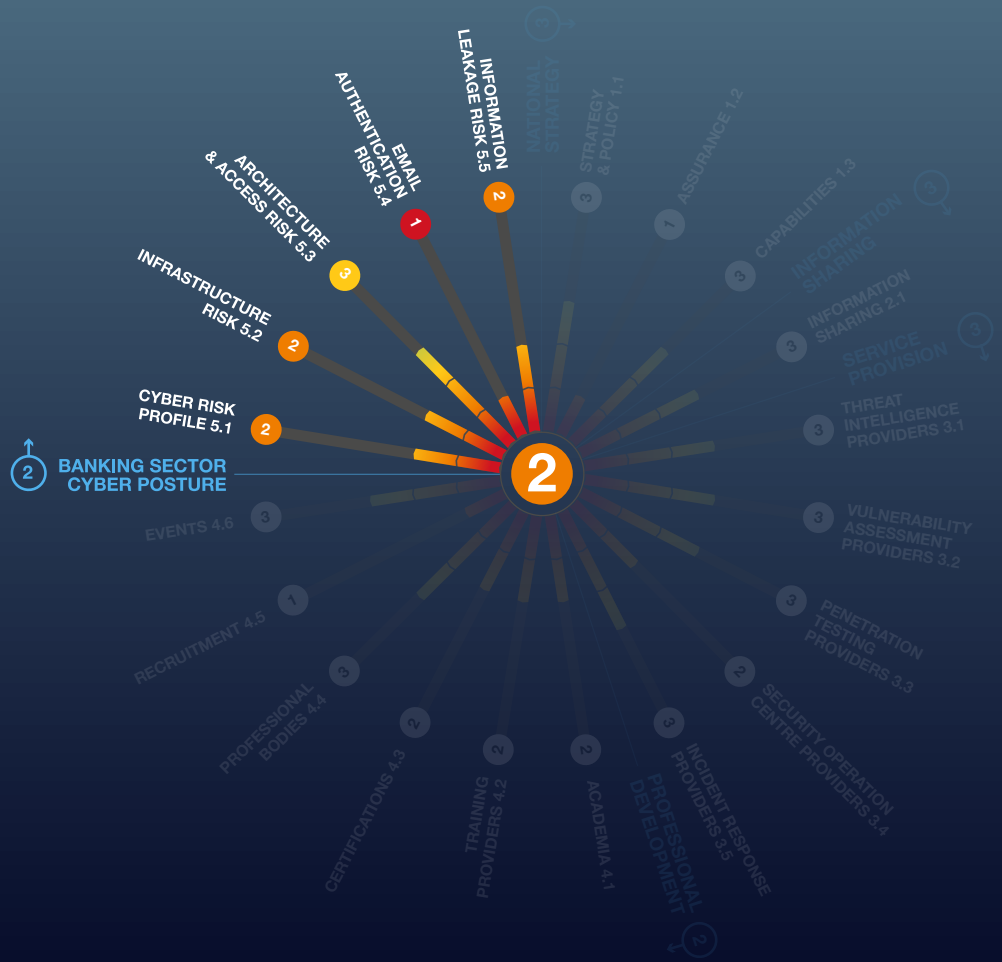
Indonesia's regulators can utilise this assessment to focus attention and highlight areas for review, provide access to the supporting guidance being developed and, where appropriate, encourage take up of technical security measures to improve cyber resilience.

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 undertaken on an organisation are limited by legal and ethical constraints.

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

Using this approach, accessible, measurable indicators were used to gain implicit insights into key risk areas. Overall, passive external assessments were carried out on the public-facing IT infrastructure of a sample of 97 financial institutions. For obvious reasons, all results were anonymised.

Risk is a combination of vulnerability and threat. Vulnerability can be assessed by measurable observations. Threat is primarily a judgement based on intelligence reports. The general threat to Indonesia's financial institutions is assessed as being lower than that for larger institutions in more advanced economies. Yet some institutions still attract a significant threat score

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

18% Of the sample, **18%** had evidence of critical vulnerabilities on their infrastructure

33% A further **33%** appeared to be carrying non-critical vulnerabilities, indicating Maturity Level 2 for Infrastructure Vulnerability Risk.

9% In respect of Architecture and Access Risk, **9%** of the sample appeared to have one or more remote access ports open on the public-facing infrastructure.

18% **18%** appeared to have one or more database ports open, leading to the award of Maturity Level 3 in this category.

58% Simple email authentication measures (Sender Policy Framework, (SPF)) have not been adopted by **58%** of the sample.

69% Advanced email authentication measures (Domain-based Message Authentication, Reporting and Conformance, (DMARC)) have not been adopted by **69%** of the sample. Our research indicates Maturity Level 1 for Email Authentication Risk.

54% In **54%** 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 Indonesia'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 Indonesia'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 Indonesia,** to help create development pathways.

Highlights Report

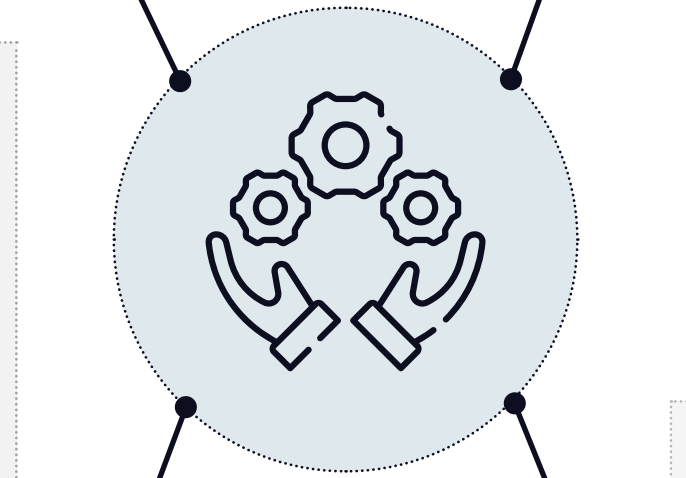
2021 Good Practices Guides and Tools

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 Indonesia's cyber security ecosystem.

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

CREST International

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

Introduction

Research Methodology

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

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

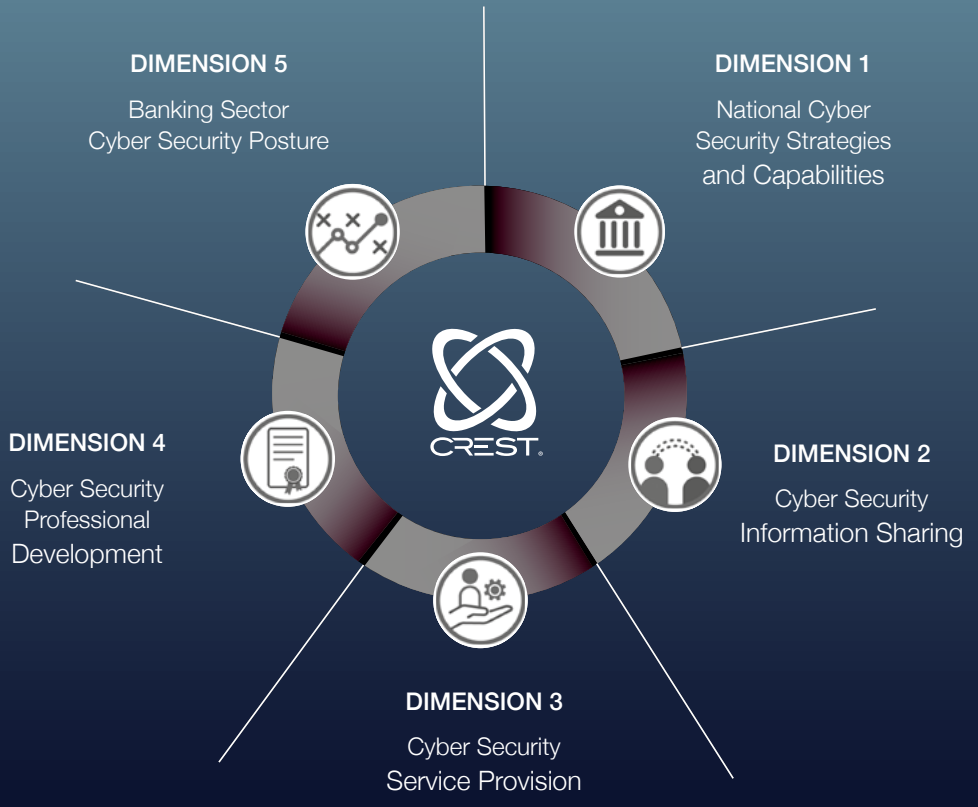
   The assessments were carried out by computer, to common standards, allowing for comparisons, benchmarking and periodic automated reassessments, if required. CREST believes this methodology is a global first - the first time rapid, automated mass assessment has been used as part of cyber security maturity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

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

CMAGE Structure

11. This Cyber security Maturity Assessment of the Global Ecosystem (CMAGE) is based upon 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.

12. 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 has also been 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 cyber security strategy it would be difficult for law enforcement and the judicial system to tackle cybercrime. Academia and professional training providers would struggle to know what courses to provide; potential students would find difficulty in understanding career options. It would also be difficult to justify and target research.

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

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

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

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

19. **The State Cyber and Crypto Agency** (BSSN, Badan Siber dan Sandi Negara) coordinates various institutions in implementing cyber security. It was established by Presidential Regulation N. 53 of 2017 (amended by Presidential Regulation N. 133 of 2017). It is responsible for implementing cybersecurity in an effective and efficient manner by utilising, developing, and consolidating all elements related to cybersecurity. It is mandated to manage national, regional, and international cooperation in cyber security affairs[4]. The BSSN is a member of the Organisation of Islamic Cooperation CERT (OIC-CERT)[5].

20. **The 2018 National Cyber Security Strategy,** initially published in outline by the BSSN, envisaged building and maintaining national cyber security by synergising stakeholders to participate in, and achieve, national security, ultimately improving national economic growth[6].

21. In December 2020, the BSSN released a press statement[7], (also published in English by DataGuidance[8]), releasing its draft Cyber Security Strategy for public consultation. A link at the end of the press release takes you to a presentation on the Draft National Cyber Security Strategy, in Indonesian[9]. The draft cyber security strategy has an updated vision (roughly translated) to achieve an advanced Indonesia with mutual-cooperation and durable national cybersecurity.

National Cyber Security Strategy & Capabilities

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

The strategy covers seven key areas:

- Governance
- Risk management
- Preparedness and resilience
- Capability and capacity development
- Legislation and regulation
- International cooperation
- Background and stakeholder actions[10].

There is a summary in English of the draft strategy (dated January 18, 2021) by Cloud Computing Indonesia[11].

22. **The forthcoming new Cyber Security Strategy is exciting news and should cause cybersecurity updates and change in all stakeholder areas involved:**
    - Government (law, legislation, and international cooperation)
    - Academia (development of centres of excellence, improve cyber lecture quality/research)
    - Business (implementation of the Network Information Sharing Analysis Centre (ISAC)
    - Society in general (growing cyber security apprentices, experts and social network influencers, cybercrime prevention)[12].
23. A 2016 working paper, *The Future of Cyber Security Capacity in Indonesia – Top 20 Recommendations for Strengthening National Cyber Security Capacity,* produced by Oxford Internet Institute[13], is a thorough document, offering assessment of Indonesia's cyber security status and future capacity.

    Some 38 stakeholders took part in a three-day consultation to review Indonesia's cyber security capacity[14]. The 20 recommendations can be found in an Executive Summary. Its first recommendation is that Indonesia needed a National Cyber Security Strategy, (which now appears to be in place).

Other recommendations include:

- Strengthening the role of the ID SIRTII/CC
- Promoting cyber security training and education programmes
- Reviewing and amending legislation, especially the ITE law no 11 of 2008
- Strengthening law enforcement capabilities for investigating cybercrime,
- Providing incentive-based solutions for local cyber security products[15].

Some of these points are likely to be covered in the proposed new National Cyber Security Strategy.

24. A useful 2013 National ICT Council presentation, entitled **"Indonesian National Cyber Security Strategy: Security and Sovereignty in Indonesian Cyberspace"**, covers the National Cyber Security Organisation Framework at that time. The presentation mentions four CERTS – the Government, Military, Banking and Education[16]. However, evidence of only three CERTS was found during research - covered in **Dimension 2**.

Overall Assessment

25. Indonesia clearly understands the benefits and threats of the information age. There appears to be a clear match between strategy and capabilities, with healthy investment in both. However, financial sector regulation and assurance now need to catch up.

Development approach

26. A focus on improving cyber security and risk regulations in the financial services sector is critical to improving overall national posture. Strategy and policy measures to strengthen provision of commercial cyber security services and reinforce a broad professional development agenda should also be considered a priority.

National Cyber Security Strategy & Capabilities

Indicator 1.1 National Strategy & Policy

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

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

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

28. **The Law on Electronic Information and Transactions (ITE),** enacted in 2008[17] and amended by Law no 19 of 2016[18] is the current cyber regulation. It covers information, electronic transactions, and information technology in general[19]. In an explanation on page 16, it states the law is for the sole purpose of guaranteeing recognition and respect for the rights and freedoms of others and to meet fair demands in accordance with moral considerations, religious values, security, and public order in a democratic society[20]. The 2016 Amendment also covers investigator's powers and consequences of breaking the law - from fines to imprisonment[21]. The original sources are in Indonesian.

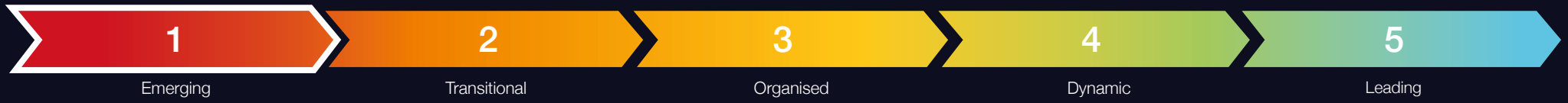
29. **The Ministry of Communication and Information Technology's (MOCI)**[22] Information Security Coordination Team is responsible for coordinating and developing policy and technical guidelines on the implementation of information security measures[23]. The same Ministry is the parent body to the official **Government Information Security Incident Response Team (ID-SIRTII/CC),** established in 2007[24].

30. The most recent piece of legislation regarding security of information, and linked to the digital economy, was issued in 2019. Government Regulation No. 71 of 2019 on Organization of Electronic Systems and Transactions (GR 71/2019) replaces Government Regulation No. 82 of 2012 with the same title[25]. A 2019 article in Conventus Law states the new regulation has wide scope, covers private and public sector electronic system organisers ("ESOs") and requires them to be registered with the Ministry of Communication and Information Technology (MOCI) before they can operate.

    The regulation also provides the right to be forgotten under Law No. 19 of 2016 on amendments to Law No. 11 of 2008 on Information Technology and Electronic Transactions, and requires ESOs to delist owner's information upon request[26].

National Cyber Security Strategy & Capabilities

Indicator 1.2 Regulator/Government Operated Assurance Schemes



Assessment – *Maturity Level 1*

No regulator operated assurance schemes identified. Limited financial services regulation by Central Bank. Little evidence of regulators operating in other sectors.

The central bank (Bank of Indonesia) 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.

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

32. The Financial Services Authority (OJK) of Indonesia is the monitoring institution that oversees the financial services industry[27]. The OJK website offers no publicly available cyber policy for the financial sector, as was also the case with Bank of Indonesia.

33. In terms of combatting cybercrime, a 2015 news release on the Bank of Indonesia's website reported that the Bank and Indonesian Police were working together to prevent cybercrime in the payment system. It stated that while fraud within the payment system is still relatively low in comparison to other countries, the modus operandi was increasingly varied - and that working with the Police was expected to provide a deterrent to the perpetrators[28].

National Cyber Security Strategy & Capabilities

Indicator 1.3 Law Enforcement & Cyber Defence Capabilities

Assessment – *Maturity Level 3*

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).

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

35. A 2015 Indonesian Ministry of Defence white paper calls for modernisation of cyber capabilities[29]. T**he white paper lists cybercrime and cyberspace war as security concerns**, identifying cyberspace as the fifth domain used as a battlefield[30].

36. The Cyber Defence Guidelines (Ministerial Regulation No. 82 of 2014) form the basis for the Ministry of Defence's implementation of cyber defence. The guidelines identify hacking activists and organised crime groups as cyber defence attackers[31]. Chapter 4.4, the phasing of cyber defence activities, mentions cyber defence trials with other agencies such as CSIRT[32]. It is assumed this is with the National Information Security Incident Response Team (ID-SIRTII/CC) as opposed to a Military CERT, of which no mention was found.

37. **The military established a Cyber Defence Operations Centre in 2013**[33] and the only other information about the Indonesian National Army (TNI) Cyber Unit (Satsiber TNI) found in CREST's research was in a structural diagram on the Indonesian Armed Forces[34] website and on Wikipedia. The unit, active since April 2017, is tasked with carrying out cyber activities and operations within the TNI to support the military's main tasks[35].

38. **The Indonesian National Police (INP) Cybercrime Unit**[36] is a separate police directorate dedicated to cybercrime, led by a one-star police general with 100 personnel. Its aim is to increase the force's capacity to tackle the growing number of criminal threats in cyberspace, via more personnel, a larger budget and by creating three specific departments delaing with economic cybercrimes, cyberterrorism and general cybercrimes[37].

39. The INP cooperates with international partners, including the Australian Federal Police (AFP), engagement with INTERPOL and via hosting the ASEANPOL Police Training Cooperation Conference in October 2015[38].

40. In 2011, the INP and AFP initiated a Cyber Crime Investigation Centre Satellite Office (CCISO). This digital forensics laboratory holds ISO 17025 accreditation[39].

    A 2013 article in the Jakarta Post (2013) stated additional CCISO offices were established in some regional Police Headquarters, with equipment provided by the AFP. However, the article also stated information sharing and intelligence cooperation between the AFP and INP had been suspended due to suspected spying by the AFP on Indonesian officials[40].

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.

41. There is no commercial advantage in withholding information. Open publication of academic research and use of sector-specific information exchanges are example mechanisms for sharing information on cyber security risks, threats, and vulnerabilities. There is not much evidence of either of these mechanisms being currently well established in Indonesia.

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

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

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

Overall Assessment

44. Excluding the inactive academic CERT, Indonesia has two active CERTs, ID-SIRTII/CC and ID-CERT. They were established in 2007 and 1998 respectively and are both members of the Asia Pacific Computer Emergency Response Team (APCERT)[41].

    ID-SIRTII/CC is the official CERT, hosted by BSSN, and a member of the Forum of Incident Response and Security Teams (FIRST)[42]. Given each CERT's external links it is assessed that Indonesia is at Maturity Level 3.

Development Approach

45. 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) & Information Sharing

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.

46. **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

47. Information on the academic **CSIRT (Computer Security Incident Response Team)** was found from its own website, but not having been updated since 2013, this CSIRT may not be active. The Academic CSIRT was established in 2011 for universities which want to focus on developing computer security in Indonesia. It has 40 members from both academia and industry.[43]

48. The official CERT for Indonesia is the Information **Security Incident Response Team (ID-SIRTII/CC)**[44], established in 2007 by the Minister of Communication and Information[45]. Its mission is to:

    - Increase internet growth via awareness campaigns to safeguard technology and information systems
    - Monitor potential security incidents
    - Support law enforcement, and
    - Provide technical support[46].

    It provides a wide range of cyber security services, including forensics, which it supports law enforcement agencies with by providing electronic evidence of cybercrimes. As previously mentioned, it is a member of both APCERT and FIRST, which gives the SIRTII/CC regional and international support and influence.

49. The Indonesia Computer Emergency Response Team (ID-CERT) is an NGO, established in 1998. ID-CERT's purpose is to coordinate incidents locally and internationally and help increase internet security awareness in Indonesia[47]. It is a member of APCERT. At the time of drafting this report, ID-CERT's website was inaccessible, so no further information was gained direct from source.

Dimension 3

Cyber Security Service Provision

Cyber Security Service Provision

Overall Dimension Assessment: *Maturity Level 2*

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

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

Overall Assessment

53. Indonesia is currently assessed as being at Level 3 across all service provision disciplines, excluding SOC services. There are no local CREST member companies, but twelve CREST member companies already have offices in Indonesia. There is a healthy number of local service providers across most disciplines, but their standards have not been benchmarked.

Development Approach

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

Cyber Security Service Provision

Indicator 3.1 Threat Intelligence Providers

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

Assessment – *Maturity Level 3*

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.

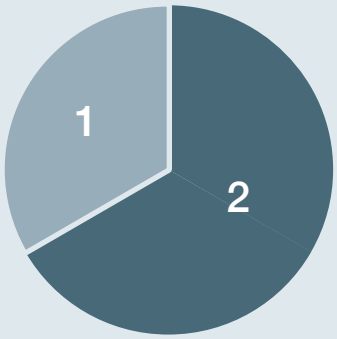
Cyber Threat Intelligence

55. Cyber Threat Intelligence (CTI) is information about current and future cyber threats and actors that adversly affect a nation's or organisation's cyberspace. Cyberspace can be defined as an interactive domain made up of digital networks[48]. Threat Intelligence includes open source information, and intelligence from technical, human, social media and dark web sources.

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

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	3	5	8
Regional	0	0	0
International	1	4	5
Total	**4**	**9**	**13**

57. **There are 13 companies providing Cyber Threat Intelligence services** into Indonesia. Five of the companies with offices located in-country are CREST-accredited international organisations. This is positive news, showing that companies of this calibre are investing in Indonesia.



Of the three others based in-country, **one is an international company and the other two are Indonesian.**

58. **There are a further five international companies that can provide services** into Indonesia, though our research did not find how often their services are used by Indonesian clients.

Cyber Security Service Provision

Indicator 3.2 Vulnerability Assessment Providers

Assessment – *Maturity Level 3*

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

Vulnerability Assessment (VA)

59. Vulnerability Assessment (VA) is defined by CREST as: "The examination of an information system or product to determine the adequacy of security measures, the identification of security deficiencies, to predict the effectiveness of the proposed security measures and to confirm the adequacy of such measures after implementation[49]." As with Threat Intelligence, research focused on looking for companies which provide VA services in Indonesia, ideally based in-country.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	8	8	16
Regional	0	0	0
International	2	8	10
Total	**10**	**16**	**26**

60. CREST's research found **26 companies providing Vulnerability Assessment (VA)** services into Indonesia. **Eight companies based in-country are CREST-accredited international organisations.** Encouragingly, **a further seven are not CREST-accredited, but *are* Indonesian companies.** The remaining company is international, with an office in Indonesia.

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

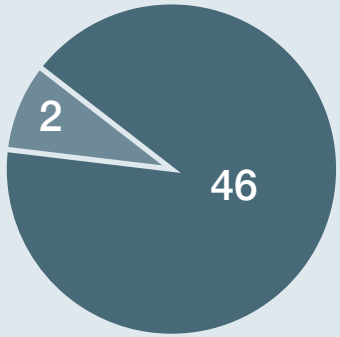
61. The UK's National Cyber Security Centre (NCSC) defines penetration testing as: "A method for gaining assurance in the security of an IT system by attempting to breach some or all of that system's security, using the same tools and techniques as an adversary might. Penetration testing should be viewed as a method for gaining assurance in your organisation's vulnerability assessment and management processes, not as a primary method for identifying vulnerabilities[50]."

62. CREST's research found significantly more companies providing penetration testing than any other cyber security service, although many service providers offer more than one cyber security service. In assessing the maturity of the cyber industry, CREST's efforts focused on looking for as many service providers based in Indonesia as could be identified.

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	12	12	24
Regional	0	0	0
International	2	46	48
Total	**14**	**58**	**72**

63. There are a **significant number of companies providing penetration services based in Indonesia, 50% of which are CREST International-accredited members** with local offices. Of the Indonesia-based non-CREST accredited companies, **11 are Indonesian and one is an international organisation.**

64. As expected with a service such as penetration testing, there are several companies offering this service. With the substantial number of international companies not based in Indonesia, it is difficult to assess how many actually provide their services to Indonesian clients.



There are **48 international organisations providing penetration services into Indonesia** from international offices, **46 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.

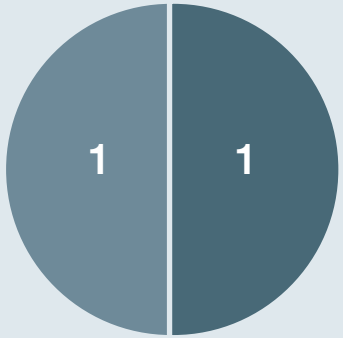
Security Operations Centres

65. **CREST defines a Security Operations Centre as:** "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[51]."

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

Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	0	3	3
Regional	0	2	2
International	1	1	2
Total	1	6	7

67. **There are seven companies offering SOC services into Indonesia.** All except one are CREST-accredited, and all are either international or regional organisations.



There are only **2 international companies, 1 of them being CREST-accredited,** which offer their services into Indonesia at clients' request.

Cyber Security Service Provision

Indicator 3.5 Incident Response Providers

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

68. **Incident response to a cyber security incident is defined by CREST as:** "An information (or IT) security incident that could be classified as a cyber security incident ranges from serious cyber security attacks on critical national infrastructure and major organised cybercrime, through hacktivism and basic malware attacks, to internal misuse of systems and software malfunction[52]."

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

70. **There are 28 companies offering SOC services in Indonesia.** A majority are CREST-accredited international organisations. Of the companies based in-country, of note are the Indonesian ID-CERT and ID-SIRTII/CC.

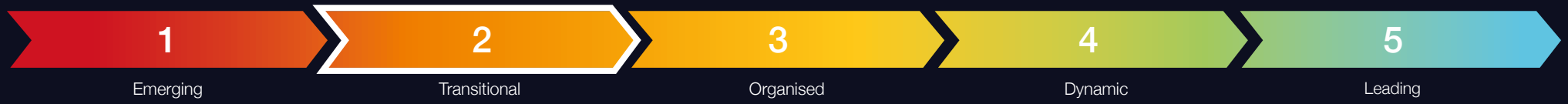
Office Location	Non-CREST Accredited	CREST Accredited	Total
In-country	5	8	13
Regional	0	3	3
International	2	10	12
Total	**7**	**21**	**28**

Dimension 4

Cyber Security Professional Development

Cyber Security Professional Development

Overall Dimension Assessment: *Maturity Level 2*



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

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

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

Overall Assessment

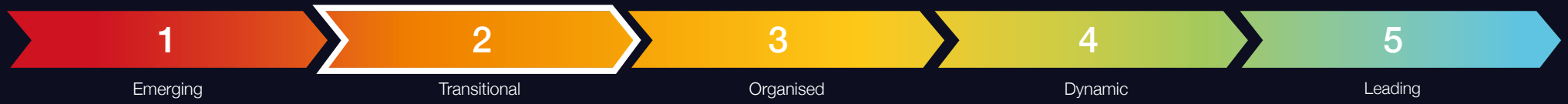
73. The six professional development indicators provide a mixed assessment – ranging from Level 3 for Professional Bodies and Events to Level 1 for Specialist Recruitment. The lack of cyber security degrees at Indonesian universities is particularly disappointing, but a national hacking competition is something of a high point.

Development Approach

74. Partnerships between local universities and internationally renowned institutions elsewhere could improve cyber security education opportunities. Investment in certifications and strengthening local chapters of professional bodies would also improve matters.

Cyber Security Professional Development

Indicator 4.1 Academia & Higher Education



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

Academia and Higher Education

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

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

77. **Of the 28 universities researched, CREST found approximately 66 ICT and computer science courses, ranging from undergraduate to postgraduate**. However, given the government's focus on improving cyber security across the country, **it is surprising that only one university (Binus University) offered cyber security degrees.**

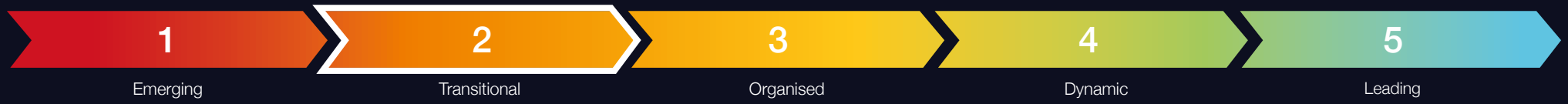
    Of the many universities that do offer computer science and similar degrees, the security content of these courses is not known. **A team from the University of Indonesia won the 2019 national hacking competition, Cyber Jawara**[53], so, it can be assumed that while cyber security content is being taught, it is just not visible on university websites.

	BA/BSc	MSc	PhD	Total
ICT Courses	53	8	5	66
Cyber Cources	1	0	0	1
Total	**54**	**8**	**5**	**67**

78. 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



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

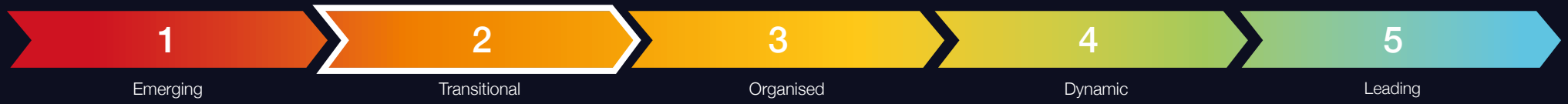
Training Providers

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

80. **Thirteen training providers were found during CREST's research, including a mix of local and international companies,** and Indonesia's CERT, ID-SIRTII/CC was one. There was a good mix of instructor lead and online training provided.

Cyber Security Professional Development

Indicator 4.3 Professional Certifications



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

Professional Certifications

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

82. **Fifteen organisations offering professional certifications were found operating in Indonesia**. Most offered certifications with online exams, or through Pearson Vue or PSI test centres, available in-country. Some certifications require practical exams and offer this element online or through connection to a remote network, but some only offer exams at specific testing sites, with these bodies offering multiple sites across Asia.

83. **Take-up of certifications is low in Indonesia,** judging by the information gathered. Certification body chapter involvement (if offered) is in initial stages, with two established chapters in Jakarta (ISACA and (ISC)2) having meetings and other engagement opportunities, and one under development (Cloud Security Alliance).

Cyber Security Professional Development

Indicator 4.4 Professional Cyber Membership Organisations

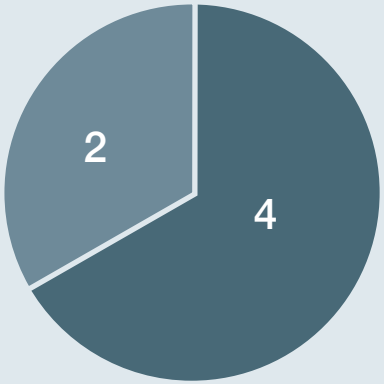
Assessment – *Maturity Level 3*
Some evidence of local cyber security membership organisations for individuals and/or companies.

Professional Cyber Membership Organisations or Associations

84. **Professional membership organisations or associations usually focus on furthering the profession they represent.** They provide membership by subscription. Membership benefits range from 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.

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

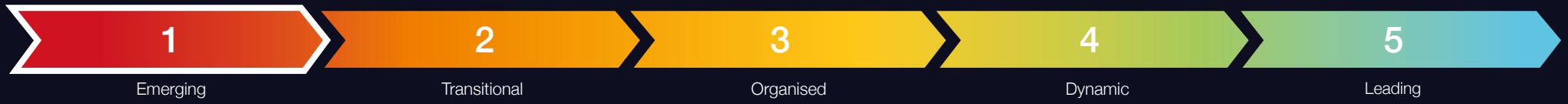
86.



There were six cyber security professional membership bodies found during research. **Four are well known international organisations**, and encouragingly, **two are local Indonesian organisations.**

Cyber Security Professional Development

Indicator 4.5 Specialist Recruitment



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

Specialist Cyber Recruitment

87. 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 Indonesia, or marketed cyber-qualified freelance professionals registered with them.

88. **Only three recruitment organisations were found during the research, all were international, and none were specific cyber-security recruitment companies.**

89. From the evidence of online recruitment activity, **some job advertisements referred to a wide variety of certifications with Offensive Security**, (ISC)2, Cisco, ISACA and EC Council being the most popular.

Cyber Security Professional Development

Indicator 4.6 Events & Exhibitions

Assessment – *Maturity Level 3*
Evidence of regular locally-organised dedicated cyber security events/exhibitions being run in-country

Events and exhibitions

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

91. CREST's research found eleven recent cyber security or information security events in 2019 and 2020, with some planned for 2021. These future events include the 9th Cyber Intelligence Asia 2021 Conference[54] to be held in Jakarta in October 2021 and the 9th World Conference on Cyber Security and Ethical Hacking (WCCSEH)[55] currently planned for September 2021.

92. In the 2016 ASPI report, "Cyber Maturity in the Asia-Pacific Region", it states Indonesia has increased efforts to engage youth in cybersecurity through events such as the Indonesia Cyber Army[56], Cyber Jawara (the national hacking competition and workshop)[57] and Cyberkids Camp[58]. The Association of South East Asia Nations' (ASEAN)[59] Cyberkids Camp is run by different member nations each year, for school children under 12 years old. The Indonesian team won in 2017[60].

93. **Events ranged from those aimed at high-level professionals to regional and local events aimed at children and student participation** - which is good to see.

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

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

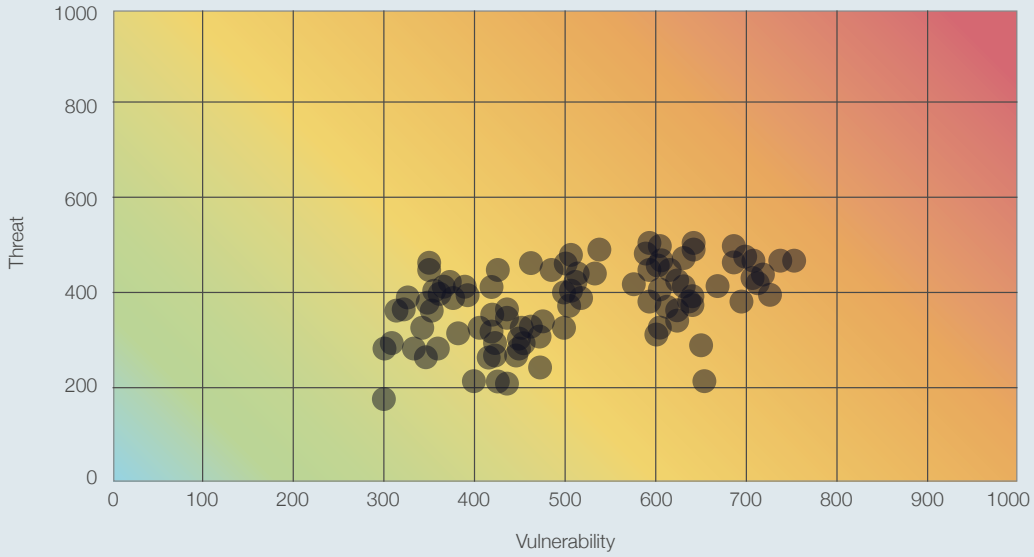
    Its brief was to examine the cyber security risk rating of each financial institution against a series of non-intrusive metrics, including:

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

    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, 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

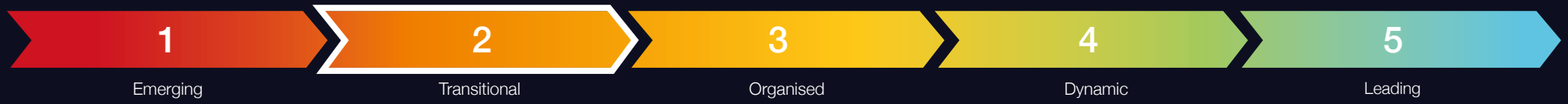
Figures represent CREST's cyber risk rating of each financial institution against a series of non-intrusive metrics



95. In determining the financial institutions to be assessed, the first source was the latest (2015) list of supervised institutions maintained by the Financial Services Authority (Indonesia)[61]. This information was cross-checked against membership information from the Indonesia Banker Institute[62], Wikipedia[63] and the websites of the financial institutions themselves, to generate a representative sample of national and international banks and microfinance institutions (MFIs) operating in Indonesia. The website addresses and email domains of 97 financial institutions were passed to Orpheus Cyber for initial assessment. The results contained in this report relate to assessments undertaken on these institutions in October 2020. For ethical reasons, all results have been anonymised.

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile



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

Banking Sector Cyber Risk Profile

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

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

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

As visible in the scatter diagram on the previous page, assessed financial institutions have been found to have **individual vulnerability scores (X-axis) ranging between 300 and 750.** The **average cyber risk score** for the sample is **440**, which corresponds to a national average risk rating of '**Medium**'.

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

Banking Sector Cyber Security Posture

Indicator 5.1 Banking Sector Cyber Risk Profile (continued)

1	2	3	4	5
Emerging	Transitional	Organised	Dynamic	Leading

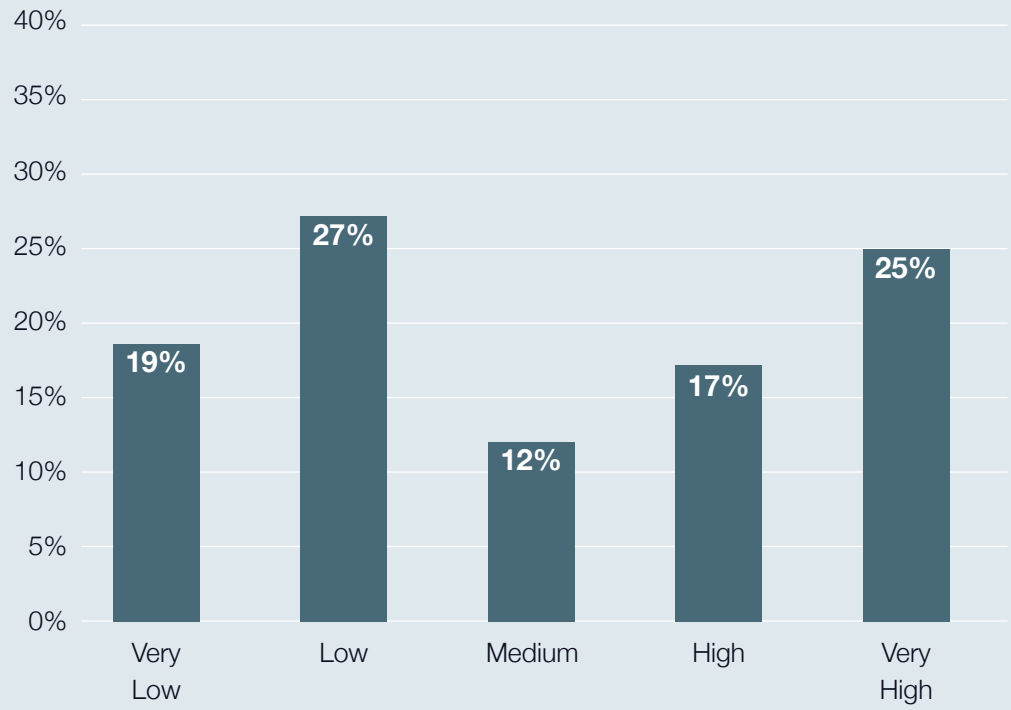
Assessment – *Maturity Level 2*

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

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

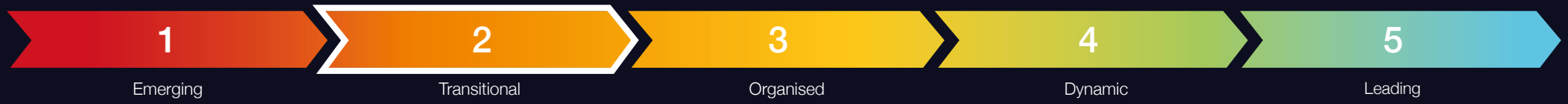
99. A breakdown by category of risk rating of the assessed sample of financial institutions is shown above, and results anonymised. **Encouragingly, 46% of the financial institutions have an overall cyber risk rating of 'Very Low' or 'Low'.** But 42% of the financial institutions have an overall cyber risk rating of 'Very High' or 'High'. Institutions in these latter two categories appear likely to not be implementing good cyber hygiene practices and/or to be operating vulnerable infrastructures. Consequently, they face higher levels of cyber risk.

Breakdown of Indonesia'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

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

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

101. Vulnerabilities, often referred to as CVEs (Common Vulnerabilities and Exposures)[64], 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 research followed a similar approach, scanning the public-facing IT infrastructure of all 97 of Indonesia's financial institutions being assessed. By restricting themselves to passive reconnaissance only, researchers were unable to confirm if the vulnerabilities they detected actually existed. There is a possibility that in some cases they were false positives.

102. **The investigation revealed 51% of Indonesia's financial institutions appear to operate an unsecure internet-facing infrastructure, featuring at least one known vulnerability.** The vulnerabilities detected mostly have patches available. Their presence on an internet-facing infrastructure suggests lax patching practices.

103. Each CVE is analysed and assigned a severity score ranging from 0 to 10, with 10 being the most severe. This score is known by the acronym CVSS (Common Vulnerability Scoring System)[65]. Vulnerabilities with a score of 9 or more are classed as critical. Critical vulnerabilities are often prioritised by those with malicious intent because of the ease with which they can be exploited, or the access they provide when successfully exploited. **CREST's research identified that 18% of Indonesia's assessed financial institutions were operating internet-facing IT infrastructure containing at least one critical vulnerability.** In those financial institutions with critical vulnerabilities, these results are indicative of a failure to adopt an 'attacker's eye perspective' and prioritise critical CVEs for remediation.

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk

Assessment – *Maturity Level 3*
Architecture & Access risk is assessed as average. 25% or fewer of the financial institutions were identified as having potential remote access vulnerabilities and 25% or fewer were identified as having potential database vulnerabilities.

Architecture & Access Risk

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

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

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

106. If a server is misconfigured and one or more ports are unintentionally left open (and unguarded), then cybercriminals can potentially gain access and compromise the computer network. In the same way 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.

107.

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

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

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

Banking Sector Cyber Security Posture

Indicator 5.3 Architecture & Access Risk (continued)

CREST's research shows just 9% of assessed financial institutions maintain at least one port associated with remote access services open to the internet.

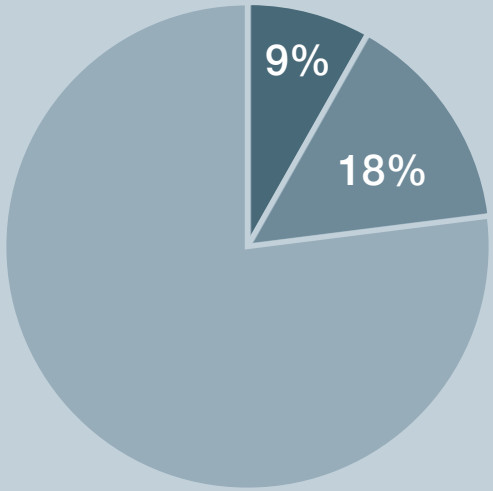
108. In most cases, these ports are configured to accept incoming data packets from the internet for valid business requirements and will have adequate security measures in place. Although banks with open remote access ports on their IT infrastructure remain susceptible to potential compromise, they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

109. Another set of ports cybercriminals deliberately target are those used by database services. **CREST's research shows 18% of the assessed financial institutions have at least one database-related port open on their public-facing infrastructure.** Although some of these internet-accessible database services are in place to meet valid business requirements and configured with adequate security controls, others could be incorrectly configured and susceptible to targeting by cybercriminals.

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

111. Understanding the threat associated with exposed database instances and reducing the possibility of suffering a data leak also reduces the risk of contravening Indonesia's various data protection regulations[66].

Indonesia's financial institution Access risk - open ports



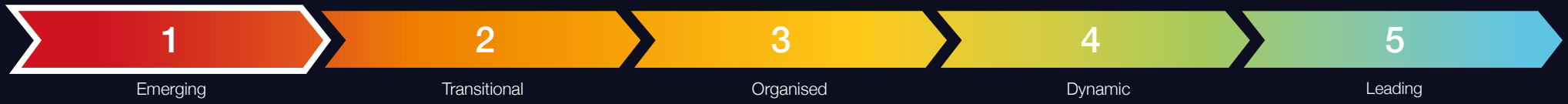
Key

9% - have remote access services open to the internet

18% - have at least one database-related port open to the internet

Banking Sector Cyber Security Posture

Indicator 5.4 Email Authentication Risk



Assessment – *Maturity Level 1*

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

Email Authentication Risk

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

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

114. SPF is regarded as the minimum (basic) standard to safeguard against spoofing and impersonation. DMARC is a more advanced security mechanism that, when correctly enabled, signals a strong cybersecurity posture. While it is still not as commonly implemented as SPF, recent global statistics confirm DMARC implementation rates are growing, with a corresponding decline in domain spoofing[67].

115. 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[68].

116. 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**[69].

117.

58%

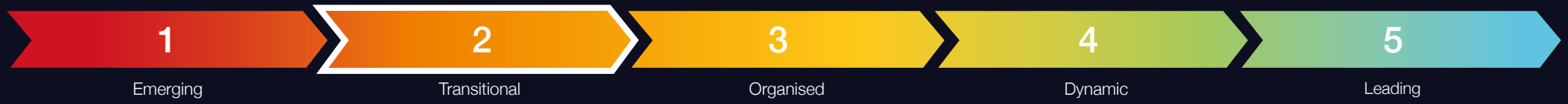
CREST's research revealed that **58% of the sample of financial institutions had not implemented basic email authentication measures (SPF)**.

69%

69% of the sample had not implemented advanced email authentication measures (DMARC). This suggests 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

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

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

> **54%** CREST's research revealed that **54% of assessed financial institutions had had at least some employee credentials leaked online** after unconnected attacks on third-party website-based service providers.

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

121. It has not been possible to verify how many of the assessed financial institutions follow good hygiene practices and enforce strong password best practices – measures that help mitigate the threat associated with third-party leaked credentials. **However, the high percentage of financial institutions who have fallen victim to third-party breaches suggests the sector remains vulnerable to such threats.**

Banking Sector Cyber Security Posture

Mitigation Measures

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

Infrastructure Vulnerability

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

Architecture & Access

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

Email Authentication

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

Information Leakage

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

Appendices

Appendix A

Glossary

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

Appendix A

Glossary (continued)

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

Appendix B

Summary of Maturity Level Definitions

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

Indicator 1.1
Government Strategy & Policy

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

Indicator 1.2
Regulator/Government Operated Assurance Schemes

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 1.3
Law Enforcement & Cyber Defence Capabilities

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 2.1
CERTs & Information Sharing

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

Indicator 3.1
Threat Intelligence Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.2
Vulnerability Assessment Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.3
Penetration Testing Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.4
Security Operation Centre Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 3.5
Incident Response Service providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.1
Academia & Higher Education

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

Indicator 4.2
Training Providers

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.3
Professional Certifications

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

Indicator 4.4
Professional Cyber Membership Organisations

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 4.5
Specialist Recruitment

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

Indicator 4.6
Events & Exhibitions

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.1
Banking Sector Cyber Risk Profile

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

Indicator 5.2
Infrastructure Vulnerability Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.3
Architecture & Access Risk

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

Indicator 5.4
Email Authentication Risk

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

Appendix B

Summary of Maturity Level Definitions (continued)

Indicator 5.5
Information Leakage Risk

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

Appendix C

Professional Certifications and Member Organisations

Background

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

Career progression model

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

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

Certification bodies

3. During CREST's research fifteen organisations were identified 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[70]		CPSA CPIA CPTIA	CRT CRTIA CRTSA CRIA CC NIA CCHIA CCMRE	CCSAS CCSAM CCTIM, CCIM CCT Inf CCT App CCWS	Fellow		✓			✓
EC Council[71]	CEH CND ECSS	ECSA ECIH EDRP CASE-Java CASE-.Net ECES CTIA	APT LPT CHFI CAST CEH(Master) CSA	ECDA ECTI		✓	✓		✓	
ISACA[72]		CSX-P	CISA CRISC CISM		CGEIT	✓		✓		
(ISC)2[73]		HCISPP SSCP CAP	CISSP CCSP CSSLP		CISSP-AP CISSP-EP CISSP-MP		✓			
SANS[74]		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[75]	Pentest+ Security+	CySA+	CASP+			✓	✓			
Offensive Security[76]		OSCP OSWP	OSCE OSWE	OSEE		✓				
Cloud Security Alliance[77]		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[78]		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[79]		CCNA CC CyberOps Associate	CCNP Security CC CyberOps Professional	CCIE Security			✓			✓
Microsoft[80]	MTA: Security Fundamentals	Azure Security Engineer Associate Microsoft 365 Security Administrator Associate				✓	✓			
Amazon Web Services[81]	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)[82]	Associate Auditor	Internal Auditor	Auditor	Lead Auditor	Principle Auditor				✓	
BCS[83]	CiSMP	BCM CIAA	CIRM				✓		✓	✓
IET[84]	ICTTech									✓

Appendix D

Country Context

Geography

1. Indonesia is an archipelago of 17,500 islands, 7,000 of which are uninhabited[85]. It lies in the Indian and Pacific Oceans, sitting on a major juncture in the Earth's tectonic plates and its neighbours are Malaysia, the Philippines, Australia, Papau New Guinea and East Timor[86].

Natural resources

2. Indonesia has diverse natural resources, most of which are not fully prospected. Crude oil, natural gas and coal are major revenue sources, and the country is a world leading exporter of coal[87]. Other mineral deposits also contribute to Indonesia's economy. It is also one of the world's leading tin producers, and holds significant nickel, manganese, copper and gold deposits[88].

3. Less than one fifth of its total land surface is devoted to crop cultivation, and these are mainly rice and cash crops. Rubber, coffee, palm oil, sugar, tea, tobacco and spices are also grown[89].

Population

4. As of 2019, Indonesia was the world's fourth most populous nation,[90-91] with a population of 274,056,00[92]. There are 300 different ethnic groups and twice as many ethnic languages[93]. The population is split 55.3% urban to 44.7% rural[94].

5. As of 2016, literacy rates for over 15-year-olds were 97.2% in men and 93.6% among women[95]. Regarding education, only 16% of young adults have tertiary education, but 90% of young men are employed regardless of education.

6. Among the female population, statistics show they become 30% more employable after tertiary education[96], therefore there is little incentive for men to gain further education, but good incentive for women to do so.

7. In health, 1 in 3 children under 5 years old suffer from stunting, which impairs brain development and future opportunities[97].

Economy

8. Indonesia has the tenth largest global economy. Some 9.4% of the population sit below the poverty line, and a further 20.6% of the population are vulnerable of falling into poverty[98]. Much industry centres on production and processing of the key natural resources previously mentioned: crude oil, natural gas, rubber, coffee, palm oil, sugar, tea, tobacco and spices[99]. As at 2017, GNI per capita is US$3,540[100].

Internet connectivity

9. The telecommunications market is liberalised and includes eight mobile companies and 35 infrastructure-owning ISPs. 4G connectivity is now available nationwide[101].

10. In absolute numbers, Indonesia has the fourth largest growth in internet users, after India, China and the USA. As of January 2019, 56% of the population, approximately 150 million people, are classed as internet users[102]. Internet use and economic growth are developing faster than government cyber strategy and the education system, making it an attractive target for cybercrime.

Appendix D

Country Context (continued)

Cyber crime

11. The following summarises articles regarding cybercrime and issues related to cybercrime in Indonesia:

    a. A 2017 Jakarta Post article commented on expansion of the police cybercrime unit. The article mentions that in handling cybercrime, the police tend to focus more on cases related to online defamation, since it is easier to obtain evidence for them and takes a shorter time to conduct investigations[103].

    b. A 2019 article in The Conversation stated that in 2018 Indonesia suffered 200 million cyber attacks[104]. Indonesia, it said, with the world's fourth largest growth in internet users, faces both great opportunities and significant threats with the development of digital technology and internet. The article states the only current regulations on cyber security are the 2016 Law on Electronic Information and Transactions and the 2012 Government Regulation on Implementation of Electronic Systems and Transactions.

    c. The article also states that in 2017, the government established the National Cyber and Crypto Agency to coordinate various institutions in implementing cyber security. In 2014, a study found just under 3% of government agencies were secure. This is evidence that Indonesia is still in the early stages of developing secure digital infrastructure[105].

    d. The 2019 Jakarta Globe article 'Hacktivists, Bots, Elections: Indonesia Stepping Up Its Cybersecurity'[106] stated one rapidly growing cybercrime is bots attacking credentials and check-ins. The article suggests cyber attackers are becoming more dangerous, due to rapid evolution of attack methods, easily staying ahead of security software developments. It also commented that while cybersecurity has improved in Indonesia over the past five years, and the establishment of the State Cyber and Crypto Agency has helped the country's cyber security posture, the use of botnets makes it easier to conduct attacks without building any infrastructure. Therefore, says the author, the role of government is crucial in preventing hacktivists from interfering with elections - and they should develop a security response team[107].

Cyber Security Professional Development

12. No significant information was found about cyber security professional development during CREST's research, other than in the article 'The Cyber Security Agency's Challenge in Indonesia' by Jon Watada (2018). This article states that as Indonesia is a net information exporter, with information highways pointing west and carrying the data of millions of residents[108], there is a need for government strategy and standards to protect and communicate cybersecurity threats. There is also a need for highly skilled staff, and to establish roles and responsibilities for critical infrastructure providers, regulators and law enforcement, military and intelligence, and private industry. The article also pushes the need for cybersecurity situational awareness for all previously mentioned[109].

13. In a 2016 ASPI report "Cyber Maturity in the Asia-Pacific Region," it comments that Indonesia has increased its efforts to engage youth in cybersecurity through events such as the Indonesia Cyber Army, Cyber Jawara and Cyberkids Camp[110].

Appendix D

Country Context (continued)

Other maturity models

14. Oxford University's Global Cyber Security Capacity Centre (GCSCC)[111] has yet to publish its report on Indonesia. However, there is a 2016 working paper, "The Future of Cyber Security Capacity in Indonesia – Top 20 Recommendations for Strengthening National Cyber Security Capacity"[112] produced by the Oxford Internet Institute.

15. In the 2016 ASPI report, "Cyber Maturity in the Asia-Pacific Region," Indonesia is covered on page 39[113]. It ranks Indonesia 12th in cyber maturity of the 23 countries covered in the report, and comments that Indonesia has maintained its bilateral engagements with Australia, Japan, the US and China. It states Indonesia cooperates in the Asia–Pacific region through APCERT, ITU-IMPACT and ASEAN, and initiated and hosted the first ASEAN Cyber Security Competition in November 2015[114].

16. The National Cyber Security Index ranks Indonesia as 75th in the world[115].

Appendix E

Bibliography

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

Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia. USA: *Encyclopaedia Britannica (online)* **https://www.britannica.com/place/Indonesia** (Accessed 15 February 2021).

Aritonang, Margareth S. (2017). Police to Support National Cyber Agency. Indonesia: *The Jakarta Post.* **https://www.thejakartapost.com/news/2017/01/04/police-to-support-national-cyber-agency.html** (accessed Jul 20)

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

Asia Pacific Computer Emergency Response Team. (APCERT). APCERT Report 2019. *Author (online)* **https://www.apcert.org/documents/pdf/APCERT_Annual_Report_2019.pdf** (accessed Jul 20)

Association of South East Asia Nations (ASEAN). **https://asean.org/** (accessed Feb 21)

Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

Ayu Mathilda Glan (2021). BSSN: Inaugurates CyberHub as an effort to realise a Cyber Security Strategy. Indonesia: *Cloud Computing Indonesia* (online). **https://www.cloudcomputing.id/berita/bssn-resmikan-cyberhub-upaya-terwujudnya-strategi-keamanan-siber** (accessed Mar 21)

Bank of Indonesia, (2015). News Release: BI AND POLRI COORDINATE TO PREVENT CYBERCRIME. Indonesia: *Author.* (online) **https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_173115.aspx** (accessed Feb 21)

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

BSA Software Alliance (2015) | Asia-Pacific Cybersecurity Dashboard- Indonesia. Washington DC: *Author.* **http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_indonesia.pdf** (accessed July 20)

Coventus Law (2019). Indonesia – New Government Regulation on Organization of Electronic Systems and Transactions. Hong Kong: *Author* (online) **https://www.conventuslaw.com/report/indonesia-new-government-regulation-on/** (accessed Jul 20)

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)

Cyber Army Indonesia (2021). Indonesia: **https://www.cyberarmy.id/en** (accessed July 20)

Cyber Intelligence Asia Conference. **https://intelligence-sec.com/events/cyber-intelligence-asia-2021-3/** (accessed Jul 20 and Feb 21)

Cyber Jawara, National Hacking Competition and Workshop (2020). Indonesia. **https://cyberjawara.id/** (accessed Feb 21)

Appendix E

Bibliography (continued)

Data Guidance (2020). Indonesia: BSSN releases National Cyber Security Strategy for Public Consultation. *Author (online)* **https://www.dataguidance.com/news/indonesia-bssn-releases-national-cybersecurity-strategy** (accessed Mar 21)

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

Global Cyber Security Capacity Centre (2021). Indonesia (GCSCC) 2015 – not yet published. Oxford: Author, **https://gcscc.web.ox.ac.uk/cmm-reviews** (accessed Mar 2020)

Government of Indonesia (2008). Laws of Republic of Indonesia, no 11 of 2008, about Electronic Information and Transactions. Indonesia: *Author (online via google translate)* **https://www.dpr.go.id/dokjdih/document/uu/UU_2008_11.pdf** (accessed Jul 20 and Feb 21)

Government of Indonesia (2016). Laws of Republic of Indonesia, no 19 of 2016, Amendment to the Law no 11 of 2008, about Electronic Information and Transactions. Indonesia: Author (online via google translate) **https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf** (accessed Jul 20)

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

Hasibuan, Zainal A. Professor, (2013). Indonesian National Cyber Security Strategy: Security and Sovereignty in Indonesian Cyberspace. Indonesia: *National ICT Council (DETIKNAS)* (online). **https://www.slideshare.net/internetsehat/indonesia-national-cyber-security-strategy**

Hutagalung, Gunawan, MT (2008). Indonesia Security Incidents Response Team on Internet Infrastructure. Indonesia: *Telecommunication Regulatory Body of Indonesia.* **https://www.itu.int/ITU-D/finance/work-cost-tariffs/events/tariff-seminars/vietnam09-tas/pdf/Gunawan_SIRT.pdf**

Indonesia Academic CSIRT. **http://www.acad-csirt.or.id/aboutus.html** (accessed Jul 20 and Feb 21)

Indonesian Armed Forces, (2021). Organisational Structure of the TNI Headquarters. Indonesia: *Author.* (online) **https://www.tni.mil.id/** or **https://translate.google.com/translate?hl=&sl=id&tl=en&u=https%3A%2F%2Fwww.tni.mil.id%2** (accessed Feb 21)

Indonesia Computer Emergency Response Team (ID-CERT). **https://www.cert.or.id/beranda/en/** (accessed July 20)

Indonesian Cyber Army, (2021) **https://www.cyberarmy.id/en/tentang** (accessed July 20)

Indonesia National ICT Council (2017). Flagship DeTIKNas. Indonesia: *Author.* **https://docplayer.net/41528709-Flagship-detiknas-indonesian-national-ict-council.html** (accessed July 20)

Indonesia National Police (2017). Cyber Crime Directorate. Cebu: *Author.* (online) **https://rm.coe.int/03-a-country-report-indonesia1/168072bd1f** (accessed Jul 20)

Information Security Incident Response Team (ID-SIRTII/CC) **https://idsirtii.or.id/en/page/history-id-sirtii-cc.html** (accessed July 20 and Feb 21)

Jakarta Metropolitan Police. Cyber Crime Investigation Satellite Office (CCISO). Jakarta. (online) **https://www.linkedin.com/company/cyber-crime-investigation-center-cciso-jakarta-metropolitan-police/** (accessed Jul 20 and Feb 21)

Muslim, Abdul. (2017). Indonesia Wins ASEAN Cyberkids Camp 2017. Indonesia: *BERITSATU* (online) **https://www.beritasatu.com/archive/443333/indonesia-juara-i-asean-cyberkids-camp-2017** (accessed Feb21)

Appendix E

Bibliography (continued)

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

National Cyber Security Index
Estonia, *e-Governance Academy.* (online)
https://ncsi.ega.ee/ncsi-index/ (Accessed July 20)

National Documentation and Legal Information Network State Cyber and Password Agency (JDIH). (2015). Indonesia:
https://jdih.bssn.go.id/sekilas-jdih (accessed July 20)

Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford: *Internet Institute, University of Oxford.*
shorturl.at/vEKY9
(accessed Jul 20)

OECD (2019). Education at a Glance 2019 – Indonesia. *Author* (online).
https://www.oecd.org/education/education-at-a-glance/EAG2019_CN_IDN.pdf (accessed Jul 20)

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

Perdain Yalasin (2013). Police Suspend Cooperation with OZ. Indonesia: *The Jakarta Post.* (online)
https://www.thejakartapost.com/news/2013/11/25/police-suspend-cooperation-with-oz.html
(accessed Feb 21)

Salaam Gateway (2015). DETIKNAS Building Indonesia's ICT Infrastructure From the Top Down. *Author.* (online)
https://www.salaamgateway.com/story/detiknas-building-indonesias-ict-infrastructure-from-the-top-down (accessed July 20)

Sapiie, Marguerite Afra, (2017). Police Playing Tough in Combating Cybercrimes in Indonesia.
Indonesia: *The Jakarta Post*. (online)
https://www.thejakartapost.com/news/2017/02/06/police-playing-tough-in-combating-cybercrimes-in-indonesia-.html (accessed Jul 20)

State Cyber and Crypto Agency (BSSN) Government of Indonesia (2018). National Cyber Security Strategy.
Indonesia: *Author* (online)
https://bssn.go.id/strategi-keamanan-siber-nasional/
(accessed July 20)

State Cyber and Crypto Agency (BSSN), Government of Indonesia (2020). BSSN Completes Draft National Cybersecurity Strategy, It is Public Turn to Give Feedback.
Indonesia: *Author* (online).
https://bssn.go.id/bssn-rampungkan-draf-strategi-keamanan-siber-nasional-giliran-publik-berikan-masukan/ (accessed Mar 21)

State Cyber and Crypto Agency, Badan Siber dan Sandi Negara (BSSN), Government of Indonesia.
https://bssn.go.id/ (accessed July 20)

The Conversation. (2019). Cybersecurity for Indonesia: What Needs to be Done?
UK: *Author.* (online)
https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009
(accessed Jul 20)

The Financial Services Authority (OJK). Indonesia:
https://www.ojk.go.id/en/tentang-ojk/Pages/Visi-Misi.aspx (accessed Jul 20 and Feb 21)

The Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika) (2021)
https://www.kominfo.go.id/
(accessed Jul 20 and Feb 21)

The Ministry of Defence of The Republic of Indonesia (2015). Indonesian Defence White Paper 2015. ISBN 978-979-8878-04-6.
Indonesia: *Author* (online).
https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf
(accessed Jul 20 and Feb 21)

The Ministry of Defence of the Republic of Indonesia (2014). Cyber Defence Guidelines ii. Regulation of the Minister of Defence of The Republic of Indonesia Number 82 of 2014.
Indonesia: *Author* (online)
https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf
(accessed Jul 20, translated into English Feb 21)

Appendix E

Bibliography (continued)

The World Bank, (2020). The World Bank in Indonesia – Economic Overview. Jakarta: *Author.* (online) **https://www.worldbank.org/en/country/indonesia** (accessed July 20)

Top Universities (2021). Indonesia (online) **https://www.topuniversities.com/universities/indonesia/computer-science-information-systems?country=[ID]** (accessed Jul 20 and Feb 21)

UN, 'UNDIR Cyber Security Portal (2019). Indonesia. *Author.* **https://unidir.org/cpp/en/states/indonesia** (accessed July 20)

Uni-Rank (2021). Universities in Indonesia. (online) **https://www.4icu.org/id/universities/** (accessed Jul 20 and Feb 21).

Watada, Jon (2018). The Cyber Security Agency's Challenge in Indonesia. Indonesia: *The Jakarta Post.* **https://www.thejakartapost.com/academia/2018/05/04/the-cyber-security-agencys-challenge-in-indonesia.html** (accessed Jul 20)

Wikipedia (2017). Cyber Unit of the Indonesian National Army. *Author* (online). **https://id.wikipedia.org/wiki/Satuan_Siber_Tentara_Nasional_Indonesia#:~:text=Satuan%20Siber%20Tentara%20Nasional%20Indonesia%20disebut%20(Satsiber%20TNI)%20bertugas%20menyelenggarakan,rangka%20mendukung%20-0tugas%20pokok%20TNI.** (accessed Jul 20 and Feb 21)

World Population Review (2021) Indonesia Population 2021. USA: *Author.* (online) **https://worldpopulationreview.com/countries/indonesia-population** (accessed Jul 20 and Feb 21)

9th World Conference on Cyber Security and Ethical Hacking (WCCSEH), (2021) **http://www.wccseh.igrnet.org/146/indonesia/** (accessed Jul 20 and Feb 21)

Yasmin, Nur (2019). Hacktivists, Bots, Elections: Indonesia Stepping Up Its Cybersecurity. Indonesia: *Jakarta Globe* (online). **https://jakartaglobe.id/context/hacktivists-bots-elections-indonesia-stepping-up-its-cybersecurity** (accessed Jul 20)

Yunair, Resty Woro, (2018). Can Indonesia's New Cybercrime Unit Win its War on Fake News? *South China Morning Post* (online) **https://crestuk.sharepoint.com/sites/GatesFoundationTeam812-GatesCountries/Shared%20Documents/Gates%20Countries/Indonesia/Archive** (accessed Jul 20)

Appendix F

Endnotes

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

1. Further information available on the Bill & Melinda Gates Foundation, Financial Services for the Poor programme website, **https://www.gatesfoundation.org/What-We-Do/Global-Growth-and-Opportunity/Financial-Services-for-the-Poor** (accessed 29 Oct 2020)
2. Further information available on the CREST International website, **https://crest-approved.org/** (accessed 29 Oct 2020)
3. Further information available on the Orpheus Cyber website, **https://orpheus-cyber.com**/ (accessed 29 Oct 2020)
4. State Cyber and Crypto Agency, Badan Siber dan Sandi Negara (BSSN), *Government of Indonesia.* **https://bssn.go.id/** (accessed July 20)
5. Organisation of Islamic Cooperation-CERT (OIC-CERT), (2021) Members. (online **https://www.oic-cert.org/en/allmembers.html#.YDVwYWj7RPY** (accessed Feb 21)
6. State Cyber and Crypto Agency (BSSN) Government of Indonesia (2018). National Cyber Security Strategy. Indonesia: *Author* (online) **https://bssn.go.id/strategi-keamanan-siber-nasional/** (accessed July 20)
7. State Cyber and Crypto Agency (BSSN), Government of Indonesia (2020). BSSN Completes Draft National Cybersecurity Strategy, It is Public Turn to Give Feedback. Indonesia: *Author* (online). **https://bssn.go.id/bssn-rampungkan-draf-strategi-keamanan-siber-nasional-giliran-publik-berikan-masukan/** (accessed Mar 21)
8. Data Guidance (2020). Indonesia: BSSN releases National Cyber Security Strategy for Public Consultation. *Author* (online) **https://www.dataguidance.com/news/indonesia-bssn-releases-national-cybersecurity-strategy** (accessed Mar 21)
9. State Cyber and Crypto Agency (BSSN), Government of Indonesia (2020). BSSN Completes Draft National Cybersecurity Strategy, It is Public Turn to Give Feedback. Indonesia: *Author* (online) Slide 11. **https://bssn.go.id/bssn-rampungkan-draf-strategi-keamanan-siber-nasional-giliran-publik-berikan-masukan/** (accessed Mar 21)
10. State Cyber and Crypto Agency (BSSN), Government of Indonesia (2020). BSSN Completes Draft National Cybersecurity Strategy, It is Public Turn to Give Feedback.] Indonesia: *Author* (online) Slide 11-18. **https://bssn.go.id/bssn-rampungkan-draf-strategi-keamanan-siber-nasional-giliran-publik-berikan-masukan/** (accessed Mar 21)
11. Ayu Mathilda Glan (2021). BSSN: Inaugurates CyberHub as an effort to realise a Cyber Security Strategy. Indonesia: *Cloud Computing Indonesia* (online). **https://www.cloudcomputing.id/berita/bssn-resmikan-cyberhub-upaya-terwujudnya-strategi-keamanan-siber** (accessed Mar 21)
12. State Cyber and Crypto Agency (BSSN), Government of Indonesia (2020). BSSN Completes Draft National Cybersecurity Strategy, It is Public Turn to Give Feedback. Indonesia: *Author* (online) Slide 11-18. **https://bssn.go.id/bssn-rampungkan-draf-strategi-keamanan-siber-nasional-giliran-publik-berikan-masukan/** (accessed Mar 21)
13. Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford: I*nternet Institute, University of Oxford* **https://rc.telkomuniversity.ac.id/wp-content/uploads/2017/08/The-Future-of-Cybersecurity-Capacity-in-Indonesia_Research-Report_2016.pdf** (accessed July 2020)

Appendix F

Endnotes (continued)

14. Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford: *Internet Institute, University of Oxford.* Pp6-7 **shorturl.at/zNP45** (accessed July 2020)

15. Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford: *Internet Institute, University of Oxford.* Pp9-15. **shorturl.at/zNP45** (accessed July 2020)

16. Hasibuan, Zainal A. Professor, (2013). Indonesian National Cyber Security Strategy: Security and Sovereignty in Indonesian Cyberspace. Indonesia: *National ICT Council (DETIKNAS)* (online). Slide 19. **https://www.slideshare.net/internetsehat/indonesia-national-cyber-security-strategy**

17. Hasibuan, Zainal A. Professor, (2013). Indonesian National Cyber Security Strategy: Security and Sovereignty in Indonesian Cyberspace. Indonesia: *National ICT Council (DETIKNAS)* (online). Slide 19. **https://www.slideshare.net/internetsehat/indonesia-national-cyber-security-strategy**

18. Government of Indonesia (2008). Laws of Republic of Indonesia, no 11 of 2008, about Electronic Information and Transactions. Indonesia: *Author* (online via google translate) **https://www.dpr.go.id/dokjdih/document/uu/UU_2008_11.pdf** (accessed Jul 20 and Feb 21)

19. Government of Indonesia (2016). Laws of Republic of Indonesia, no 19 of 2016, Amendment to the Law no 11 of 2008, about Electronic Information and Transactions. Indonesia: *Author* (online via google translate) **https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf** (accessed Jul 20)

20. UN, 'UNDIR Cyber Security Portal (2019). Indonesia. *Author.* **https://unidir.org/cpp/en/states/indonesia** (accessed July 20)

21. Government of Indonesia (2016). Laws of Republic of Indonesia, no 19 of 2016, Amendment to the Law no 11 of 2008, about Electronic Information and Transactions. Indonesia: *Author* (p16) (online via google translate) **https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf** (accessed Jul 20)

22. Government of Indonesia (2016). Laws of Republic of Indonesia, no 19 of 2016, Amendment to the Law no 11 of 2008, about Electronic Information and Transactions. Indonesia: *Author* (P11) (online via google translate) **https://web.kominfo.go.id/sites/default/files/users/4761/UU%2019%20Tahun%202016.pdf** (accessed Jul 20)

23. The Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika) (2021) **https://www.kominfo.go.id/** (accessed Jul 20 and Feb 21)

24. BSA Software Alliance (2015) | Asia-Pacific Cybersecurity Dashboard- Indonesia. Washington DC: *Author.* (online) p2. **http://cybersecurity.bsa.org/2015/apac/assets/PDFs/country_reports/cs_indonesia.pdf** (accessed July 20)

25. Information Security Incident Response Team (ID-SIRTII/CC) **https://idsirtii.or.id/en/page/history-id-sirtii-cc.html** (accessed July 20 and Feb 21)

26. Coventus Law (2019). Indonesia – New Government Regulation on Organization of Electronic Systems and Transactions. Hong Kong: *Author* (online) **https://www.conventuslaw.com/report/indonesia-new-government-regulation-on/** (accessed Jul 20)

27. Coventus Law (2019). Indonesia – New Government Regulation on Organization of Electronic Systems and Transactions. Hong Kong: *Author* (online) **https://www.conventuslaw.com/report/indonesia-new-government-regulation-on/** (accessed Jul 20)

Appendix F

Endnotes (continued)

28. The Financial Services Authority (OJK). Indonesia: **https://www.ojk.go.id/en/tentang-ojk/Pages/Visi-Misi.aspx** (accessed Jul 20 and Feb 21)

29. Bank of Indonesia, (2015). News Release: BI AND POLRI COORDINATE TO PREVENT CYBERCRIME. Indonesia: *Author.* (online) **https://www.bi.go.id/en/publikasi/ruang-media/news-release/Pages/sp_173115.aspx** (accessed Feb 21)

30. Defence Ministry of The Republic of Indonesia (2015). Indonesian Defence White Paper 2015. ISBN 978-979-8878-04-6. Indonesia: *Author* (online) (Ch2.3 p 8). **https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf** (accessed Jul 20 and Feb 21)

31. Defence Ministry of The Republic of Indonesia (2015). Indonesian Defence White Paper 2015. ISBN 978-979-8878-04-6. Indonesia: *Author* (online) (Ch2.11 p16). **https://www.kemhan.go.id/wp-content/uploads/2016/05/2015-INDONESIA-DEFENCE-WHITE-PAPER-ENGLISH-VERSION.pdf** (accessed Jul 20 and Feb 21)

32. The Ministry of Defence of the Republic of Indonesia (2014). Cyber Defence Guidelines ii. Regulation of the Minister of Defence of The Republic of Indonesia Number 82 of 2014. Indonesia: *Author* (online) **https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf** (accessed Jul 20, translated into English Feb 21)

33. The Ministry of Defence of the Republic of Indonesia (2014). Cyber Defence Guidelines ii. Regulation of the Minister of Defence of The Republic of Indonesia Number 82 of 2014. Indonesia: *Author* (online) (Ch4.4-d-1 p44) **https://www.kemhan.go.id/pothan/wp-content/uploads/2016/10/Permenhan-No.-82-Tahun-2014-tentang-Pertahanan-Siber.pdf** (accessed Jul 20, translated into English Feb 21)

34. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp41. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

35. Indonesian Armed Forces, (2021). Organisational Structure of the TNI Headquarters. Indonesia: Author. (online) **https://www.tni.mil.id/** or **https://translate.google.com/translate?hl=&sl=id&tl=en&u=https%3A%2F%2Fwww.tni.mil. id%2F** (accessed Feb 21)

36. Wikipedia (2017). Cyber Unit of the Indonesian National Army. *Author* (online). **https://id.wikipedia.org/wiki/Satuan_Siber_Tentara_Nasional_Indonesia#:~:text=Satuan%20Siber%20Tentara%20Nasional%20Indonesia%20disebut%20(Satsiber%20TNI)%20bertugas%20menyelenggarakan,rangka%20mendukung%20-0tugas%20pokok%20TNI.** (accessed Jul 20 and Feb 21)

37. Indonesia National Police (2017). Cyber Crime Directorate. Cebu: *Author.* (online) **https://rm.coe.int/03-a-country-report-indonesia1/168072bd1f** (accessed Jul 20)

38. Sapiie, Marguerite Afra, (2017). Police Playing Tough in Combating Cybercrimes in Indonesia. Indonesia: *The Jakarta Post.* (online) **https://www.thejakartapost.com/news/2017/02/06/police-playing-tough-in-combating-cybercrimes-in-indonesia-.html** (accessed Jul 20)

Appendix F

Endnotes (continued)

39. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp41. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

40. Jakarta Metropolitan Police. Cyber Crime Investigation Satellite Office (CCISO). Jakarta. (online) **https://www.linkedin.com/company/cyber-crime-investigation-center-cciso-jakarta-metropolitan-police/** (accessed Jul 20 and Feb 21)

41. Perdain Yalasin (2013). Police Suspend Cooperation with OZ. Indonesia: *The Jakarta Post.* (online) **https://www.thejakartapost.com/news/2013/11/25/police-suspend-cooperation-with-oz.html** (accessed Feb 21)

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

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

44. Indonesia Academic CSIRT. **http://www.acad-csirt.or.id/aboutus.html** (accessed Jul 20 and Feb 21)

45. Information Security Incident Response Team (ID-SIRTII/CC) **https://idsirtii.or.id/en/page/history-id-sirtii-cc.html** (accessed July 20 and Feb 21)

46. The Ministry of Communication and Information Technology (Kementerian Komunikasi dan Informatika) (2021) **https://www.kominfo.go.id/** (accessed Jul 20 and Feb 21)

47. Information Security Incident Response Team (ID-SIRTII/CC) **https://idsirtii.or.id/en/page/history-id-sirtii-cc.html** (accessed July 20 and Feb 21)

48. Indonesia Computer Emergency Response Team (ID-CERT). **https://www.cert.or.id/beranda/en/** (accessed July 20)

49. 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)

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

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

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

53. 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)

54. Cyber Jawara, National Hacking Competition and Workshop (2020). Indonesia. **https://cyberjawara.id/** (accessed Feb 21)

55. Cyber Intelligence Asia Conference. **https://intelligence-sec.com/events/cyber-intelligence-asia-2021-3/** (accessed Jul 20 and Feb 21)

56. 9th World Conference on Cyber Security and Ethical Hacking (WCCSEH), (2021) **http://www.wccseh.igrnet.org/146/indonesia/** (accessed Jul 20 and Feb 21)

57. Indonesian Cyber Army, (2021) **https://www.cyberarmy.id/en/tentang** (accessed July 20)

Appendix F

Endnotes (continued)

58. Cyber Jawara, National Hacking Competition and Workshop (2020). Indonesia. **https://cyberjawara.id/** (accessed Feb 21)

59. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp41. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

60. Association of South East Asia Nations (ASEAN). **https://asean.org/** (accessed Feb 21)

61. Muslim, Abdul. (2017). Indonesia Wins ASEAN Cyberkids Camp 2017. Indonesia: *BERITSATU* (online) **https://www.beritasatu.com/archive/443333/indonesia-juara-i-asean-cyberkids-camp-2017** (accessed Feb21)

62. Financial Services Authority (Indonesia), Directory of Regulated Banks, 2015, **https://www.ojk.go.id/en/kanal/perbankan/data-dan-statistik/Direktori-Perbankan-Indonesia-Baru/Default.aspx** (accessed May 2020)

63. Indonesia Banker Institute, **http://ikatanbankir.or.id/en/home** (accessed May 2020)

64. Wikipedia, List of Banks in Indonesia, **https://en.wikipedia.org/wiki/List_of_banks_in_Indonesia** (accessed May 2020)

65. 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)

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

67. Indonesia Data Protection Overview, **https://www.dataguidance.com/notes/indonesia-data-protection-overview** (accessed 23 Dec 2020)

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Appendix F

Endnotes (continued)

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

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

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

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

86. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia - Land.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

87. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

88. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Resources and Power.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

89. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Resources and Power.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

90. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Agriculture, Forestry and Fishing.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

91. The World Bank, (2020). The World Bank in Indonesia – Economic Overview. Jakarta: Author. (online)
https://www.worldbank.org/en/country/indonesia
(accessed July 20)

92. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

93. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Introduction and Quick Facts.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

94. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia - Languages.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

95. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Introduction and Quick Facts.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

96. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia – Introduction and Quick Facts.
USA: *Encyclopaedia Britannica* (online)
https://www.britannica.com/place/Indonesia
(Accessed 15 February 2021)

Appendix F

Endnotes (continued)

97. OECD (2019). Education at a Glance 2019 – Indonesia. *Author* (online). **https://www.oecd.org/education/education-at-a-glance/EAG2019_CN_IDN.pdf** (accessed Jul 20)

98. The World Bank, (2020). The World Bank in Indonesia – Economic Overview. Jakarta: *Author.* (online) **https://www.worldbank.org/en/country/indonesia** (accessed July 20)

99. The World Bank, (2020). The World Bank in Indonesia – Economic Overview. Jakarta: *Author*. (online) **https://www.worldbank.org/en/country/indonesia** (accessed July 20)

100. The World Bank, (2020). The World Bank in Indonesia – Economic Overview. Jakarta: *Author.* (online) **https://www.worldbank.org/en/country/indonesia** (accessed July 20)

101. Adam, Asvi Warman. McDivitt, James F. Mohamad, Goenawan Susatyo, Leinbach, Thomas R. Wolters, Oliver W. and Legge, John David. (2021) Indonesia. USA: *Encyclopaedia Britannica* (online) **https://www.britannica.com/place/Indonesia** (Accessed 15 February 2021)

102. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp41. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

103. The Conversation. (2019). Cybersecurity for Indonesia: What Needs to be Done? UK: *Author.* (online) **https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009** (accessed Jul 20)

104. Sapiie, Marguerite Afra, (2017). Police Playing Tough in Combating Cybercrimes in Indonesia. Indonesia: *The Jakarta Post*. (online) **https://www.thejakartapost.com/news/2017/02/06/police-playing-tough-in-combating-cybercrimes-in-indonesia-.html** (accessed Jul 20)

105. The Conversation. (2019). Cybersecurity for Indonesia: What Needs to be Done? UK: Author. (online) **https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009** (accessed Jul 20)

106. The Conversation. (2019). Cybersecurity for Indonesia: What Needs to be Done? UK: *Author.* (online) **https://theconversation.com/cybersecurity-for-indonesia-what-needs-to-be-done-114009** (accessed Jul 20)

107. Yasmin, Nur (2019). Hacktivists, Bots, Elections: Indonesia Stepping Up Its Cybersecurity. Indonesia: *Jakarta Globe* (online). **https://jakartaglobe.id/context/hacktivists-bots-elections-indonesia-stepping-up-its-cybersecurity** (accessed Jul 20)

108. Yasmin, Nur (2019). Hacktivists, Bots, Elections: Indonesia Stepping Up Its Cybersecurity. Indonesia: *Jakarta Globe* (online). **https://jakartaglobe.id/context/hacktivists-bots-elections-indonesia-stepping-up-its-cybersecurity** (accessed Jul 20)

109. Watada, Jon (2018). The Cyber Security Agency's Challenge in Indonesia. Indonesia: *The Jakarta Post.* **https://www.thejakartapost.com/academia/2018/05/04/the-cyber-security-agencys-challenge-in-indonesia.html** (accessed Jul 20)

110. Watada, Jon (2018). The Cyber Security Agency's Challenge in Indonesia. Indonesia: *The Jakarta Post.* **https://www.thejakartapost.com/academia/2018/05/04/the-cyber-security-agencys-challenge-in-indonesia.html** (accessed Jul 20)

111. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp41. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

Appendix F

Endnotes (continued)

112. Global Cyber Security Capacity Centre (2021). Indonesia (GCSCC) 2015 – not yet published. Oxford: *Author,* **https://gcscc.web.ox.ac.uk/cmm-reviews** (accessed Mar 2020)

113. Nugraha, Y., Roberts, T., Brown, I., Sastrosubroto, A.S. (2016) The future of cybersecurity capacity in Indonesia: Top 20 Recommendations for Strengthening National Cybersecurity Capacity. Oxford: *Internet Institute, University of Oxford.* **https://rc.telkomuniversity.ac.id/wp-content/uploads/2017/08/The-Future-of-Cybersecurity-Capacity-in-Indonesia_Research-Report_2016.pdf** (accessed July 2020)

114. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp39. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

115. Australian Strategic Policy Institute (ASPI) (2016). The Cyber Maturity in the Asia-Pacific Region. Australia: *Author* (online) pp40. **https://s3-ap-southeast-2.amazonaws.com/ad-aspi/import/ASPI-Cyber-Maturity-2016.pdf?rL6DRSNr06xET_0OEycZuhHj_54SLbC1** (accessed Jul 20 and Feb 21)

116. National Cyber Security Index Estonia, *e-Governance Academy.* (online) **https://ncsi.ega.ee/ncsi-index/** (Accessed July 20)