CYBERSECURITY CAPACITY REVIEW

Republic of Sierra Leone

Global
Cyber Security
Capacity Centre

OXFORD
MARTIN
SCHOOL

UNIVERSITY OF
OXFORD

ITU

Contents

List of Abbreviations

CI	Critical Infrastructure
CID	Criminal Investigation Department
CIRT	Computer Incident Response Team
CISU	Central Intelligence and Security Unit
CMM	Cybersecurity Capacity Maturity Model
CSIRT	Computer Security Incident Response Team
FISU	Force Intelligence and Security Unit
GLACY	Global Action on Cybercrime
GCSCC	Global Cyber Security Capacity Centre
IGO	Intergovernmental Organisation
ICT	Information and Communication Technologies
ISOC.SL	Internet Society Sierra Leone Chapter
ISP	Internet Service Provider
ITU	International Telecommunications Union
MIC	Ministry of Information and Communications
MOD	Ministry of Defence
NATCOM	National Telecommunications Commission
NGO	Non-governmental Organisation
ONS	Office of National Security
SLIX	Sierra Leone Internet Exchange

Executive Summary

Through collaboration with the International Telecommunications Union (ITU), the Global Cyber Security Capacity Centre (GCSCC, or 'the Centre') has facilitated a review of the maturity of cybersecurity capacity of the Republic of Sierra Leone, hosted by the Ministry of Information and Communications. The objective of this review is to enable the Republic of Sierra Leone to gain an understanding of its cybersecurity capacity in order to strategically prioritise further investment in capacities.

Between 29th June and 1st July 2016, stakeholders from the following sectors participated in roundtable consultations: government departments and ministries, academia, civil society, legislators and policy owners, diplomatic missions, Information Technology leaders from government and the private sector, Internet Service Providers and the banking sector. The consultations were premised on the Centre's Cybersecurity Capacity Maturity Model (CMM), which defines five distinct areas of cybersecurity capacity:

- Cybersecurity Policy and Strategy
- Cyber Culture and Society
- Cybersecurity Education, Training and Skills
- Legal and Regulatory Frameworks
- Standards, Organisations, and Technologies

Cybersecurity Policy and Strategy

Through roundtable discussions, the *cybersecurity policy and strategy* dimension of cybersecurity capacity for the Republic of Sierra Leone was identified to range from *start-up* to *formative* stages of maturity. Currently, Sierra Leone does not have a national cybersecurity strategy document. However, a draft cybersecurity policy is in the process of adoption and a Cyber Task Force was established by the Ministry of Information and Communications (MIC), with representation from different sectors of government, such as representatives from the armed forces, law enforcement, the Office of National Security (ONS), and others.

No national computer security incident response team (CSIRT) or command and control centre structure exists, which poses a challenge to effective and coordinated incident response and management. No regulation that requires incidents to be reported is in place and Sierra Leone lacks a mandated authority or protocol to handle such a process.

The draft cybersecurity policy contains a central list of critical infrastructure (CI) assets. However, the government needs to ensure dissemination of this list to relevant stakeholders. Communication between the government and CI operators is ad-hoc and therefore coordination is limited. In cases where a coordinated response would be required, neither a cybersecurity operational strategy or plan, nor an official mandate is in place to manage and mitigate cybersecurity incidents. Similarly, risk management exercises or cyber drills are not conducted at a national level.

In the case of crisis management, national planning and evaluation of crisis management protocols and procedures is taking place, but as yet these plans and evaluations do not incorporate cybersecurity elements.

The Republic of Sierra Leone does not have a specific cyber Defence policy or strategy. While cybersecurity threats are starting to be recognised in the security architecture, there is no strategic coordination or command and control structure for cyber Defence and operational capacity has not yet been developed.

Basic redundancy for communication system fallouts has been established through the Dedicated National Security Information System (DNSIS), but system backups are currently lacking.

Cyber Culture and Society

During the consultations, the national capacity considered in the c*yber culture and society* dimension was identified to range between *start-up* and *formative* stages. The private sector was highlighted as the furthest advanced with regard to cybersecurity awareness and understanding, as leading organisations have started to incorporate cybersecurity considerations into their business processes. Similar observations were made with regard to government institutions that work on technology-related issues. General cybersecurity awareness of Internet users is, however, minimal.

Some e-government services in Sierra Leone have been developed, but uptake is low and there is currently no coordinated effort to secure and promote trust in these services. Similarly, available online banking services and e-commerce services are still very limited. Initiatives to promote trust in the use of online services are generally lacking and, consequently, the knowledge of users regarding safe online practices is limited. This has led to an environment where users often ‘blindly’ use the Internet, while more skilled users have developed a general distrust of the level of security of online services. This ‘blind’ trust or lack of trust is also reflected in the perception of the protection of personal information online. Doubts were raised regarding the handling of data that are shared online, while the average user lacks awareness and understanding of personal information protection online.

No central dedicated mechanism that enables citizens to report computer-related or online incidents and crimes has been established in Sierra Leone. While the police has taken on primary responsibility to receive and respond to reported incidents, coordination among relevant actors is lacking and reporting channels are not effectively communicated to the broader public. Moreover, fear of reputational harm prevents some private sector organisations from reporting incidents.

Finally, media and social media are not yet taking an active role in reporting cybersecurity threats and incidents and raising awareness. In particular, communication of messages about measures that users can take to protect themselves online is lacking.

Cybersecurity Education, Training and Skills

Through the consultations, it was observed that the *cybersecurity education, training and skills* capacity in Sierra Leone ranged from the *start-up* to *formative* stage. As ICT infrastructure and services are only starting to proliferate across the country, cybersecurity awareness raising has not yet gathered momentum. Some ad-hoc initiatives have been established, but these lack coordination.

At the university level, limited educational offerings are available in network security, but there are no specific cybersecurity modules or courses. Education on information and communications technology (ICT) and related security issues has not yet penetrated into the curriculum of all levels of education and cooperation between educational institutions is lacking.

Some certification courses are offered in Sierra Leone, particularly for ICT and several sectors are offering ad-hoc trainings on IT security. However, cybersecurity training needs in the public and private sector have not yet been documented and coordination between training providers, but also between academia and the private sector, is minimal. Transferring knowledge between employees and linking awareness-raising efforts with training programmes were noted as important steps towards enhancing capacity within this dimension efficiently.

Legal and Regulatory Frameworks

Legal and regulatory capacities were identified to range between *start-up* and *formative* stages of maturity. The cybersecurity legal and regulatory framework in Sierra Leone is dispersed and rudimentary, with no dedicated law or legislative framework on cybersecurity or cybercrime. A number of general laws are applied to cybersecurity and related issues in an ad-hoc manner. While these laws cover some aspects of cybersecurity, legislative gaps and inconsistent application of law have led to a lack of online protection for consumers, vulnerable groups and user data in general. Discussions have begun regarding the development of legislation on data protection and cybercrime, but some aspects, such as intellectual property online, are not yet a topic of concern.

Regarding operational capacities, law enforcement has some capacity to investigate computer-related crimes, in particular through the cybercrime unit within the Criminal Investigation Department (CID). Specialised and regular training, however, is not widely available for law enforcement officers, which limits investigative capabilities. Prosecutors and judges are not trained adequately and do not have the capacity to prosecute and preside over computer-related crimes.

Domestic and international cooperation to combat cybercrime is largely informal in nature, in particular through INTERPOL channels. Formal mechanisms that complement these informal relationships have not yet been established.

Standards, Organisations, and Technologies

The capacity of Sierra Leone in *standards, organisations and technologies* was identified to range from *start-up* to *formative* stages. No coordinated effort to adopt and implement cybersecurity standards can be evidenced. The adoption of standards varies from organisation to organisation, in accordance with individual needs and parent organisation regulations, but there is no coordination across sectors. Procurement and software development standards are partially deployed, but, overall, the strategic focus is primarily on function and price rather than security aspects.

Even though Sierra Leone is independently managing its network, services are not yet reliable and affordable. Institutions that are involved in the provision of Internet services lack effective coordination and cooperation.

When reviewing the deployed security measures across different sectors of the country, the level of capacity varies significantly and is generally inconsistently applied. Software quality is not monitored and there is no catalogue of secure software platforms and applications. Even though ISPs offer anti-malware software as part of their services, users lack awareness of available offerings and only have a limited understanding of the available technical security controls. Similarly, cryptographic techniques for protection of data at rest and data in transit are not yet deployed consistently within the government, private sector and the general public, even though leading organisations within the public and private sector are starting to recognise the importance of cryptographic controls.

The cybersecurity marketplace is underdeveloped and foreign technologies are being deployed instead of producing security products domestically. Furthermore, the need for developing a cybercrime insurance market was not yet identified at a national level. No responsible disclosure policy or framework has been established.

Additional Reflections

This was the twelfth country review that we have supported directly, and the first conducted in collaboration with the International Telecommunications Union (ITU). We hope that this review will offer useful insights to the Republic of Sierra Leone and that our recommendations on how to increase cybersecurity capacity will contribute to the development of a National Cybersecurity Strategy and a national CIRT.

1) Introduction

Through collaboration with the International Telecommunications Union (ITU), the Global Cyber Security Capacity Centre (GCSCC) has conducted a review of cybersecurity capacity maturity in the Republic of Sierra Leone, supported by the national host team from the Ministry of Information and Communications. The objective of this exercise is to enable the government to prioritise areas of capacity in which the country might strategically seek to invest in, in order to improve their national cybersecurity posture.

From 29 June to 1 July 2016, stakeholders from the following sectors participated in a four-day consultation to review the cybersecurity capacity of the Republic of Sierra Leone:

- Public Sector Entities:
    - Ministry of Information and Communications;
    - Ministry of Defence;
    - Ministry of Energy;
    - Ministry of Transport and Aviation;
    - National Telecommunications Commission (NATCOM);
    - Ministry of Justice;
    - Ministry of Tourism and Cultural Affairs;
    - Ministry of Lands, Country Planning and the Environment;
    - Ministry of Education, Science and Technology;
    - Minister of Agriculture, Forestry and Food Security;
    - Ministry of Fisheries and Marine Resources;
    - Ministry of Mines and Mineral Resources;
    - Ministry of Presidential & Public Affairs;
    - Public Service Commission;
    - Constitutional Review Committee.
- Legislators/Policy owners
- Criminal Justice and Law Enforcement
- Armed forces
- Academia
- Civil Society
- Private Sector
- Telecommunications companies
- Finance sector
- Diplomatic missions

Consultations were premised on the GCSCC's Cybersecurity Capacity Maturity Model (CMM) which is composed of five distinct dimensions of cybersecurity capacity:

1. Cybersecurity Policy and Strategy;
2. Cyber Culture and Society;
3. Cybersecurity Education, Training and Skills;
4. Legal and Regulatory Frameworks;
5. Standards, Organisations, and Technologies.

Each dimension consists of a set of factors, which describe and define what it means to possess cybersecurity capacity therein. Table I below shows the five dimensions with their comprising factors:

Table I: Description of Factors within Each Dimension

Dimension	Factors
Dimension 1 **Cybersecurity Policy and Strategy**	F 1.1: National Cybersecurity Strategy
	F 1.2: Incident Response
	F 1.3: Critical Infrastructure (CI) Protection
	F 1.4: Crisis Management
	F 1.5: Cyber Defence Consideration
	F 1.6: Communications Redundancy
Dimension 2 **Cyber Culture and Society**	F 2.1: Cybersecurity Mind-set
	F 2.2: Trust and Confidence on the Internet
	F 2.3: User Understanding of Personal Information Protection Online
	F 2.4: Reporting Mechanisms
	F 2.5: Media and Social Media
Dimension 3 **Cybersecurity Education, Training and Skills**	F 3.1: Awareness Raising
	F 3.2: Framework for Education
	F 3.3: Framework for Professional Training
Dimension 4 **Legal and Regulatory Frameworks**	F 4.1: Legal Frameworks
	F 4.2: Criminal Justice System
	F 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime
Dimension 5 **Standards, Organisations, and Technologies**	F 5.1: Adherence to Standards
	F 5.2: Internet Infrastructure Resilience
	F 5.3: Software Quality
	F 5.4: Technical Security Controls
	F 5.5: Cryptographic Controls
	F 5.6: Cybersecurity Marketplace
	F 5.7: Responsible Disclosure

In each factor there are indicators spanning five stages of maturity. The start-up stage implies an ad-hoc approach to capacity and ranges up to the dynamic stage where a strategic approach and the ability to dynamically adapt or change against environmental considerations is included. The five stages are as follows:

- **Start-up:** At this stage, there is either no cybersecurity maturity, or it is embryonic in nature. Initial discussions about cybersecurity capacity building might be in place, but no concrete actions have been taken. There is an absence of observable evidence at this stage.
- **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. However, 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 organisation or nation. The strategic stage reflects the fact that these choices have been made, conditional upon the nation or organisation's particular circumstances.
- **Dynamic:** Clear mechanisms are in place to alter strategy, depending on the prevailing circumstances such as the technology of the threat environment, global conflict or a significant change in one area of concern (e.g. cybercrime or privacy). Dynamic organisations 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 features of this stage.

This report presents the results following the cybersecurity capacity review of the Republic of Sierra Leone and includes recommendations on the next steps to be considered in order to increase the cybersecurity capacity maturity of the country.

2) Cybersecurity Context in Sierra Leone

The development of Internet infrastructure in Sierra Leone is still at initial stages and Internet penetration throughout the country is still comparatively low, partly due to fluctuating service quality and high service costs. Around 4.4% of the population had access to the Internet in 2015.[1] However, Internet usage is increasing rapidly as infrastructure becomes more reliable, in particular due to two important milestones. Firstly, the launch of a new Internet exchange point, the Sierra Leone Internet Exchange (SLIX) in 2010, enabled Internet Service Providers (ISPs) to exchange local data traffic directly through Sierra Leone rather than links in other countries, thereby decreasing international bandwidth costs and enhancing efficiency of local Internet traffic.[2] Secondly, in 2013, Sierra Leone launched the first fibre optic connection to the Africa Coast to Europe (ACE) submarine cable, which has substantially increased bandwidth capacity for national operators.[3]

Alongside improved Internet performance, Sierra Leone has also seen the emergence of various forms of cybercrime of varying scales. Common forms of cybercrime prevalent in Sierra Leone include: telecom related fraud, in particular SIM boxing, computer-related fraud, such as phishing, spam, as well as crimes involving messaging applications, gender-based violence, and online grooming.

As a result of these developments, Sierra Leone has started to prioritise securing the Internet, most prominently signified by the development of a national ICT and cybersecurity policy, which is currently in draft status. In this process, the Ministry of Information and Communications (MIC) has taken on a lead role in coordinating the development of policy and promoting the advancement of national cybersecurity capacity. Other important stakeholders include, but are not limited to, the National Telecommunications Commission (NATCOM), the Office of National Security (ONS), the Criminal Investigation Department (CID), the Ministry of Defence (MOD), the Central Intelligence and Security Unit (CISU), Force Intelligence and Security Unit (FISU) and the Internet Society Sierra Leone Chapter (ISOC.SL).

3) Review of Cybersecurity Capacity Maturity

In this section, we provide an overall presentation of the cybersecurity capacity in the Republic of Sierra Leone. The graphic (Graphic I) presents the maturity estimates in each dimension. The stages of maturity for each factor extend out from the middle as an individual bar, and each dimension is a fifth of the graphic.

As seen in this graphic, the collected evidence shows that for most factors the cybersecurity capacity in the Republic of Sierra Leone lies between a *start-up* and *formative* stage of maturity. Only some elements of the development of a national cybersecurity strategy in Dimension 1 (Cybersecurity Policy and Strategy) lie fully within the formative stage of maturity. However, according to the methodology followed during the application of the Cybersecurity Capacity Maturity Model (CMM), all the indicators for a certain stage need to be achieved for that stage of maturity to be assigned. Otherwise, maturity is recognised only at the highest completed stage. The assignment of maturity stages is based upon the evidence

[1] See http://www.internetworldstats.com/africa.htm.

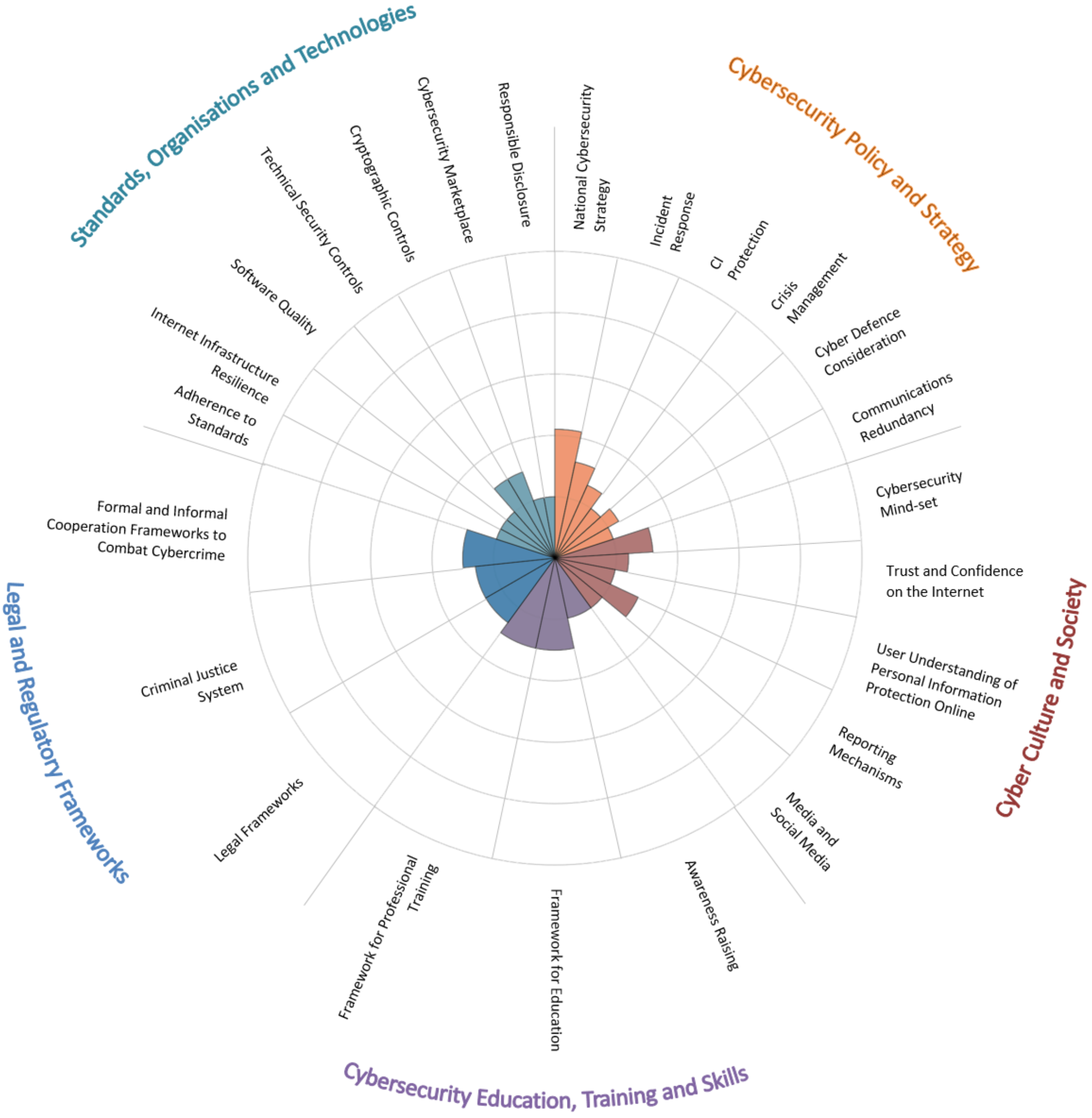
[2] See http://isoc-ny.org/tag/isoc-sl.

[3] See https://www.telegeography.com/products/commsupdate/articles/2013/08/09/sierra-leones-fibre-optic-infrastructure-project-still-on-track/.

collected, including the general or average view of accounts presented by stakeholders, desktop research conducted and our professional judgement.

Table II (see Appendix) presents a summary of the results on the stage of maturity for each factor, including a brief description of those results. Links to key policy and strategy documents, laws and other additional information are provided in the table. The table also presents a total of seventy-four recommendations regarding the enhancement of the existing capacity for each factor.

Graphic I: Review Results



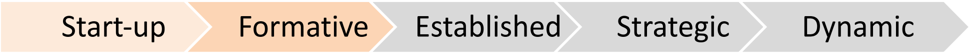
Dimension 1: Cybersecurity Policy and Strategy

This dimension explores the country’s capacity to develop and deliver cybersecurity strategy and enhance its cybersecurity resilience through improving its incident response, crisis management, redundancy, and critical infrastructure protection capacities. Delivering cybersecurity must include capability in early warning, deterrence, resistance and recovery. This dimension considers effective security policy in delivering national defence and resilience capability, while maintaining the benefits of a cyberspace vital for government, international business and society in general.

F 1.1: National Cybersecurity Strategy

Cybersecurity strategy is essential to mainstreaming a cybersecurity agenda across government because it helps prioritise cybersecurity as an important policy area, determines responsibilities and mandates of key cybersecurity government and non-governmental actors, and directs allocation of resources to the emerging and existing cybersecurity issues and priorities.

Stage: Formative



Currently, there is no official national cybersecurity strategy document in Sierra Leone which would serve as a coordinative document for the various existing initiatives. However, proactive efforts are underway to begin the process of developing such a document. The development of the national cybersecurity policy, which was discussed and reviewed through a multi-stakeholder process, represents the first step towards a comprehensive national strategy. The policy is linked to specific national risks and priorities and addresses three key focus areas, which relate to securing vital services, combating cybercrime and enhancing national defence capabilities. It also lays out a number of actions to advance cybersecurity in the country. While the policy sets an overall framework to address cybersecurity nationally and includes goals to be reached until 2020, participants agreed that the policy does not represent a strategic document. Once the policy has been adopted, the Ministry of Information and Communications (MIC) indicated that it would endeavour to develop a dedicated national cybersecurity strategy.

The MIC has taken the lead in developing and communicating the policy document, as well as in consolidating the newly formed Cyber Task Force. In addition, several key institutions were mentioned during the review, which should be considered for the development and implementation of a national cybersecurity strategy, including: the National Telecommunications Commission (NATCOM), the Office of National Security (ONS), the Criminal Investigation Department (CID), the Ministry of Defence (MOD), the Central Intelligence and Security Unit (CISU), Force Intelligence and Security Unit (FISU) and the Internet Society Sierra Leone Chapter (ISOC.SL). In light of the existing range of organisations that have taken initiative in the area of cybersecurity, the establishment of a central organisation with mandate to coordinate the country’s cybersecurity posture is a critical step towards enhancing the cybersecurity capacity of Sierra Leone.

An important finding of the review of this factor was the fact that some relevant stakeholders were not aware of the current status of the development of the cybersecurity policy, or the fact that a team has been created to work specifically on cybersecurity. Effectively communicating ongoing cybersecurity initiatives as well as keeping relevant stakeholders informed is crucial to maintain clear roles and responsibilities within the sector, avoid duplication of efforts and facilitate the involvement of all relevant stakeholders.

F 1.2: Incident Response

This factor addresses the capacity of the government to identify and determine characteristics of national level incidents in a systematic way. It also reviews the government's capacity to organise, coordinate, and operationalise incident response.

Stage: Start-up to Formative

Start-up Formative Established Strategic Dynamic

Currently, there is no national computer-related incident response organisation that would serve as the coordinating body for the reporting and management of cybersecurity incidents in the country. Such organisations mostly take the form of Computer Security Incident Response Teams (CSIRT) or Computer Incident Response Teams (CIRT). Due to the lack of a central organisation, there is no single entity holding a central registry of national level incidents.

Incidents that are reported by private sector institutions, such as banks, and individuals, are registered by law enforcement agencies, which also serve as responders to the incidents. A decision on whether or not an incident is considered to be a matter of national security is made on an ad-hoc basis by top-level management, which then refers national-scale cases to ONS. NATCOM additionally holds responsibility for fraud cases. Although a basic level of coordination has been established between these institutions, in particular through the recently formed Cyber Task Force, cooperation should be enhanced to effectively register and respond to cybersecurity incidents.

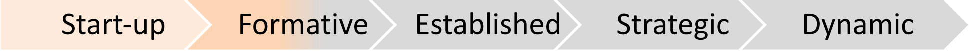
On an operational level, basic incident response processes have been established through the CID, NATCOM and ONS. However, institutionalisation, documentation and coordination of these processes is still lacking and staff are trained irregularly. Nevertheless, participants indicated that established procedures of secondment of staff from relevant organisations for the formation of a central organisation in the security sector could be utilised to create a central incident response organisation, such as a CIRT.

In the course of the cybersecurity capacity review, ITU has conducted a readiness assessment to establish a national CIRT in Sierra Leone, thereby commencing engagement to plan the formation of the national CIRT.

F 1.3: Critical Infrastructure (CI) Protection

This factor studies the government's capacity to identify CI assets and the risks associated with them, engage in response planning and critical assets protection, facilitate quality interaction with CI asset owners, and enable comprehensive general risk management practice including response planning.

Stage: Start-up to Formative


Start-up Formative Established Strategic Dynamic

In the draft cybersecurity policy of Sierra Leone, 13 critical infrastructure (CI) sectors, which operationally rely on functional and secure national critical information infrastructure, have been identified.[4] However, not all review participants were aware of this list, even though most felt that they would be able to identify sectors that represent critical infrastructure.

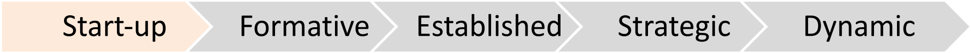
Coordination across CI owners and between CI owners and the government with relation to cybersecurity threat and vulnerability disclosure is largely ad-hoc and has not yet been institutionalised. Participants raised that one obstacle of establishing effective coordination mechanisms is the lack of cybersecurity awareness and knowledge of senior non-IT executives within CI, in contrast to IT staff that are more familiar and skilled in this area, but do not have the necessary authority to influence decision-making. To enhance coordination, participants noted that the existing security structure, which is managed by ONS, could serve as a scheme for integrating cybersecurity into the established relationships. Moreover, establishing a central mechanism for regular vulnerability disclosure with defined scope for reporting incidents (either mandatory or voluntary) between CI asset owners and the government is an important step towards enhancing capacity of this factor.

If cybersecurity is considered in risk management, it is done on an ad-hoc basis throughout the different parts of CI. This is mainly due to its recent emergence as a new topic, which has not yet been integrated into common business practices. Many participants were of the opinion that the implementation of a national cybersecurity strategy and an enhancement of the overall cybersecurity posture of the country would help to improve risk management, as managers will increasingly recognise the importance of cybersecurity risks.

F 1.4: Crisis Management

Crisis management planning addresses conducting specialised needs assessments, training exercises, and simulations that produce scalable results for policy development and strategic decision-making. Through qualitative and quantitative techniques, cybersecurity evaluation processes aim to produce structured and measurable results that would solicit recommendations for policymakers and other stakeholders and inform national strategy implementation as well as inform budgetary allocations.

Stage: Start-up


Start-up Formative Established Strategic Dynamic

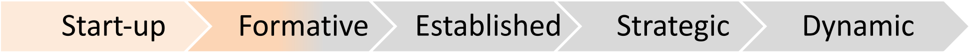
While ONS conducts crisis management exercises in the framework of various national security challenges and threats, such as to prepare for the national elections in 2012 or to address the growing terrorism threat, no cybersecurity elements have been integrated into these exercises. Some participants felt that the required infrastructure needs to be fully established before national cybersecurity exercises would be relevant. As cybersecurity becomes an increasing priority in the national threat analysis, it can be integrated as a component into the existing crisis management structures and tested through similar simulations, including the established evaluation mechanisms.

[4] Namely: Communications Sector; Government Facilities Sector; Manufacturing Sector; Defence Sector; Power and Energy Sector; Trade Facilities Sector; Financial Services Sector; Food and Agriculture Sector; Emergency Services Sector; Transportation Systems Sector; Public Health and Healthcare Sector; Water & Waste Water systems; Information Technology Sector.

F 1.5: Cyber Defence Consideration

This factor explores whether the government has the capacity to design and implement a cyber Defence strategy and lead its implementation, including through a designated cyber Defence organisation. It also reviews the level of coordination between various public and private sector actors in response to malicious attacks on strategic information systems and critical national infrastructure.

Stage: Start-up



Cyber Defence capacity maturity in Sierra Leone is mainly at the *start-up* stage, with some indications towards the *formative* stage of maturity. Currently, there is no Cyber Defence strategy and no overarching strategy or policy that would provide a framework for managing cyber Defence at the national level. The implementation of the general national security strategy is coordinated by ONS, with relevant ministries and emergency responders carrying ownership for their respective security sectors, but this strategy does not have any specific component addressing cyber Defence. However, participants from the armed forces indicated that cybersecurity threats have been recently incorporated as a consideration for national security, which can form the basis for the integration into the national security strategy.

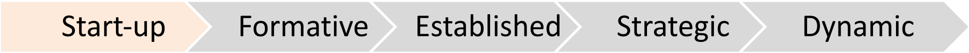
The discussion of cybersecurity within the context of national Defence has only recently begun, thus the operational capacity has not yet been developed. Participants highlighted that a robust overall security structure has been established, which was considered as one of the best in the sub-region after a review of the security setup a few years ago. The national security architecture consists of various actors, including civilian components, with specified roles and responsibilities and regular meetings. Collection and dissemination of intelligence is routinized across the security sector, whose highest body is the National Security Council. Moreover, private sector entities are approached directly where necessary. Even though the Central Intelligence and Security Unit (CISU) only sporadically addresses issues related to cyber Defence, participants were convinced that the existing institutional and communication structures would be more effective in proactively developing cyber Defence capacity once the national cybersecurity policy has been adopted and implemented.

Overall, cyber Defence is not yet a priority in the national cybersecurity posture. Once capacities are starting to be built in this area, the existing security architecture, including networks, communication channels and institutionalised coordination mechanisms, can be utilised to integrate cyber Defence efficiently and seamlessly into the national Defence sector.

F 1.6: Communications Redundancy

This factor reviews a government's capacity to identify and map digital redundancy and redundant communications among stakeholders. Digital redundancy foresees a cybersecurity system in which duplication and failure of any component is safeguarded by proper backup. Most of these backups will take the form of isolated (from mainline systems) but readily available digital networks, but some may be non-digital (e.g. backing up a digital communications network with a radio communications network).

Stage: Start-up



Communications redundancy as a broad concept has been considered in Sierra Leone, resulting in the establishment of an alternative form of communication for emergency responders in crisis situations, which is mainly done through using mobile phones rather than Internet communication forms. This dedicated mobile phone - based network is not only used as redundant communications, but also take over primary communication due to lacking resilience of networks. Moreover, the Dedicated National Security Information System (DNSIS) is held responsible for failures in the network across government. However, currently there is no alternative automated backup network. As a result, there is no national redundant network or data recovery or backup centre, nor has mapping of such redundancies taken place.

Recommendations

Following the information presented from the review of the maturity of *Cybersecurity Policy and Strategy*, the Global Cyber Security Capacity Centre has developed the following set of recommendations for consideration by the government of Sierra Leone. These recommendations provide advice and steps aimed to increase existing cybersecurity capacity as per the considerations of the Centre's Cybersecurity Capacity Maturity Model. The recommendations are provided specifically for each factor.

National Cybersecurity Strategy

For the Republic of Sierra Leone to make progress on cybersecurity, the key issue to address is the lack of a national cybersecurity strategy. The establishment of the Cyber Task Force has been an essential first step towards developing such a strategy, with multi-stakeholder collaboration as a crucial key component. This strategy should refer to the cybersecurity policy currently before parliament. The following recommendations have been outlined for consideration:

- **R1-1:** Embark toward developing a National Cybersecurity Strategy to set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. This strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives.
- **R1-2:** Allocate a specific mandate for the implementation of the National Cybersecurity Strategy.
- **R1-3:** Design and disseminate coordinated cybersecurity programmes.
- **R1-4:** Strengthen and promote inter-departmental cooperation in cybersecurity.

Incident Response

Without a national CSIRT/CIRT or other central computer-related incident response body, there will be no effective way to share information and resolve incidents at the national level. Communication channels between actors remain ad-hoc and inconsistent, impeding effective incident management. Therefore, the following recommendations have been outlined for consideration, in addition to those to be provided by the ITU:

- **R1-5:** Categorise and record national-level cyber incidents in a central registry, possibly hosted by the national CSIRT/CIRT.

- **R1-6:** Work towards the development of a national CSIRT/CIRT with clear processes and defined roles and responsibilities.
- **R1-7:** Draft legislation, which allocates mandates to the national CSIRT/CIRT.
- **R1-8:** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and the public sector, as well as within the cybersecurity community at national, regional and international levels.
- **R1-9:** Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting.

Critical Infrastructure (CI) Protection

While a central list of CI assets has been identified by the government in the draft cybersecurity policy, there is no defined cybersecurity operational strategy or plan in place to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CI. Incident response by CI is also uncoordinated, without a formal cyber response plan or official mandate. Risk management exercises and drills are not conducted at a national level. Therefore, the following recommendations have been outlined for consideration:

- **R1-10:** Once the cybersecurity policy has been adopted formally, disseminate the list of Critical Infrastructure (CI) assets with identified risk-based priorities.
- **R1-11:** Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector.
- **R1-12:** Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan.
- **R1-13:** Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CNI operators.

Crisis Management

No official planning and evaluation of cybersecurity crisis management protocols and procedures are in place. Therefore, the following recommendations have been outlined for consideration:

- **R1-14:** Conduct a needs assessment of measures that require testing with consideration of a simple exercise scenario.
- **R1-15:** Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively.
- **R1-16:** Evaluate the exercises and feed the findings back into the decision-making process.

Cyber Defence Consideration

There is no defence policy or strategy for cyber Defence considerations. Cyber Defence is discussed in various sectors of the security network, but operational capacity has not yet been developed. Existing security structures may serve as the foundation for cyber Defence considerations to be integrated into broader Defence and security approaches. Therefore, the following recommendations have been outlined for consideration:

- **R1-17:** Develop a cyber Defence component in the national security strategy, which takes into consideration identified threats to national security in cyberspace.
- **R1-18:** Develop a communication and coordination framework for cyber Defence, building on existing security structures.
- **R1-19:** Expand coordination in response to malicious cyber-attacks on military information systems and critical infrastructure.
- **R1-20:** Conduct consistent review of the evolving threat landscape in cybersecurity to ensure that cyber Defence policies continue to meet national security objectives.

Communications Redundancy

While basic communications redundancy has been implemented, no backup systems have been established. Therefore, the following recommendations have been outlined for consideration:

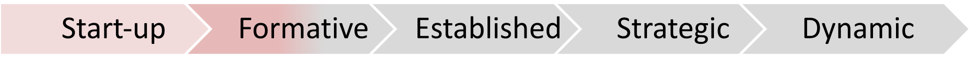
- **R1-21:** Allocate appropriate resources to not just hardware integration, technology stress testing, personnel training and crisis simulation drills, but also on ensuring redundancy efforts are appropriately communicated.
- **R1-22:** Hardwire all emergency response assets into a national emergency communication network.
- **R1-23:** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities.
- **R1-24:** Ensure the security of communication among stakeholders within the redundant communication network.

Even the most forward-thinking cybersecurity strategies and policies are of little help if a wide array of actors are not formally charged with implementing cybersecurity or actors do not understand their roles and responsibilities as users and stakeholders in safeguarding sensitive and personal data as they use digital media and resources. This dimension reviews important elements of a responsible cybersecurity culture such as the understanding of cyber-related risks in society, the level of trust in Internet services, e-government and e-commerce services, and users' understanding of personal information protection online. Moreover, this factor explores the existence of reporting mechanisms functioning as channels for users to report cybercrime. In addition, this factor reviews the role of media and social media in shaping cybersecurity values, attitudes and behaviour. This dimension underscores the centrality of users in achieving cybersecurity, but seeks to avoid conventional tendencies to blame users for problems with cybersecurity. Instead, cybersecurity experts need to build systems and programs for users – systems they can use easily and incorporate in their everyday practices online.

F 2.1: Cybersecurity Mind-set

This factor evaluates the degree to which cybersecurity is prioritised and embedded in the values, attitudes, and practices of government, the private sector, and users across society-at-large. A cybersecurity mind-set consists of values, attitudes and practices, including habits, of individual users, experts, and other actors in the cybersecurity ecosystem that increase the resilience of users to threats to their security online.

Stage: Start-up to Formative


Start-up | Formative | Established | Strategic | Dynamic

When reviewing the cybersecurity mind-set within Sierra Leone, the review looked at three groups of actors: government, private sector, and users. Overall, participants emphasised that cybersecurity is considered a new phenomenon in Sierra Leone, hence awareness and knowledge is still at initial levels.

Among government institutions, some lead agencies with mandates that relate to ICT have begun to place priority on cybersecurity, but the majority of government officials has no understanding of cybersecurity risks. Even though awareness is generally still low, participants noted that the importance of securing government network systems is increasingly acknowledged, which is demonstrated by a growing number of job vacancies and higher salaries for IT staff.

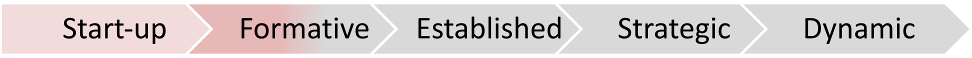
Similarly, some participants were of the opinion that some large organisations in the private sector are aware of cybersecurity and associated risks, while acknowledging that the level of understanding varies significantly across sectors. Other participants claimed that a large proportion of IT departments within firms do not have the knowledge or skills to address security issues, but only provide general IT support. In many cases, IT is also not considered to be a core part of the organisation. Higher levels of awareness can be observed in organisations with parent or partner companies abroad. When asked about the reasons for low cybersecurity awareness across the majority of the private sector, participants referred to the lack of policies and laws, the lack of a reporting mechanism to report cybercrime, missing communication networks for small companies and low recognition of the IT sector in general. Participants also felt that the low level of awareness was linked to the fact that Sierra Leone had not yet been victim of a large-scale cybersecurity incident.

Even though some lead organisations within government and private sector have begun to recognise the importance of cybersecurity, the vast majority of users has no or minimal levels of awareness of cybersecurity risks and secure online behaviour. With Internet availability and speed increasing, cybersecurity threats are proliferating. However, no cybersecurity mind-set has yet developed among users and some that assume knowledge have wrong perceptions of cybersecurity.

F 2.2: Trust and Confidence on the Internet

This factor reviews the level of user trust and confidence in the use of online services in general, and e-government and e-commerce services in particular.

Stage: Start-up to Formative


Start-up
Formative
Established
Strategic
Dynamic

Review participants saw a strong connection between the levels of cybersecurity awareness in the country and the trust and confidence of users on the Internet. Participants agreed that the majority of users are not worried when engaging with ICT, partly because of ‘blind’ trust into technologies that have been created overseas and partly because users do not feel that they could become victims of cybercrime.[5] On the other hand, participants themselves expressed a lack of trust in ISPs’ ability to secure the offered services. In their perception, most ISPs themselves are still struggling to establish cybersecurity and, currently, the user pays for the Internet provision only, rather than security or related services.[6] ISPs are thereby handing down the responsibility for maintaining cybersecurity to the end-user. Similar perceptions were prevalent among participants as regards the banking sector. Establishing and enforcing regulations that put clear responsibilities on banks and ISPs to secure their systems and services and provide comprehensive information to users was considered to be an essential step to improve capacity in this aspect. NATCOM could have a key role in this process.

Both e-government and e-commerce services are in the initial stage of development in Sierra Leone. Over the last years, the government has enhanced its efforts to utilise the full benefits of the Internet and has started to expand its online services, including through the online platform of the Open Government Initiative[7], an online application system for construction

[5] One participant cited a study that was conducted in Freetown, indicating that 72% of citizens did not know about the difference between a safe and an unsafe website.

[6] However, in a separate session, ISP representatives indicated that they do provide firewalls to their users. A lack of promotional efforts by ISPs might be the reason why end-users are not aware of the available services.

[7] See http://www.ogi.gov.sl/ and http://opendata.gov.sl/. However, the e-government components are not yet fully functional and uptake is limited.

permits of the Ministry of Works, Housing and Infrastructure[8], an online application system for registering of businesses and property by the Office of Administrator and Registrar General[9], and other governmental websites that provide useful information to citizens. However, the scope and uptake of these services is still limited and not all participants were aware of the available services. Moreover, some participants were concerned about the security of the new services.

Apart from limited online banking services, review participants were not aware of any e-commerce services offered within Sierra Leone. Many users would use services from foreign providers, but risk awareness and trust among users were considered to be low.

F 2.3: User Understanding of Personal Information Protection Online

This aspect looks at whether Internet users and stakeholders within the public and private sectors recognise and understand the importance of protection of personal information online, and whether they are sensitised to their privacy rights.

Stage: Start-up

The protection of personal information online was of great concern for review participants. Due to a lack of legal and regulatory measures to protect data and privacy of users, many participants were sceptical as to how data that they provide online are handled by service providers. Some participants called upon NATCOM to adopt and enforce regulation that would require ISPs to put in place adequate security measures for the protection of personal data. When asked about the average user, however, participants agreed that there is a lack of awareness and understanding of personal information protection online.

F 2.4: Reporting Mechanisms

This aspect explores the existence of reporting mechanisms functioning as channels for users to report internet related crime such as online fraud, cyber-bullying, child abuse online, identity theft, privacy and security breaches, and other incidents.

Stage: Start-up to Formative

No central dedicated mechanism that enables citizens to report computer-related or online incidents and crimes has been established in Sierra Leone. If an incident has occurred, citizens are able to contact the police through the 119 telephone line, or contact the local police directly. However, participants were unsure about the level of capacities and effectiveness of ONS and the police to respond to reports and incidents. Moreover, there is a general lack of coordination among actors and reporting channels are not effectively communicated to the

[8] See http://www.mwhi.gov.sl/online-application/.

[9] See http://www.oarg.gov.sl/Registration%20forms.html.

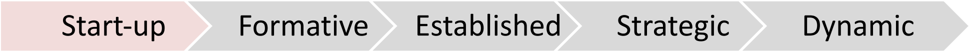
broader public. In some cases, citizens and stakeholders fear reputational harm as a result of reporting a crime of incident, which prevents them from reporting the incident.

While some participants indicated that the cybercrime unit within the CID would be best placed to establish a reporting mechanism, others considered ONS or NATCOM to be most suitable to take on such a role. Coordination among the different relevant stakeholders is key to create an effective mechanism and promote trust among citizens, so that incidents are reported.

F 2.5: Media and Social Media

This aspect explores whether cybersecurity is a common subject across mainstream media, and an issue for broad discussion on social media. Moreover, this aspects speaks about the role of media in conveying information about cybersecurity to the public, thus shaping their cybersecurity values, attitudes and online behaviour.

Stage: Start-up



Start-up Formative Established Strategic Dynamic

The role of media and social media in threat-reporting and raising awareness of cybersecurity is insignificant in Sierra Leone. Even though some specific issues are starting to be discussed, such as the right to access information in the context of the Open Data Festival held in April 2016[10] or data protection, cybersecurity is generally not a topic of media reports. Even when information about cybersecurity incidents is disseminated, the focus mainly lies on the threat rather than communicating messages about measures that users can take to protect themselves online.

Nevertheless, participants highlighted the need to explore how media and social media, in particular YouTube, WhatsApp or other messaging services, can be used for cybersecurity education. As cybersecurity is still a comparatively new topic in Sierra Leone, international best practice might help shape successful media campaigns to enhance cybersecurity awareness. Participants noted that the MIC could play a key role in encouraging media and social media to actively promote cybersecurity. During the review, various media representatives showed great interest in the discussions and a dedicated press conference was held to inform the broader public of the meetings and the importance of cybersecurity. This momentum could be utilised to enhance the role of media in disseminating positive messages about cybersecurity.

Recommendations

Based on the consultations, the following recommendations are provided for consideration by the government of Sierra Leone regarding the maturity of *cyber culture and society*. These aim to provide advice and next steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

[10] See, for example, http://news.sl/drwebsite/publish/article_200528259.shtml or ttp://www.sierraexpressmedia.com/?p=77603.

Cybersecurity Mind-set

Cybersecurity is not yet a priority across all levels of the government however, some government agencies whose mandates relate to ICT are seen to have a higher level of understanding of cybersecurity. Some large organisations in the private sector are aware of cybersecurity and associated risks, but the level of understanding varies significantly across sectors. Most companies are found not to recognise the importance of cybersecurity. Users generally lack a cybersecurity mind-set. To promote a cybersecurity mind-set across all sectors, it is recommended to:

- **R2-1:** Enhance efforts at all levels of government to promote understanding of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services.
- **R2-2:** Promote the sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set.
- **R2-3:** Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices.
- **R2-4:** Develop programmes and materials to train the public and improve cybersecurity practices.

Trust and Confidence on the Internet

Trust in online services is identified as a concern. Users do not have enough knowledge regarding safe online practises and the Internet is often used with “blind” trust or general distrust. E-government and e-commerce services are still underdeveloped and their use is limited. In order to enhance the level of capacity, we suggest the following actions:

- **R2-5:** Develop campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content.
- **R2-6:** Expand e-government services with recognition of the need for the application of security measures to promote trust in e-services.
- **R2-7:** Promote the need for security in e-commerce services.

User Understanding of Personal Information Protection Online

Stakeholders within the public and private sectors have minimal knowledge about how personal information is handled online, and they do not believe that adequate measures are in place to protect their personal information online. There is no or limited awareness and discussion regarding the protection of personal information online. In order to enhance the level of trust in secure online services we suggest the following actions:

- **R2-8:** Establish programmes to train users in managing their privacy online and protect themselves from unwanted access.
- **R2-9:** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.

Reporting Mechanisms

There is no centrally coordinated reporting mechanism for cybersecurity incidents in Sierra Leone. Police and ONS channels are available to citizens, but are not effectively communicated to the public. Therefore, the following actions are recommended:

- **R2-10:** Establish a central mechanism that allows citizens to report cybersecurity incidents and cybercrime.
- **R2-11:** Promote existing reporting channels to the wider public.

Media and Social Media

Media rarely cover information about cybersecurity or report on issues relating to cybercrime or other incidents. Social media are not currently used to communicate and disseminate messages on cybersecurity. In order to enhance the capacity of all forms of media to disseminate information on cybersecurity, we recommend to:

- **R2-12:** Encourage media and social media providers to disseminate information on specific cybersecurity issues and good cybersecurity practice.
- **R2-13:** Develop programmes to raise awareness among media and social media providers and actors on cybersecurity issues, including through a dedicated cybersecurity awareness month.

Dimension 3: Cybersecurity Education, Training and Skills

This dimension reviews the availability of cybersecurity awareness raising programmes for both the public and executives. Moreover, it evaluates the availability, quality, and uptake of educational and training offerings for various groups of government stakeholders, private sector, and the population as a whole.

F 3.1: Awareness Raising

This factor focuses on the prevalence and design of programmes to raise awareness of cybersecurity risks and threats as well as how to address them, both for the general public and for executive management.

Stage: Start-up

Start-up
Formative
Established
Strategic
Dynamic

Cybersecurity awareness raising efforts have not yet been implemented nationally. Many of the participants indicated that awareness of the effective use of ICT is still only gaining initial traction in Sierra Leone, and that security is seen as only relevant once ICT and Internet literacy is sufficient.

There are some ad-hoc initiatives in cybersecurity awareness-raising, such as Facebook posts on the US Embassy Facebook page, and ISOC.SL has offered basic security efforts as a component of their ICT literacy programs. These efforts, however, are not yet coordinated at the national level, and, therefore, a more centralised awareness campaign would greatly expand fundamental understanding of cybersecurity capacity. Additionally, integrating cybersecurity awareness efforts into ICT literacy courses could provide an established vehicle for cybersecurity awareness campaigns.

While there may be some uncoordinated awareness raising efforts for the public, there are no current efforts to raise the awareness of executive staff in any sector. This is an important gap, as executives are usually the final arbiters on investment into security.

F 3.2: Framework for Education

This factor addresses the importance of high quality cybersecurity education offerings and the existence of qualified educators. Moreover, this factor examines the need for enhancing cybersecurity education at the national and institutional level and the collaboration between government, and industry to ensure that the educational investments meet the needs of the cybersecurity environment across all sectors.

Stage: Start-up to Formative

Start-up
Formative
Established
Strategic
Dynamic

While network security is a module in some technical Master's degrees, like computer science at universities, such as the University of Sierra Leone and Njala University, no cybersecurity specific courses are offered in Sierra Leone. One obstacle to providing such courses is the lack of trained instructors to conduct these courses. Several participants also thought that instructors do not necessarily have enough training to use technologies, much less teach their secure use. There was also an impression that youth is increasingly more technology literate than the adult population, and therefore cybersecurity education should begin at an early age so that young people understand how to behave safely online.

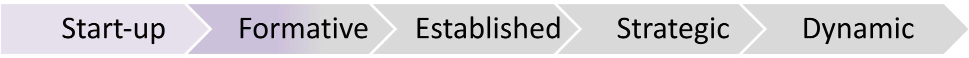
It was also made clear that there is a low level of coordination for cybersecurity education between the universities and public/private sectors. While the Ministry of Education is not responsible for developing curricula, they could help serve as a coordinating body for better harmonising offerings in the field. Additionally, creating a link between industry and academia would help ensure that the courses offered by universities meet the needs of industry.

It is important to note that there was a detailed discussion regarding whether it is first more important to improve the Internet infrastructure, reduce 'technophobia' of the overall population, or raise the level cybersecurity awareness in addition to providing coursework. These are all critical points and, while it is not easy to select only one of these activities as the most important, it is useful to note that, when developing an awareness campaign, the campaign developers should ensure that those already wary of technology do not increase their apprehension due to fear of threats posed to Internet users.

F 3.3: Framework for Professional Training

This factor addresses the availability and provision of cybersecurity training programmes building a cadre of cybersecurity professionals. Moreover, this factor reviews the uptake of cybersecurity training and horizontal and vertical cybersecurity knowledge transfer within organisations and how it translates into continuous skills development.

Stage: Start-up to Formative



Some certification courses are offered in Sierra Leone, particularly for IT (such as Microsoft certifications) and some CISCO security courses. Several other sectors are also offering ad-hoc trainings, such as those offered in the financial sector and by the national regulator NATCOM. However, the critical mass to understand broad public and private sector cybersecurity training needs has not yet been reached. Most participants agreed that professional training providers need to coordinate with academic partners so that university courses provide the foundation for such trainings.

Additionally, several participants mentioned that there needs to be more knowledge transfer within organisations from those who do receive trainings in order to maximise resources. Given that the demand for such courses exceeds the supply, enhancing knowledge transfer between employees is an effective and resource-efficient way of enhancing the skills base. Finally, it was deemed important to ensure that awareness-raising is also implemented alongside such professional training.

Recommendations

Following the information presented on the review of the maturity of cybersecurity *cybersecurity education, training and skills*, the following set of recommendations are provided to the government of Sierra Leone. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

Awareness Raising

Cybersecurity awareness raising efforts are limited to uncoordinated ad-hoc initiatives. There are no current efforts to raise the awareness of executive staff in any sector. In order to enhance the level of capacity regarding cybersecurity awareness-raising, we recommend the following actions:

- **R3-1:** Develop a national cybersecurity awareness raising programme with specified target groups, focusing on the most vulnerable users.
- **R3-2:** Link the development of the programme to the process of the national cybersecurity strategy development, as indicated in R1-1.
- **R3-3:** Engage multiple stakeholders in the development and delivery of the awareness raising programme.
- **R3-4:** Develop a dedicated awareness raising programme for executive managers within the public and private sectors.

Framework for Education

While network security is offered as a module at some universities, no cybersecurity specific courses are offered in Sierra Leone, nor are there trained instructors to conduct these courses. Coordination for cybersecurity education between universities and public/private sectors is limited. Regarding the development of cybersecurity education, we recommend the following actions:

- **R3-5:** Develop specialised university courses and degree programmes on cybersecurity.
- **R3-6:** Create cybersecurity education programmes for instructors to ensure that skilled staff is available to teach newly formed cybersecurity courses.
- **R3-7:** Allocate additional resources to cybersecurity education for public universities.
- **R3-8:** Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.

Framework for Professional Training

Some certification courses and ad-hoc trainings are offered in Sierra Leone, but the understanding of cybersecurity training needs is restricted. There is also a need for coordination between training providers and academic partners to ensure a harmonized approach towards education and training offerings. Knowledge transfer within organisations is uncommon. The following recommendations are proposed to enhance the capacity within professional training:

- **R3-9:** Identify training needs and develop training courses, seminars and online resources for targeted demographics, such as users and experts.

- **R3-10:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools.
- **R3-11:** Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia.
- **R3-12:** Invite more private companies and organisations to offer their certificates in Sierra Leone.

Dimension 4: Legal and Regulatory Frameworks

This dimension examines the government's capacity to design and enact national legislation directly and indirectly relating to cybersecurity, with a particular emphasis placed on the topics of ICT security, privacy and data protection issues, and other cybercrime-related issues. The capacity to enforce such laws is examined through law enforcement, prosecution, and court capacities. Moreover, this dimension observes issues such as formal and informal cooperation frameworks to combat cybercrime.

F 4.1: Legal Frameworks

This factor addresses legislation and regulation frameworks related to cybersecurity, including: ICT security legislative frameworks, privacy, freedom of speech, and other human rights online, data protection, child protection, consumer protection, intellectually property, substantive and procedural cybercrime legislation.

Stage: Start-up to Formative

Start-up | Formative | Established | Strategic | Dynamic

The legal framework regulating cybersecurity and related topics in Sierra Leone is generally undeveloped and dispersed. There is no dedicated law or legislative framework on cybersecurity or cybercrime. In lieu of a comprehensive framework, review participants indicated that a number of general laws are applied to cybersecurity and related issues in an ad-hoc manner, including the *Criminal Procedure Acts of 1965*, the *Telecommunications Act of 2006*, the *Child Rights Act of 2007*, the *Payment Systems Act of 2009*, the *Copyright Act of 2011* and the Sex*ual Offences Act of 2012*. However, participants also identified the need for a specialised cybercrime law, as the existing legal framework is only partially applicable to computer-facilitated crime. The draft ICT policy might facilitate this process once it is adopted, though it is not adequate as a replacement for legislation itself.

While Sierra Leone has not adopted a specific law on human rights online, it has acceded to or ratified the *International Covenant on Civil and Political Rights*, the *Convention Against Torture and Other Cruel, Inhuman and Degrading Treatment or Punishment*, the *Convention on the Elimination of All Forms of Discrimination against Women*, and the *African Charter on Human and Peoples' Rights*. Review participants noted that existing human rights legislation does not cover cybercrime or Internet-related human rights issues. In the absence of clear regulation or a specialised organisation responsible for ensuring the protection of human rights online, several entities have started to work towards ensuring that human rights are respected online, such as the Legal and Trusties Department of NATCOM, NGOs, IGOs, etc., but these initiatives remain dispersed and uncoordinated.

Similarly, there is currently no data protection regime in place, which has led to a general perception of participants that data are generally not protected. A particular example was brought up in the context of the recent Ebola crisis in Sierra Leone. A stakeholder noted that a number of national and international NGOs have collected and stored a huge amount of data during the Ebola outbreak, which are not regulated under any law. Participants raised concerns both regarding data being stored unsafely and privacy of Ebola survivors being violated. On the other hand, self-regulated data protection has become common practice in other sectors, such as the banking sector and telecommunications. In order to establish a comprehensive data protection regime, the development of a draft data protection law has commenced, which includes the right to access information.

With regards to the protection of children online, the *Sexual Offences Act of 2012* inter alia prohibits child pornography that is stored or distributed through computers or other electronic means. General child protection measures are also contained in the *Child Rights Act of 2007*. However, several participants noted that concrete efforts and measures to protect children, such as monitoring of online activities, are lacking and law enforcement intervention is largely reactive. Moreover, a lack of awareness of child protection issues and potential methods to report incidents is impeding effective child online protection.

Similar concerns were raised by participants regarding consumer protection online. While the *Payment Systems Act of 2009* regulates electronic and other payments and transactions, participants found the law to be insufficient and containing loopholes. In particular, international transactions through VISA and MasterCard are currently not secured domestically. Several participants also felt that banks are not operating in a transparent and secure manner. As e-payments and e-commerce are developing domestically and more and more users start to use the new services, gaps in the regulation need to be addressed as a priority to ensure that consumers are protected online.

While general laws are in place, intellectual property legislation is not applicable to the Internet and the development of such provisions are not being discussed.

Although there is currently no draft legislation containing substantive and procedural cybercrime provisions, representatives of Sierra Leone participated in the Council of Europe's workshop "Improving international cooperation on cybercrime and electronic evidence in West Africa", which was held in the framework of the GLACY project in May 2016.[11] Stakeholders indicated that, as a result of that workshop, discussions of a potential cybercrime law have begun.

Sierra Leone signed the *African Union Convention on Cyber Security and Personal Data Protection* on 29 January 2016,[12] but has not yet ratified the Convention. Moreover, during the stakeholder discussions, no participant mentioned the recent signing of the Convention and many participants were not aware of the existence of the Convention, which indicates a generally low awareness of legislative developments in the field of cybersecurity.

Overall, the legislative framework regulating cybersecurity and related topics is still in the start-up to formative stages of development. While draft legislation has been developed in

[11] See https://www.coe.int/en/web/cybercrime/-/glacy-improving-international-cooperation-on-cybercrime-and-electronic-evidence-in-west-africa.

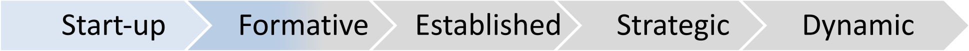
[12] See http://www.au.int/en/sites/default/files/treaties/29560-sl-african_union_convention_on_cyber_security_and_personal_data_protection.pdf.

some legal areas, such as data protection, other topics, such as human rights online, are still in the initial stages of discussion.

F 4.2: Criminal Justice System

This factor studies the capacity of law enforcement to investigate cybercrime, and the prosecution's capacity to present cybercrime and electronic evidence cases. Finally, this factor addresses the court capacity to preside over cybercrime cases and those involving electronic evidence.

Stage: Start-up to Formative



The capacity of law enforcement to investigate cybercrime is developing in Sierra Leone. A specialised cybercrime unit, the Sierra Leone Police Cyber Crime Prevention Unit, has been established within the Criminal Investigation Department (CID) and staff receive training from NATCOM when commencing their appointment in the unit. One participant noted that national police officers had participated in cybercrime trainings offered by the Council of Europe in Nigeria and Senegal. However, the capacities of the cybercrime unit are still in an infancy stage and regular training programmes that would prepare law enforcement officers for the changing threat landscape have not been established. In lieu of regulation on digital chain of custody, police officers largely rely on traditional measures and chain of custody principles rather than applying specialised methods.

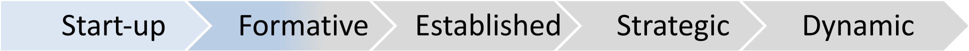
The capacities of prosecutors to handle cybercrime cases and cases involving digital evidence was considered to be even more limited. No participant was aware of any successfully prosecuted cybercrime case and no training for prosecutors is available nationally.

Similarly to prosecutors, the capacity of courts to handle cybercrime cases was perceived as low. Judges do not receive training to understand the expert opinions in cybercrime cases and even basic technical terms have to be explained to judges.

F 4.3: Formal and Informal Cooperation Frameworks to Combat Cybercrime

This factor addresses the existence and functioning of formal and informal mechanisms that enable cooperation between domestic actors and across borders to deter and combat cybercrime.

Stage: Start-up to Formative



When cooperating domestically or internationally to combat cybercrime, informal channels are more commonly used in Sierra Leone, as formal mechanisms have not yet been established. The primary channel to conduct cybercrime investigations is through the domestic Interpol office, which regularly engages with foreign counterparts. Similarly, NATCOM has established working relationships with its counterparts in other countries within the region. However, these relationships have not been institutionalised and are ad-hoc in nature. The establishment of a formal mechanism that ensures mutual legal assistance and extradition in cybercrime cases is essential to effectively prosecute.

Recommendations

Based on the review of the cybersecurity capacity maturity of *legal and regulatory frameworks,* the Centre has developed the following set of recommendations to be considered by the government of Sierra Leon for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

Legal Frameworks

There is no comprehensive legislative cybersecurity framework in Sierra Leone. General laws are applied to cybersecurity and related issues in an ad-hoc manner, including the *Criminal Procedure Acts of 1965*, the *Telecommunications Act of 2006*, the *Child Rights Act of 2007*, the *Payment Systems Act of 2009*, the *Copyright Act of 2011* and the *Sexual Offences Act of 2012*. However, these laws are only partially applicable to ICTs and contain gaps and loopholes. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R4-1:** Develop and adopt a comprehensive legislative framework addressing cybersecurity, cybercrime, human rights online, child online protection, data protection, consumer protection and intellectual property online by amending existing legislation or adopting new laws.
- **R4-2:** Fully ratify and implement regional cybercrime instruments, including through the allocation of sufficient resources according to national priorities.
- **R4-3:** Develop and adopt legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime.

Criminal Justice System

Law enforcement officers have some capacity to investigate cybercrime in accordance with domestic law, however this is minimal. Prosecutors and courts are not trained and do not have the capacity to prosecute and preside over cybercrime cases. In order to enhance the capacity of the criminal justice system, we recommend the following:

- **R4-4:** Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody.
- **R4-5:** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence.

Formal and Informal Cooperation Frameworks to Combat Cybercrime

Informal channels of cooperation are predominantly used to combat cybercrime domestically and across borders. Formal cooperation mechanisms have not been established. In order to fully move to the formative stage of maturity in this factor, we recommend the following:

- **R4-6:** Establish formal international cooperation mechanisms, including mutual legal assistance and extradition, to combat cybercrime.

- **R4-7:** Strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders.

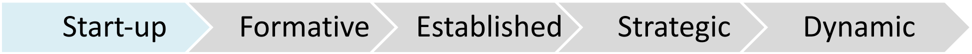
Dimension 5: Standards, Organisations, and Technologies

This dimension addresses effective and widespread use of cybersecurity technology to protect individuals, organisations and national infrastructure. The dimension specifically examines the implementation of cybersecurity standards and good practices, the deployment of processes and controls, and the development of technologies and products in order to reduce cybersecurity risks.

F 5.1: Adherence to Standards

This factor reviews government's capacity to design, adapt and implement cybersecurity standards and good practice, especially those related to procurement procedures and software development.

Stage: Start-up


Start-up Formative Established Strategic Dynamic

No coordinated effort to adopt and implement cybersecurity standards can be evidenced in Sierra Leone. While some organisations that have an international parent company are obliged to apply organisational standards, participants agreed that there is no overarching entity or system that coordinates and synchronises the implementation of standards. There is also no mechanism to establish synergies between government and private sector to harmonise approaches towards cybersecurity standards. Hence, each organisation follows their own procedures and policies in silos.

Within procurement standardisation, most participants stated that the strategic focus of procurement is primarily on function and price rather than security aspects. This is a significant gap in the adoption of security standards to enhance cybersecurity in procurement. While participants highlighted the key role of NATCOM in approving technical equipment that is used within organisations according to a set of internal rules and regulations, the enforcement of those rules is lacking in practice. The need for a collaborative effort to develop national standards, led by NATCOM, was raised and provides an important step in the enhancement of the maturity of this factor.

Similarly, the adoption of cybersecurity standards within software development is at early stages in Sierra Leone. Human resources applications are often produced in-house, without clear security standards across organisations. Similarly to procurement standards, software development cybersecurity standards need to be developed and proliferated to key institutions in order to enhance maturity in this capacity.

Overall, participants expressed a keen interest in adopting international cybersecurity standards and the ITU could provide assistance in this process.

F 5.2: Internet Infrastructure Resilience

This factor addresses the existence of reliable Internet services and infrastructure in the country as well as rigorous security processes across private and public sectors. Also, this aspect reviews the control that the government might have over its Internet infrastructure and the extent to which networks and systems are outsourced.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

The discussion of current Internet infrastructure resilience in Sierra Leone sparked an extensive discussion about the role of different actors and the pricing of services. Some participants were of the opinion that the fibre optic network was working efficiently, but that ISPs are limiting the provision of services, resulting in slow Internet connections. Other participants disagreed with that assessment and stated that the operational costs are not reasonable, which has led to a process of "handing down" the costs to the customers. Multiple participants called on NATCOM to regulate the prices and establish tax incentives. Overall, the discussion clearly indicated a lack of coordination and collaboration between the institutions that are involved in the provision of Internet services. Even though the nation has control over its network infrastructure thanks to the Sierra Leone Internet Exchange (SLIX), services are not yet reliable and affordable, which has led to low adoption rates. Energy supply remains a problem in Sierra Leone, as well as low Internet penetration (approximately 4.4%). As penetration expands, resilience will become an increasingly important issue. Moreover, enhanced coordination and discussion among network owners and operators is required to enhance maturity of this capacity.

F 5.3: Software Quality

This factor examines the quality of software deployment and the functional requirements in public and private sectors. In addition, this factor reviews the existence and improvement of policies on and processes for software updates and maintenance based on risk assessments and the criticality of services.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

The quality and performance of software was raised as a concern by participants. Even though some organisations have put in place internal procedures to update software applications, software quality is not monitored and there is no catalogue of secure software platforms and applications. Participants noted that there is no organisation that collects data on the kinds of software that are deployed in the country and, as a result, counterfeit software if pervasive. The MIC could take the lead in identifying this information and making it available to the wider public to promote the use of secure software solutions.

F 5.4: Technical Security Controls

This factor reviews evidence regarding the deployment of technical security controls by users, public and private sectors and whether the technical cybersecurity control set is based on established cybersecurity frameworks.

Stage: Start-up to Formative

Start-up
Formative
Established
Strategic
Dynamic

Participants expressed different opinions on the level of security with regards to technical security controls. Participants from ISPs indicated that robust firewalls have been put in place, anti-malware software is offered to customers and rudimentary Basic Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed. However, other private sector companies claimed that only large ministries would benefit from technical security controls and that they were not aware of any firewalls or malware protection offered by ISPs. Generally, the level of understanding and deployment of security controls by public and private sectors, and users, is low. Raising awareness of security controls and promoting their use among all sectors of the country is an important step in enhancing the capacity within this factor.

F 5.5: Cryptographic Controls

This factor reviews the deployment of cryptographic techniques in all sectors and users for protection of data at rest or in transit, and the extent to which these cryptographic controls meet international standards and guidelines and are kept up-to-date.

Stage: Start-up to Formative

Start-up
Formative
Established
Strategic
Dynamic

Similarly to the deployment of technical security controls, participants had diverging views on the capacity to implement cryptographic controls. Even though there is no national standard or regulation, ISPs have established internal policies across partner networks that require mandatory encryption for data in transit and data at rest. According to participants representing ISPs, point-to-point encryption (P2PE) is commonly applied to secure transactions. However, other participants pointed towards the lack of regulations on data at rest and in transit and the fact that they were not aware of how ISPs are handling their data or whether or not cryptographic techniques are deployed. In order to enhance maturity in this capacity, broader discussion and exchange of information across sectors and between ISPs and their customers need to be established, alongside the expanded deployment of cryptographic techniques, including the securing of web services through tools such as Secure Sockets Layer (SSL) and Transport Layer Security (TLS).

F 5.6: Cybersecurity Marketplace

This factor addresses the availability and development of competitive cybersecurity technologies and insurance products.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

A domestic market for cybersecurity technologies and cybercrime insurance products has not yet been developed. Due to the availability of international offerings, some participants did not recognise the need for domestically produced security products, as the national demand has not yet emerged. Both cybersecurity technologies and cybercrime insurance were considered as premature for the state of cybersecurity capacity in Sierra Leone, as the priority should be placed on raising awareness and developing specialised education and training offerings, before a domestic cybersecurity marketplace could be pursued.

F 5.7: Responsible Disclosure

This factor explores the establishment of a responsible disclosure framework for the receipt and dissemination of vulnerability information across sectors and if there is sufficient capacity to continuously review and update this framework.

Stage: Start-up

Start-up | Formative | Established | Strategic | Dynamic

No responsible disclosure policy or framework in public and private sector has been established. Fear of reputational damage is preventing banks and other companies from reporting vulnerabilities and cybersecurity incidents. In addition, review participants expressed different views on the role of ethical hackers in this context. Some were of the opinion that there are no 'white hat' hackers, because hackers would either have primarily malicious intentions when they detect and report vulnerabilities or the 'white hat' hackers of today become the 'black hat' hackers of tomorrow. Other participants stated that their organisations regularly accept and appreciate vulnerability reports from hackers, while maintaining their privacy. In light of this discrepancy in participants' views on vulnerability disclosure, raising awareness among all stakeholders on the value of responsible disclosure is an important component of establishing trust and a functioning mechanism to disclose vulnerabilities. Some participants suggested that ISOC.SL would be in a suitable position to establish and promote a responsible disclosure framework.

Recommendations

Based on the review of the maturity of *standards, organisations, and technologies*, the following recommendations are provided to be considered by the government of Sierra Leone. These recommendations aim to provide advice and steps to be followed for the enhancement of existing cybersecurity capacity as per the considerations of the GCSCC's Cybersecurity Capacity Maturity Model.

Adherence to Standards

No coordinated effort to adopt and implement cybersecurity standards can be evidenced in Sierra Leone. There is also no synergy between government and private sector to harmonise approaches towards cybersecurity standards. Standards are not promulgated widely and different departments within the government and organisations adhere to different standards according to their needs. Procurement and software development security standards are not yet widely adopted. Therefore, the following actions are recommended:

- **R5-1**: Establish a programme to strengthen government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity.
- **R5-2:** Promote adoption of international IT standards, in particular during procurement, software and code development.
- **R5-3:** Promote the awareness and implementation of standards among SME.

Internet Infrastructure Resilience

There is a lack of coordination and collaboration between the institutions that are involved in the provision of Internet services. Even though the nation has control over its network infrastructure, services are not yet reliable and affordable. The following recommendations are provided to increase the maturity of national Internet infrastructure resilience:

- **R5-4:** Increase reliability of Internet infrastructure and develop a national programme for infrastructure development.
- **R5-6:** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors.
- **R5-7:** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.

Software Quality

Software quality is not monitored and there is no catalogue of secure software platforms and applications. Policies and processes regarding updates of software applications have not yet been formulated. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R5-8:** Develop a catalogue for secure software platforms and applications within the public and private sectors.
- **R5-9:** Develop policies and processes on software updates and maintenance.
- **R5-10:** Gather and assess evidence of software quality deficiencies regarding its impact on usability and performance.

Technical Security Controls

There is minimal or no understanding or deployment of the technical security controls offered in the market, by users, public and private sectors. ISPs offer anti-malware software as part of their services, but awareness of available offerings is generally low. Basic Network

Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed but not in a consistent manner. In order to enhance the capacity of this factor, we recommend the following:

- **R5-11:** Promote user understanding of the importance of anti-malware software and network firewalls across devices.
- **R5-12:** Encourage ISPs to establish policies for technical security control deployment as part of their services.

Cryptographic Controls

Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit have been identified as a concern but are not yet deployed consistently within the government, private sector and the general public. Awareness of the importance of cryptographic controls is generally low. Therefore, in order to improve maturity to a higher stage, we recommend the following:

- **R5-13:** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest or in transit, according to international standards and guidelines.
- **R5-14:** Raise public awareness of secure communication services, such as encrypted/signed emails.

Cybersecurity Marketplace

Technologies are not produced domestically, but imported. Cybercrime insurance is neither available, whether domestically or from the region, nor is it a topic of public discussion. Therefore, we recommend:

- **R5-15:** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development.
- **R5-16:** Promote sharing of information and best practices among organisations, to explore potential cybercrime insurance coverages.

Responsible Disclosure

No responsible disclosure policy or framework in public and private sector has been established. In order to enhance the capacity of this factor, we recommend the following:

- **R5-17:** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report.
- **R5-18:** Encourage sharing of technical details of vulnerabilities among critical infrastructure.

Dimension	Capacity Factor	Stage of Maturity	Brief Description	References	Recommendations
Dimension 1 Cybersecurity Policy and Strategy	**F 1.1 National Cybersecurity Strategy**	**Start-up to Formative**	The drafting of a national cybersecurity strategy has not yet commenced. A draft cybersecurity policy is currently in the process of adoption, which will lay the foundation for the development of a national cybersecurity strategy. The Ministry of Information and Communications (MIC) has taken the lead in driving cybersecurity policy-making through a multi-stakeholder process, but responsibilities remain dispersed and often uncoordinated among different organisations.	Draft National Cybersecurity Policy	• **R1-1:** Embark toward developing a National Cybersecurity Strategy to set out the objectives, roles and responsibilities necessary for achieving a comprehensive and integrated national cybersecurity posture. This strategy should be aligned with national goals and risk priorities to be effective and provide actionable directives. • **R1-2:** Allocate a specific mandate for the implementation of the National Cybersecurity Strategy. • **R1-3:** Design and disseminate a coordinated cybersecurity programme. • **R1-4:** Strengthen and promote inter-departmental cooperation in cybersecurity.
	F 1.2 Incident Response	**Start-up to Formative**	There is no national CSIRT and no command and control centre. Communication channels between actors remain reactive, ad-hoc and inconsistent in incident response, impeding effective incident management.		• **R1-5:** Categorise and record national-level cyber incidents in a central registry, possibly hosted by the national CSIRT/CIRT. • **R1-6:** Work towards the development of a national CSIRT/CIRT with clear processes and defined roles and responsibilities. • **R1-7:** Draft legislation, which allocates mandates to the national CSIRT/CIRT. • **R1-8:** Develop coordination and information/cybersecurity threat sharing mechanisms between the private and the public sector, as well as within the cybersecurity community at national, regional and international levels. • **R1-9:** Appoint and publicize a national-level lead to ensure reporting of incidents and promote reporting.

	F 1.3 Critical Infrastructure (CI) Protection	**Start-up to Formative**	A central list of CI assets has been identified by government in the draft cybersecurity policy. Interaction between government ministries and owners of critical assets on cybersecurity is limited. A cybersecurity operational strategy or plan to manage and mitigate cybersecurity incidents in case of a coordinated cyber-attack on CI is not in place. Incident response by CI is uncoordinated, without a formal cyber response plan or official mandate. Risk management exercises and drills specific to cybersecurity are not conducted at a national level.	Draft National Cybersecurity Policy	• **R1-10:** Once the cybersecurity policy has been adopted formally, disseminate the list of Critical Infrastructure (CI) assets with identified risk-based priorities. • **R1-11:** Establish a mechanism for regular vulnerability disclosure and information sharing between the public and private sector. • **R1-12:** Establish information protection and risk management procedures and processes, supported by adequate technical security solutions, which inform the development of an incident response plan. • **R1-13:** Establish regular dialogue between tactical and executive strategic levels regarding cyber risk practices and encourage communication among CNI operators.
	F 1.4 Crisis Management	**Start-up**	While national crisis management exercises are held periodically with institutionalised evaluation mechanisms, cybersecurity elements have not yet been integrated into these exercises.		• **R1-14:** Conduct a needs assessment of measures that require testing with consideration of a simple exercise scenario. • **R1-15:** Conduct compromised communication scenarios and exercises to test emergency response assets interoperability and function effectively. • **R1-16:** Evaluate the exercises and feed the findings back into the decision-making process.
	F 1.5 Cyber Defence Consideration	**Start-up to Formative**	Sierra Leone does not have a specific national cyber Defence policy or strategy. A robust general security architecture has been established, which		• **R1-17:** Develop a cyber Defence component in the national security strategy, which takes into consideration identified threats to national security in

			can serve as a guiding structure for cyber Defence capacity development.		cyberspace • **R1-18:** Develop a communication and coordination framework for cyber Defence building on existing security structures. • **R1-19:** Expand coordination in response to malicious cyber-attacks on military information systems and critical infrastructure. • **R1-20:** Conduct consistent review of the evolving threat landscape in cybersecurity to ensure that cyber Defence policies continue to meet national security objectives.
	F 1.6 Communications Redundancy	**Start-up**	Basic communications redundancy has been established. However, no backup systems are in place.		• **R1-21:** Allocate appropriate resources to not just hardware integration, technology stress testing, personnel training and crisis simulation drills, but also on ensuring redundancy efforts are appropriately communicated. • **R1-22:** Hardwire all emergency response assets into a national emergency communication network. • **R1-23:** Establish communication channels across emergency response functions, geographic areas of responsibility, public and private responders, and command authorities. • **R1-24:** Ensure the security of communication among stakeholders within the redundant communication network.
Dimension 2 Cyber Culture	**F 2.1 Cybersecurity**	**Start-up to Formative**	A cybersecurity mind-set is adopted inconsistently and not engrained across		• **R2-1:** Enhance efforts at all levels of government to promote understanding

and Society	**Mind-set**		society. Cybersecurity is a concern, but mainly for government agencies with mandates relating to ICT. Within some large private sector organisations an increasing understanding of cybersecurity threats and risks is developing. However, most private sector entities do not recognise the need for cybersecurity yet. Users are generally unaware of cybersecurity threats.		of risks and threats, but also to design systems that enable users across society to more easily embed secure practices into their everyday use of the Internet and online services. • **R2-2:** Promote the sharing of information on incidents and best practices among organisations to promote a proactive cybersecurity mind-set. • **R2-3:** Promote prioritisation of risk and threat understanding for private sector entities by identifying high-risk practices. • **R2-4:** Develop programmes and materials to train the public and improve cybersecurity practices.
	F 2.2 Trust and Confidence on the Internet	**Start-up to Formative**	Trust in online services is identified as a concern. Users do not have enough knowledge regarding safe online practises and the Internet is often used with "blind" trust or distrust. E-government and e-commerce services are still underdeveloped and their use is limited.	http://www.statehouse.gov.sl/index.php/state-house-blog/1150-government-working-on-electronic-transactions-under-the-scope-of-e-governance http://www.thepatrioticvanguard.com/president-koroma-launches-e-governance-platform?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+ThePatrioticVanguard+%28The+Patriotic+Vanguard%29	• **R2-5:** Develop campaigns that promote the safe use of online services across the general public, enabling users to critically assess online content. • **R2-6:** Expand e-government services with recognition of the need for the application of security measures to promote trust in e-services. • **R2-7:** Promote the need for security in e-commerce services

				http://www.ogi.gov.sl/ http://opendata.gov.sl/	
	F 2.3 User Understanding of Personal Information Protection Online	**Start-up**	Stakeholders within the public and private sectors have minimal knowledge about how personal information is handled online, and they do not believe that adequate measures are in place to protect their personal information online. Awareness and discussion regarding the protection of personal information online are limited.		• **R2-8:** Establish programmes to train users in managing their privacy online and protect themselves from unwanted access. • **R2-9:** Encourage a public debate regarding the protection of personal information and about the balance between security and privacy to inform policy-making.
	F 2.4 Reporting Mechanisms	**Start-up to Formative**	There is no centrally coordinated reporting mechanism for cybersecurity incidents in Sierra Leone. Police and ONS channels are available to citizens, but are not effectively communicated to the public.		• **R2-10:** Establish a central mechanism that allows citizens to report cybersecurity incidents and cybercrime. • **R2-11:** Promote existing reporting channels to the wider public.
	F 2.5 Media and Social Media	**Start-up**	Media rarely cover information about cybersecurity or report on issues relating to cybercrime or other incidents. Social media are not currently used to communicate and disseminate messages on cybersecurity.		• **R2-12:** Encourage media and social media providers to disseminate information on specific cybersecurity issues and good cybersecurity practice. • **R2-13:** Develop programmes to raise awareness among media and social media providers and actors on cybersecurity issues, including through a dedicated cybersecurity awareness month.

Dimension 3 Cybersecurity Education, Training and Skills	**F 3.1 Awareness Raising**	**Start-up**	Cybersecurity awareness raising efforts are limited to uncoordinated ad-hoc initiatives. There are no current efforts to raise the awareness of executive staff in any sector.		• **R3-1:** Develop a national cybersecurity awareness raising programme with specified target groups, focusing on the most vulnerable users. • **R3-2:** Link the development of the programme to the process of the national cybersecurity strategy development, as indicated in R1-1. • **R3-3:** Engage multiple stakeholders in the development and delivery of the awareness raising programme. • **R3-4:** Develop a dedicated awareness raising programme for executive managers within the public and private sectors.
	F 3.2 Framework for Education	**Start-up to Formative**	While network security is offered as a module at some universities, no cybersecurity specific courses are offered in Sierra Leone, nor are there trained instructors to conduct these courses. Coordination for cybersecurity education between the universities and public/private sectors is limited.	Njala University http://njala.edu.sl/academics-programmes	• **R3-5:** Develop specialised university courses and degree programmes on cybersecurity. • **R3-6:** Create cybersecurity education programmes for instructors to ensure that skilled staff is available to teach newly formed cybersecurity courses. • **R3-7:** Allocate additional resources to cybersecurity education for public universities. • **R3-8:** Develop partnerships for the development of interfaces to research and innovation and interaction between universities and the local economy.
	F 3.3 Framework for Professional Training	**Start-up to Formative**	Some certification courses and ad-hoc trainings are offered in Sierra Leone, but the understanding of cybersecurity training needs is restricted. There is also a need for coordination between		• **R3-9:** Identify training needs and develop training courses, seminars and online resources for targeted demographics, such as users and experts.

			training providers and academic partners to ensure a harmonized approach towards education and training offerings. Knowledge transfer within organisations is uncommon.		- **R3-10:** Provide training for experts on various aspects of cybersecurity, such as technical training in data systems, tools, models, and operation of these tools. - **R3-11:** Create a knowledge exchange programme targeted at enhanced cooperation between training providers and academia. - **R3-12:** Invite more private companies and organisations to offer their Certificates in Sierra Leone.
Dimension 4 Legal and Regulatory Frameworks	**F 4.1 Legal Frameworks**	**Start-up to Formative**	There is no comprehensive legislative cybersecurity framework in Sierra Leone. General laws are applied to cybersecurity and related issues in an ad-hoc manner, including the Criminal Procedure Acts of 1965, the Telecommunications Act of 2006, the Child Rights Act of 2007, the Payment Systems Act of 2009, the Copyright Act of 2011 and the Sexual Offences Act of 2012. However, these laws are only partially applicable to ICTs and contain gaps and loopholes.	The Criminal Procedure Acts, 1965 The Telecommunications Act, 2006 The Telecommunications (Amendment) Act, 2007 The Telecommunications (Amendment) Act, 2009 The Child Rights Act, 2007 The Payment Systems Act, 2009 The Copyright Act, 2011 The Sexual Offences Act, 2012 All available at http://www.sierra-leone.org/laws.html or	- **R4-1:** Develop and adopt a comprehensive legislative framework addressing cybersecurity, cybercrime, human rights online, child online protection, data protection, consumer protection and intellectual property online by amending existing legislation or adopting new laws. - **R4-2:** Fully ratify and implement regional cybercrime instruments, including through the allocation of sufficient resources according to national priorities. - **R4-3:** Develop and adopt legal provisions on procedural powers for investigations of cybercrime and evidentiary requirements to deter, respond to and prosecute cybercrime.

				http://www.sierralii.org/ Ratification status of the AU Convention on Cyber Security and Personal Data Protection http://www.au.int/en/treaties	
	F 4.2 Criminal Justice System	**Start-up to Formative**	Law enforcement officers have some capacity to investigate cybercrime in accordance with domestic law, however this is minimal. Prosecutors and courts are not trained and do not have the capacity to prosecute and preside over cybercrime cases.		• **R4-4:** Strengthen national investigation capacity for computer-related crimes, including human, procedural and technological resources, full investigative measures and digital chain of custody. • **R4-5:** Develop and institutionalise specialised training programmes for police, prosecutors and judges on cybercrime and electronic evidence.
	F 4.3 Formal and Informal Cooperation Frameworks to Combat Cybercrime	**Start-up to Formative**	Informal channels of cooperation are predominantly used to combat cybercrime domestically and across borders. Formal cooperation mechanisms have not been established.		• **R4-6:** Establish formal international cooperation mechanisms, including mutual legal assistance and extradition, to combat cybercrime. • **R4-7:** Strengthen informal cooperation mechanisms within the police and criminal justice system, and between police and third parties, both domestically and across borders.
Dimension 5 Standards, Organisations and Technologies	**F 5.1 Adherence to Standards**	**Start-up**	No coordinated effort to adopt and implement cybersecurity standards can be evidenced in Sierra Leone. There is also no synergy between government and private sector to harmonise approaches towards cybersecurity standards. Standards are not		• **R5-1**: Establish a programme to strengthen government's capacity to adapt or adopt international standards in order to acquire a baseline in the context of organisational cybersecurity. • **R5-2:** Promote adoption of international IT standards, in particular during

			promulgated widely and different departments within the government and organisations adhere to different standards according to their needs. The implementation of standards in procurement and software development practices do not yet fully meet international IT guidelines, standards and acceptable practices.		procurement, software and code development. • **R5-3:** Promote the awareness and implementation of standards among SME
	F 5.2 Internet Infrastructure Resilience	**Start-up**	There is a lack of coordination and collaboration between the institutions that are involved in the provision of Internet services. Even though the nation has control over its network infrastructure, services are not yet reliable and affordable.		• **R5-4:** Increase reliability of Internet infrastructure and develop a national programme for infrastructure development. • **R5-6:** Enhance coordination and collaboration regarding resilience of Internet infrastructure across public and private sectors. • **R5-7:** Establish a system to formally manage national infrastructure, with documented processes, roles and responsibilities, and redundancy.
	F 5.3 Software Quality	**Start-up**	Software quality is not monitored and there is no catalogue of secure software platforms and applications. Policies and processes regarding updates of software applications have not yet been formulated.		• **R5-8:** Develop a catalogue for secure software platforms and applications within the public and private sectors. • **R5-9:** Develop policies and processes on software updates and maintenance. • **R5-10:** Gather and assess evidence of software quality deficiencies regarding its impact on usability and performance.
	F 5.4 Technical Security Controls	**Start-up to Formative**	There is minimal or no understanding or deployment of the technical security controls offered in the market, by users,		• **R5-11:** Promote user understanding of the importance of anti-malware software and network firewalls across

			public and private sectors. ISPs offer anti-malware software as part of their services but awareness of available offerings is generally low. Basic Network Introduction Detection Systems (NIDS) and Host Intrusion Detection Systems (HIDS) are deployed but not in a consistent manner.		devices. • **R5-12:** Encourage ISPs to establish policies for technical security control deployment as part of their services.
	F 5.5 Cryptographic Controls	**Start-up to Formative**	Cryptographic techniques (e.g. encryption and digital signatures) for protection of data at rest and data in transit have been identified as a concern but are not yet deployed consistently within the government, private sector and the general public. Awareness of the importance of cryptographic controls is generally low.		• **R5-13:** Encourage the development and dissemination of cryptographic controls across all sectors and users for protection of data at rest or in transit, according to international standards and guidelines. • **R5-14:** Raise public awareness of secure communication services, such as encrypted/signed emails.
	F 5.6 Cybersecurity Marketplace	**Start-up**	There is no domestic cybersecurity marketplace. Foreign technologies are being solely deployed and no security products are produced domestically. The need for developing a cybercrime insurance market was not yet identified at a national level.		• **R5-15:** Extend collaboration with the private sector and academia regarding research and development of cybersecurity technological development. • **R5-16:** Promote sharing of information and best practices among organisations, to explore potential cybercrime insurance coverages.
	F 5.7 Responsible Disclosure	**Start-up**	No responsible disclosure policy or framework in public and private sector has been established.		• **R5-17:** Develop a responsible vulnerability disclosure framework or policy within the public sector and facilitate its adoption in the private sector, including a disclosure deadline, scheduled resolution and an acknowledge report.

					• **R5-18:** Encourage sharing of technical details of vulnerabilities among critical infrastructure.

4) Appendix

Table II: Review Results

Lead Editors and Authors

Ms Eva Ignatuschtschenko
Mr Taylor Roberts

Authors (listed alphabetically)

Ms Lara Pace
Prof Basie von Solms

Global Cyber Security Capacity Centre

University of Oxford

Department of Computer Science

15 Parks Road | Oxford OX1 3QD | UK

Tel: +44 (0)1865 287430 | Fax: +44 (0) 1865 287435

Email: cybercapacity@oxfordmartin.ox.ac.uk

Web: www.oxfordmartin.ox.ac.uk/cybersecurity

Cybersecurity Capacity Portal: https://www.sbs.ox.ac.uk/cybersecurity-capacity