Global
Cyber Security
Capacity Centre

Cybersecurity Capacity Review of the Republic of Uganda

2016

Contents

Cybersecurity Capacity Review of the Republic of Uganda

Introduction

Through Collaboration with *The Commonwealth Telecommunications Organisation (CTO),* The Global Cyber Security Capacity Centre has facilitated a self-assessment of cybersecurity capacity of the Republic of Uganda. The objective of this exercise is to enable the Republic of Uganda to determine areas of capacity which the country might strategically invest in in order to become more cyber secure. Stakeholders from the following groups participated in a three-day consultation for the review of cybersecurity capacity in Uganda:

1. Ministries: Ministry of Defence, Ministry of Foreign Affairs, Ministry of Justice, Ministry of Finance, Planning and Economic Development, Ministry of Public Service, Ministry of ICT, National Information Technology Authority, Uganda (NITA-U);
2. Academia;
3. Civil society;
4. Law enforcement;
5. Internet governance representatives;
6. Internet Society chapters;
7. Criminal Justice;
8. Intelligence Community;
9. National Security representatives;
10. CSIRT team;
11. Commercial sectors and SME's;
12. Finance Sector; and
13. Telecommunications Companies.

The consultations were based on the Centre's Cyber Security Capacity Maturity Model which is composed of five distinct areas of Cybersecurity Capacity; a) Cybersecurity policy and strategy; b) Cyber culture and society; c) Cybersecurity education, training and skills; d) Legal and regulatory frameworks; e) Standards, organisations, and technologies. There are multiple factors in each dimension, which describe cybersecurity capacity. The factors that comprise each one of the dimensions are presented on *Table 1* below:

Table 1: Description of Factors within Each Dimension

Dimension	Factors in Each Dimension
Dimension 1 Cybersecurity Policy and Strategy	D1-1: Documented or Official National Cybersecurity Strategy
	D1-2: Incident Response
	D1-3: Critical National Infrastructure (CNI) Protection
	D1-4: Crisis Management
	D1-5: Cyber Defence Consideration
	D1-6: Digital Redundancy
Dimension 2 Cyber Culture and Society	D2-1: Cybersecurity Mind-set
	D2-2: Cybersecurity Awareness
	D2-3: Confidence and Trust on the Internet
	D2-4: Privacy Online
Dimension 3 Cybersecurity Education, Training and Skills	D3-1: National Availability of Cyber Education and Training
	D3-2: National Development of Cyber Security Education
	D3-3: Training and Educational Initiatives within the Public and Private Sector
	D3-4: Corporate Governance, Knowledge and Standards
Dimension 4 Legal and Regulatory Frameworks	D4-1: Cybersecurity Legal Frameworks
	D4-2: Legal Investigation
	D4-3: Responsible Reporting
Dimension 5 Standards, organisations, and technologies	D5-1: Adherence to Standards
	D5-2: National Infrastructure Resilience
	D5-3: Cybersecurity Marketplace

Each factor includes indicators with five levels of capacity maturity, whereby the initial stage implies a rather ad-hoc level of capacity, the highest stage describes both a strategic approach and an ability to dynamically adapt or change following environmental considerations. These are the following:

- **Start-up:** At this level either no cybersecurity maturity exists, or it is very embryonic in nature. It could also include initial discussions about cyber capacity building, but no concrete actions have been taken. It also includes a lack of observed evidence in this particular indicator.

- **Formative:** Some features of the indicators have begun to grow and be formulated, but may be ad-hoc, disorganized, poorly defined - or simply "new". However, evidence of this activity can be clearly demonstrated.
- **Established:** The elements of the sub-factor are in place, and working. There is not, however, well-thought-out consideration of the relative allocation of resources. Little trade-off decision-making has been made concerning the ‘’relative’’ investment in the various elements of the sub-factor. But the indicator is functional and defined.
- **Strategic:** Choices have been made about which parts of the indicator are important, and which are less important for the particular organization or nation. Everything can’t be as important as everything else due to finite resources, therefore certain choices must be made. The strategic level reflects the fact that these choices have been made. They should have been made contingent on the nation or organization's particular circumstances.
- **Dynamic:** At the Dynamic level, there are clear mechanisms in place to alter strategy depending on the prevailing circumstances: for example, the technology of the threat environment, global conflict, a significant change in one area of concern (e.g. Cybercrime or privacy). Dynamic organizations have developed methods for changing strategies in stride, in a "sense-and-respond" way. Rapid decision-making, reallocation of resources, and constant attention to the changing environment are feature of this level.

Following the cybersecurity capacity review in the Republic of Uganda, results are being displayed in the present report.

Figure 1 below presents the maturity level for each dimension. The stages of maturity for each factor are represented by individual bars extending from the middle of the graph, and each dimension is a fifth of the graph.

As seen in the graph, for most factors of cybersecurity capacity in Uganda lies between an *initial and formative stage* of maturity. Evidently, some identified categories within these factors at an *established stage* of maturity.

Figure 1: CMM Review Results per Factor

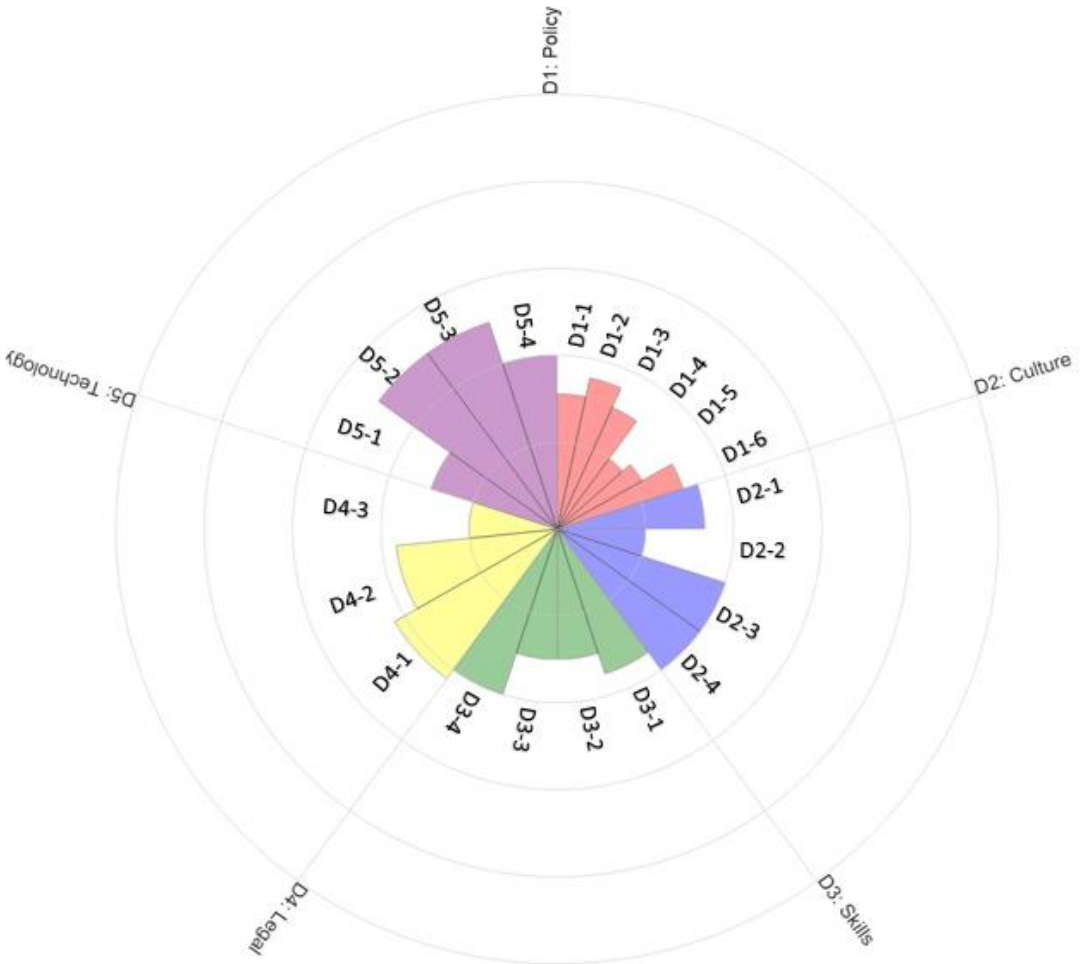


Figure 2: CMM Review Results per Dimension

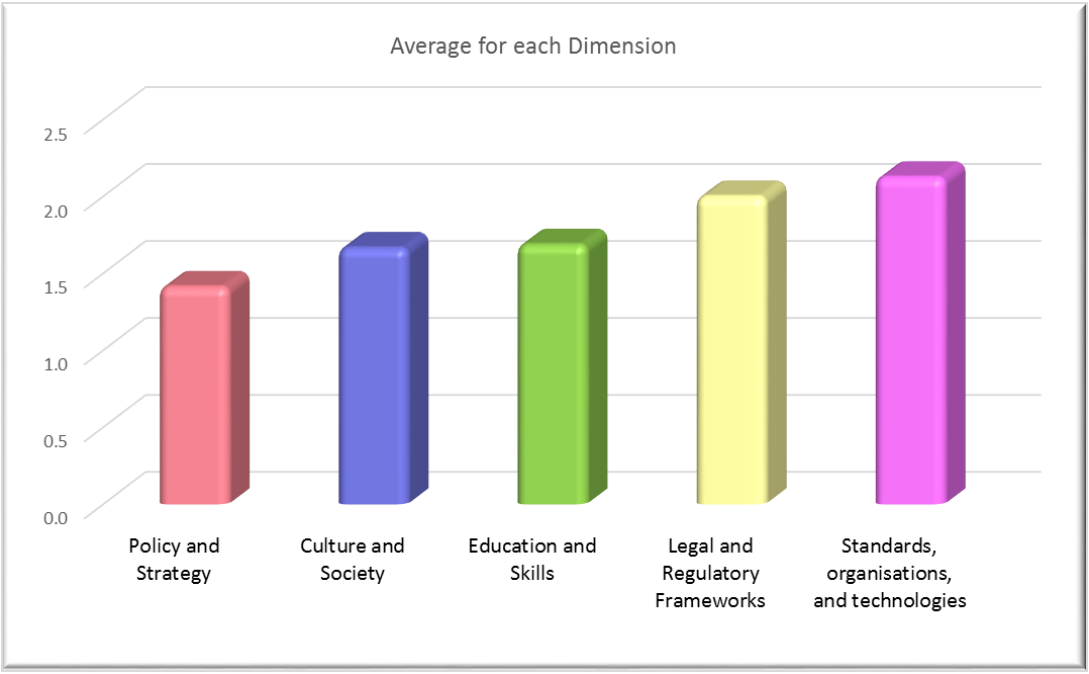
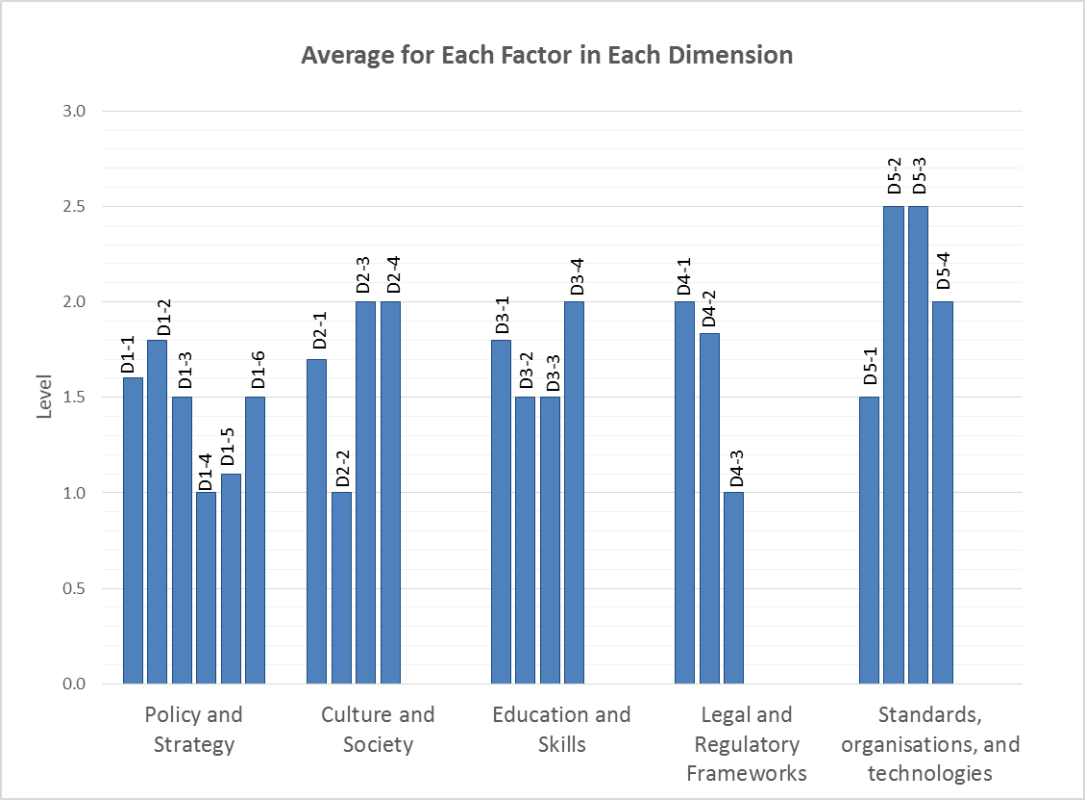


Figure 3: CMM Review Results for Each Factor in Each Dimension



Dimension 1: Cybersecurity Policy and Strategy

Not every government has a national level cybersecurity policy and strategy or responsible body, for cybersecurity as a policy area is still evolving. However, importance of designating an overarching government body for cybersecurity coordination and having a national cybersecurity strategy and policy cannot be overemphasized. International experience shows that those governments better cope and mitigate against cyber incidents and attacks that do have a designated government body and cybersecurity strategy and policy in place. This dimension explores the capacity of the government to design, produce, coordinate and implement a cybersecurity strategy as well as policies upholding the strategy.

Level: Start-up

It was established that there was no official document on Uganda national cybersecurity strategy. Instead, Uganda has a National Information Security Policy (NISP)[1] and a National Information Security Strategy (NISS)[2]. The National Information Technology Authority (NITA-U) brought together different stakeholders for consultation to develop both documents. Different Ministries have been using the National Information Security Policy as their guideline to inform their decision making.

NITA-U is the lead organisation responsible for cybersecurity. Therefore, it is responsible for the National CERT-UG and operates in close collaboration with other CERTs. The National Information Advisory Group is housed by NITA-U and provides complimentary advisory services to the Government of Uganda (GoU) on Information Security. It also gathers experience & advice from different stakeholders (e.g. Banks, Telecom) in order to fill in existing gaps.

Public-administration entities and ministries have internal security policies that inform the operation of their own internal independent networks. Specifically, within the Ministry of Defence and other agencies there is a cyber-strategy and policy. The Ministry of ICT is in the process of developing an IT policy. It was a common agreement among different stakeholders that every entity should be involved in the development of the national cybersecurity strategy in order to identify and fill existing gaps.

There is no centralised budget for cybersecurity. Every Ministry allocates its budget separately and depends on previous experience and future plans to allocate budget for cybersecurity. Law-enforcement cooperates with NITA-U (IT, ICT implementation) and Uganda Communications Commission (UCC)[3] the telecommunications regulator in Uganda. NITA-U and UCC are under the Ministry of ICT. During the consultation meeting, stakeholders agreed that there has to be a framework, a core IT Department, and a budget as minimal prerequisites for supporting cybersecurity activities. It was also noted that there

[1] http://cert.ug/sites/default/files/National%20Information%20Security%20Policy%20v1.0.pdf
[2] http://sites.miis.edu/cysec/files/2014/01/Uganda.pdf
[3] http://www.ucc.co.ug/

is a need for a more effective process for allocating Cybersecurity budget and prioritisation of investments. It was suggested that the need could be fulfilled by providing one organisation with the mandate to oversee/manage the allocation of Cybersecurity budget and investments. If a Ministry or entity is responsible for budget allocation, then conflicting actions of different entities as well as delays on decision making can be prevented. It was suggested by stakeholders that NITA-U could play that role.

The National Information Security Strategy (NISS) does not provide specific actionable directives that relate to cybersecurity. The document recognises that risks may exist but it is not aligned with national goals. At the moment every Agency has their own list of incidents and have different priorities. Different institutions place different levels of importance to technology, depending on their priorities.

It was noted that there is a need for Uganda to have a National Cybersecurity Strategy in order to identify and include other national risks and priorities areas of Cybersecurity. For example, the current rick register needs to be enhanced so that it can include all critical sectors in Uganda. It was suggested that NITA-U could coordinate the update, review and collation of all sectorial risk register in the country. There are general risks, which can be listed as internal and external at national level and their respective impacts needs to be considered.

Incident response is coordinated at a national level by NITA-U. The Uganda National Computer Emergency Response Team (CERT-UG) was established few years ago and is responsible for incident response at a national level. There is a telecommunication sector CERT, which is being developed by UCC, which is responsible for the telecommunications sector. Other sectors are likely to follow, such as the financial sector CERT and Ministry of Defence CERT. At the moment, IT departments within ministries and government agencies are responsible for dealing with any internal computer related incidents or breaches. It was noted that the financial sector has a special incident response teams, within banks that are adequately equipped to deal with CERT related incidents.

The channels of communication between ministries and government agencies remain ad-hoc and there are no lines of communication prepared for crisis situations. All ministries receive alerts and information on vulnerabilities from CERT-UG. Currently, only the IT department in each agency receives CERT related information. There is no policy framework or a set of guidelines on information sharing between the government agencies & CERT-UG. However, there is some form of coordination and communication between different government agencies and CERT-UG based at NITA-U. For example, the National Social Security Fund (NSSF) of Uganda has an Investigation Security Officer (ISO) who is responsible for sharing information with the relevant personnel at NSSF on incidents and vulnerabilities. The stakeholders agreed that there is no way to learn of an attack (or incidences) if there is no central channel of communication between different ministries, government departments/agencies and CERT-UG. Having an information sharing framework

will strengthen the CERT-UG team will be beneficial to Uganda, since it will provide a central team of skilled experts and introduce accepted processes & procedures for incident information sharing & dissemination.

Currently, there are no specific disclosure requirements for stakeholders to comply with. It is up to each entity or organisation to disclose vulnerabilities to CERT-UG. An Information Security Working Group was created to enable government communication officials to share information on incidents and other related challenges. This Group, however, does not include the private sector, but the National Security Information Advisory Group includes industry and other private sector representatives. It is expected that once the Information Security Working Group starts meeting regularly, then there will be adequate collaboration and sharing of information with CERT-UG

Uganda does not have an official list of Critical National Infrastructure (CNI) sectors in Uganda. This is mainly attributed to the lack of clear understanding of what constitutes a CNI sector list and the difficulty in recognising what needs to be protected. Experts believe they generally have the ability to recognise what is important for Uganda and will take the appropriate & necessary measures to protect Uganda's CNI. The National Information Security (NIS) Policy defines the concept of critical information infrastructure (CII), but does not clear address the CNI issue in detail. According to the National Information Security Policy ''*the information and communication technologies (ICTs), that form CII, increasingly operate and control critical national sectors such as health, water, transport, communications, government, energy, food, finance and emergency services*''. This is an areas that needs to be developed further.

Uganda does not have an official emergency response plan or business-continuity plan for its CNI. It is important that a continuity plan is established, as part of Uganda's CNI resilience capability strategy. Critical sectors such as finance and telecommunications services are important for Uganda, and cannot afford to have long downtime.

Having a risk register and risk-management framework is critical for Uganda, including the Internet Exchange Point Agency. Currently, information is provided to the IXP's board so that they can take decisions based on risk management assessments. According to the National Information Security Strategy ''*Organisations must adapt security controls to their circumstances in particular their business needs, risk appetite, value and sensitivity of their information*''.

The National Information Security Advisory Group (NISAG) is responsible for national exercises. It was noted that Cyber drills and exercises are planned, but only within the law-enforcement (i.e. Uganda Police) and not at a national level. There are a few penetration-testing exercises and security audits conducted by private companies. The Police and Ministry of Defence perform Cyber drills/exercises within their own organisations. Normally, after every penetration-testing exercise, there are reports on identified vulnerabilities are

selectively shared on a need-to-know basis. It was suggested that NITA-U is best placed to provide guidance at both national level and in each government agency.
Within the military and the defence apparatus, there is an advanced level of capacity now being built and there are dedicated IT officials. The military is yet to develop a fully functional Cybersecurity command Centre. Moreover, the Police have Digital Forensics' capacity. The Ministry of ICT is serving as the body, which coordinates different entities and departments regarding emergency response.

There is power backup capacity at the national level to ensure continuity of critical services when there is electric power failure. However, there is no national contingency plan or response framework in place to mitigate an emergency situation i.e. power failure on the critical infrastructure. Moreover, it was noted that digital-redundancy planning is not a priority at the moment. There is no central information repository data/information backup Centre but, there are data backup capability within each agency. For example, the Bank of Uganda has a private data backup capability.

Dimension 2: Cyber culture and society

Even the most forward-thinking cybersecurity strategy and policy are of little help if nongovernment actors do not understand their roles and responsibilities in safeguarding sensitive data and protecting their personal and organizational resources as they interact with them daily through digital means. This dimension assesses important elements of a cyber culture on an individual and organizational level and their perception by various stakeholders. As well, it determines the level of trust in e-government and e-commerce services and adherence to privacy standards by the entities that engage in provision of these services.

Level: Start-up

There is an absence or at best minimal recognition of a cybersecurity mind-set within most of the government agencies. However, there is a recognition of cyber risks and threats, and efforts towards cybercrime awareness campaigns have been initiated. Most government agencies do recognise the need for raising awareness on cybersecurity but that is not the norm yet. It was noted that the IT experts within government departments are aware of cybersecurity, but most employees are not aware.

Many businesses and industry have minimal recognition of the need for creating a cybersecurity mind-set in the work or business environment. The private sector is increasingly becoming more aware of the need for cybersecurity but usually it's only a handful of people in the organisation who might be focusing on or driving Cybersecurity issues. The majority of employees in business and industry understand the risks and threats. Financial institutions such as banks have prioritized creating a cybersecurity mind-set at work places. They are aware of Cybersecurity threats and risks, and are developing capacity

respectively. A number of SMEs are aware of Cybersecurity risks and threats, but lack of expertise to know the right mechanisms to address the risks identified.

Society-at-large has adopted a cybersecurity mind-set, but inconsistently. There are privacy settings online and people might know how to create a password, but that does not mean that they have a cybersecurity mind-set. It was noted that the market maturity usually determines security awareness.

A national awareness programme has not yet been developed. The need for awareness and outreach of cybersecurity threats and vulnerabilities across public and private sector is at an initial stage of discussion.

Trust in online services is identified as a concern. Infrastructure operators are aware of the implications and consider measures to promote trust in online services. However these are not yet established. Users do not trust online services because they do not understand the risks of online transactions. This is why, the Ugandan citizens tend to prefer face-to-face interactions. . The Electronic Transactions Act[4] includes all these implications but people are not aware of the threats online Moreover, budget allocation for security measures for online services is very limited. Although infrastructure operators consider measures to promote trust in online services, measures are not established.

E-government services are under development, with the exception of the eTax at Uganda Revenue Authority. The Directorate of E-Government Services is mandated to coordinate efforts to promote trust in e-government services. Provision of e-services is currently limited and although e-commerce is deployed, it also remains limited. International e-commerce service providers are more trusted by users than local providers.

The Law on Data Protection and Privacy is currently under development and is before Parliament. NITA-U and sub sector institutions (both public and private) have already provided input during the development of the Law. Laws and policies promoting access to personal data collected and stored across Government and other public institutions are under consideration but not yet agreed. This development process is premised on multistakeholder consultation.

Privacy in the workplace is recognised as an important component of Cybersecurity both in the public and private sectors. Sectors such as the Finance and Telecoms have privacy policies, but the public sector employees are not sensitised on such policies.

[4] http://www.nita.go.ug/sites/default/files/publications/Electronic-Transactions-Act.pdf

Dimension 3: Cybersecurity Education, Training and Skills

This dimension assesses the availability and quality of cybersecurity education, training, and skills in Uganda for various groups of government stakeholders, private sector, and population as a whole. In particular, it evaluates existing educational offerings and national development of cybersecurity education; training and educational initiatives within public and private sector; and corporate governance, knowledge, and standards.

Level: Start-up

There is gradual increase in information-security education and training in Uganda. A number of information Security training initiatives are starting to focus towards increasing the attractiveness of cybersecurity as a career and its relevance to both the private and public sector.

A significant number of institutions in Uganda are starting to offer information security related courses. Some of the undergraduate and postgraduate programmes are offering course modules in Information Security. There are also certified courses offered widely across Uganda mainly by private institutions. These private institutions mainly offer undergraduate courses in information security assurance and awareness programmes. And recently they've started offering courses on basic cybersecurity awareness for targeted groups including judges, legal practitioners and law enforcement officers. There is a noticeable increase in ISO certified experts and incident handlers in Uganda.

In general, training in information security is still ad-hoc and it is not part of the national education curriculum. In addition, it is also uncoordinated at the national level. At present a number of private firms such as banks and other multinational companies, based in Uganda, offer specialised training to their employees. These training programmes are usually sponsored by the organisation, through in-house training or through training institutions based abroad. There is a need for a structured training and certification programme/ framework for Cybersecurity related careers in Uganda. For example, there is a mismatch between many education curriculums of major Universities and the market demand for Cybersecurity expertise. In the interim, NITA-U is currently developing a register of skilled Cybersecurity experts in Uganda.

Education on ICT and security issues is not offered as part of the curriculum in all levels of education, and there is limited budgetary allocation for research and development in this field. The National Council of Education is in the process of amending the curriculum at all levels of education (primary, secondary & tertiary) to make it relevant in addressing the Cybersecurity expertise shortage in Uganda. It was also suggested by a number of stakeholders that Uganda needs to develop a framework that will enable Universities, National Council of Education, Private and Public Sector and other key stakeholders, to address the current mismatch of the curriculum not addressing the market needs.

Educational programmes to enhance skills and capability in cybersecurity need to be aligned with real world problems and funding for national research needs to be dedicated.

Moreover, a coordinating Mandate for these initiatives needs to be identified. Although private ICT companies are better organized and funded, majority still lack internal technical expertise in cybersecurity. A few multinational organisations have adopted standard good practices and policies on cybersecurity training and deployment. There is very minimal and in some cases non-existence culture of transferring and sharing knowledge among employees, especially after attending a course or training. Cybersecurity awareness and understanding at the executive level management still remains a challenge in a number of private and public organizations. In general, most executive boards rely on IT departments, with limited understanding of the overall organizational business risk and potential external threats.

Dimension 4: Legal and regulatory frameworks

International experience attests to the crucial role legal and regulatory frameworks play in mainstreaming cybersecurity across sectors while presenting prevention, mitigation, and dispute mechanisms to individuals and organizations affected by cyber threats. This dimension looks into the Government's capacity to design and enact national legislation and accompanying by-laws directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, cybercrime, and on the stakeholder groups represented by law enforcement, prosecution services, and courts.

Level: Formative

Uganda has a number of legislations in place, which address Internet misuse (the Computer Misuse Act[5], the Electronic Signatures Act[6], The Electronic Transactions Act[7], Electronic Misuse Act, the Access to Information Act[8] and the Regulation of Interception of Communications Act[9]). Different stakeholders were involved in drafting these legislations. As of writing this report, the Ministry of Information and Communications Technology (MoICT) in conjunction with Ministry of Justice and Constitutional Affairs (MoJCA), Uganda Communications Commission and National Information Technology Authority (NITA-U) of Uganda have jointly coordinated the drafting of the Data Protection and Privacy Bill, which is currently due for debate Parliament. It was suggested that in future the East African Community (EAC) countries should have a harmonized Data Protection and Privacy Law for all member states (Kenya, Uganda, Tanzania, Rwanda & Burundi).

There is limited capacity by the law enforcement agencies to investigate computer-related crimes, in-line with known global best practices. This has been attributed largely due to lack of sufficient technical expertise in digital forensic in Cybercrime cases. This has been

[5] http://www.nita.go.ug/sites/default/files/publications/Computer-Misuse-Act.pdf
[6] http://www.ulii.org/files/ug/legislation/act/2011/2011/electronic_signatures_act_2011_pdf_90247.pdf
[7] http://www.nita.go.ug/sites/default/files/publications/Electronic-Transactions-Act.pdf
[8] http://opm.go.ug/assets/media/resources/5/Access-to-Information-Act-2005.pdf
[9] http://www.ulii.org/files/Regulations%20of%20Interception%20of%20Communications%20Act,%202010.pdf

exacerbated by personnel churn from Government/public sector to the private sector, of Government sponsored trained officials. The Cyber Crime Unit and Electronic and Counter Measures Department[10], within the Ugandan Police Force, have the technical capacity and training to successfully investigate computer-related crimes.

There are existing laws which are being applied to prosecute digital crimes in Uganda today. Some of these prosecution cases have been based on the Computer Misuse Act, the Electronic Signature Act, and the Electronic Misuse Act, and applied as ''cyber Laws''. Cross-border prosecutions of Cybercrime are still a challenge for law enforcement agencies. Differences in laws between Uganda (where the victim might be residing) and other countries (where the crime might have originated) has been a major limitation. The Uganda Financial Intelligence Authority (FIA) has signed up with International Bodies (such as Interpol) to enforce anti-money laundering regulations.

Prosecutors and judges are being encouraged to take-up training or refresher courses on how to deal with computer related crimes, especially when it involved digital equipment & communications. Investigators are required also to be trained on handling digital evidence. There have been cases such as bank fraud, child pornography, possession of hacking tools, cyber-stalking, and harassment. The Computer Misuse Act for Uganda includes all these matters by law.

The need for a responsible-disclosure policy in public and private sector organisations is not fully enforced and in some cases there is no formal disclosure framework or policy to follow. If there is a need to disclose information, this has been done informally in a number of cases. There are internal and informal disclosure mechanisms for each public-administration entity and within the private sector. There is no regulation or framework to impose disclosure of information. Mainly it is voluntary and informal.

Dimension 5: Standards, organisations, and technologies

This dimension brings forward the importance of implementation of cybersecurity standards and minimal acceptable practices; existence of well-functioning and high capacity organisations coordinating cybersecurity with formal authority over multiple stakeholders; and existence of a vibrant cybersecurity marketplace of technologies and cyber insurance services.

Level: Formative

Information security standards are being adhered to by the Government of Uganda. There has been some initial signs of promotion and take-up across the public sector and Critical National Infrastructure (CNI) organisations. NITA-U has adopted the ISO 27001 standard, including the Ministry of Defence, Law Enforcement and National Intelligence agencies that

[10] http://pctechmag.com/2015/09/nita-launches-online-child-sexual-abuse-reporting-portal/

follow national and organisational standards. There is no total compliance to ISO standards or certification yet in a number of Government institutions. A number of these agencies or departments implement a few elements of the standards and known best practices. Currently, it is the decision of each public-administration entity to adhere to standards.

Usually the private sector follows ISO standards. Implementation of standards is essential and it promotes compliance but it is not widely the case for CNI. Telecoms inherit their standards just by being compliant to the National Standards, while the financial sector complies with and implement both national and organisational standards.

In procurement, cybersecurity standards, practices and procedures are usually being followed by the private sector. In the Financial sector there is a list of standards which have to be followed in order to produce products. It actually depends on the organisation and on the complexity of the procurement. There is limited adherence to software-development standards in public or private sectors.

There is no fully fledged Command and Control Centre at a national level, but this is being considered. CERT-UG is the organisation which performs this function at a national level. An incident-response team, CERT-UG, exists in the country, with identified roles and responsibilities. This capacity was established in 2014 through an Act of parliament. Apart from CERT-UG there is also a Communication Sector CERT run by the regulator-Uganda Communications Commission (UCC) and a Military CERT. However, coordination of all these CERTS remains a challenge. The Communications Sector CERT has identified and partially implemented key procedures for aspects such as Information sharing, handling incidents, and collaboration. There is collaboration with threat-intelligence agencies and CERT-UG. The private sector shares information with CERT-UG and the Communications Sector CERT. The CERTs share information and there is exchange of information at least every week.

Technology and processes are deployed in public and private sectors with no formal management. Online Government services, information and digital content are available online, but not fully deployed. There is some reliability of online services. The infrastructure is under development every day. If there is a black-out, there is back-up. Uganda is partially reliant on their neighbouring countries for infrastructure support.

Some companies provide local solutions within Uganda, and they develop applications, policies and software, while also carrying out regular penetration-testing services. There are local companies specialised in cybersecurity. Although, within the private sector and especially in the Banking sector, some insurance companies offer cybercrime insurance, a demand for a market in cybercrime insurance has not been identified.

Recommendations

Following the information presented on the review of the cybersecurity maturity of the Republic of Uganda, the Global Cyber Security Capacity Centre has produced a set of recommendations to be considered by the Government.

These recommendations refer to all five dimensions of cyber capacity and aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity in Uganda.

Dimension 1

Capacity Gap – develop a national cybersecurity strategy

Recommended Course of Action:

- Develop a National Cybersecurity Strategy.
- Assign an entity responsible for the development and implementation of the National Cybersecurity Strategy.
- Establish lines of communication between ministries and government agencies for crisis situations
- Establish a national programme for promoting standards' adoption in procurement or software development.
- Conduct crisis and risk management exercises-simulations at a national level at least once a year
- Develop an official list of Critical National Infrastructure (CNI) sectors.
- Strengthen formal coordination regarding Critical National Infrastructure (CNI) and information sharing between public and private sector and especially between different Banks. Develop a risk register and risk-management framework.

Dimension 2

Capacity Gap – develop a national cybersecurity awareness campaign

Recommended Course of Action:

- Develop an awareness programme to cover various target groups and link the programme to the national cybersecurity strategy development.
- Enact evaluation measurements to study effectiveness of the awareness programme.
- Promote trust in e-government and e-commerce services through regulation ensuring personal data privacy and adherence of e-government services to the highest cybersecurity protection standards.

Dimension 3

Capacity Gap – engrain information security training and education through all stages of education

Recommended Courses of Action:

- Engrain information security training and education through all stages of education.
- Allocate additional resources to cybersecurity education and training for public universities.
- Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy, so that skills are linked to market needs.
- Introduce a regular mandatory cybersecurity training for public sector staff.
- Develop a structured training and certification programme/framework for Cybersecurity related careers in Uganda.Create a national-level register of cyber-security experts.

Dimension 4

Capacity Gap – strengthen investigation capacity for computer-related crimes and develop a responsible disclosure policy

Recommended Courses of Action:

- Provide training and education of prosecutors and judges on computer related crimes.
- Allocate additional resources to cybersecurity education & training for prosecutors and judges.
- Promote cybersecurity knowledge transfer to public sector and cybersecurity cooperation at an international level.
- Develop a responsible disclosure policy within public sector and facilitate its adoption in the private sector through targeted outreach.

Dimension 5

Capacity Gap – promote the adoption of international standards within the public sector, and establish cooperation between academia and research & development (R&D) industry to strengthen the software-engineering competencies of domestic ICT companies

Recommended Courses of Action:

- Establish a programme to strengthen government's capacity to adapt or adopt international standards.
- Ensure reliability of online government services and promote their full deployment.

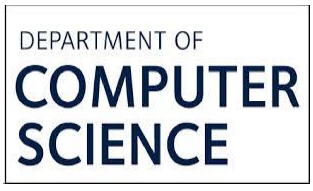
- Coordinate performance of the national CERT, allocating sufficient resources and accredited training to its employees.
- Establish a national Command and Control Centre[11].Invest in ICT research and cooperation between academia, research and industry to strengthen the software-engineering competencies of domestic ICT companies.

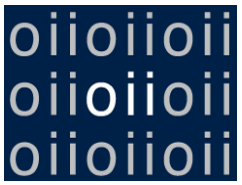
Conclusion

Overall, cybersecurity capacity in Uganda lies between an initial and formative stage of maturity. This expresses a state of maturity where some features have begun to grow and be formulated, but may be ad-hoc, while these can be clearly evidenced.

As a conclusion, the Republic of Uganda is in the process of developing different aspects of cybersecurity capacity. The country is in the process of developing the national cybersecurity strategy, whilst the Uganda National Computer Emergency Response Team is already established and active.

[11] The Command and Control Centre is established by the Government. A national Command and Control Centre, receives and correlates information from incident response capability organisations, public/private organisations, Layered Service Providers, Critical Information Infrastructure, defence and intelligence organisations, and provides advanced situational awareness.





Global Cyber Security Capacity Centre
Oxford Martin School, University of Oxford
Old Indian Institute, 34 Broad Street, Oxford OX1 3BD,
United Kingdom

Tel: +44 (0)1865 287430 • Fax: +44 (0) 1865 287435
Email: cybercapacity@oxfordmartin.ox.ac.uk
Web: www.oxfordmartin.ox.ac.uk
Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity/explore/home