New Bill
Draft: Cybersecurity Bill, 2024
(Subject to change)
Author: Malawi Communications Regulatory Authority
Date: 11th March, 2024

CYBERSECURITY BILL, 2023

MEMORANDUM

This Bill seeks to make provision for the establishment of the Malawi Computer Emergency Response Team (Malawi CERT); for the appointment of cyber inspectors; for the development and enforcement of cybersecurity standards; for the designation and registration of critical information infrastructure; and for the reporting of cybersecurity incidents.

The Bill is divided into seven Parts.

Part I provides for preliminary matters, namely; short title and commencement, the interpretation of key words and terms used in the Bill, the objectives and principles of the Act, and the application of the Act.

Part II provides for the establishment of the Malawi CERT, as a unit under the Authority, and generally responsible for preventing, responding to, managing, and mitigating cybersecurity incidents. The Part also provides for the specific functions of the Malawi CERT, classification of incidents, and the establishment and functions of sectoral CERTs. The Part further provides for interagency coordination and international cooperation.

Part III provides for the appointment of cyber inspectors, and functions and powers of the cyber inspectors. The Part also provides for offences against cyber inspectors, including the offences of hindering and obstructing cyber inspectors.

Part IV makes provision for the development, establishment and adoption of standards, by the Authority, in the cybersecurity space for purposes of governance and risk management. The Part also provides for the issuance, by a cyber inspector, of a certificate of compliance where the cyber inspector is satisfied that the standards set by the Authority have been met.

Part V makes provision for the designation, by the Minister, of a computer system or computer network as a critical information infrastructure if the Minister considers that the computer system or computer network is essential for national security or the economic and social

wellbeing of citizens of Malawi. The Part also provides for the registration of critical information infrastructure, and the withdrawal of the designation of critical information infrastructure. The Part further provides for the duties of owners of critical information infrastructure, access to critical information infrastructure, and the localization of critical data.

Part VI provides for the duty to report a cybersecurity incident to the relevant sectoral CERT where a particular sector has experienced a cybersecurity incident. The Part also provides for the establishment, by the Malawi CERT, of a cybersecurity incident point of contact in order to facilitate the reporting of cybersecurity incidents by the general public, and for international co-operation in cybersecurity matters. The Part further provides for the establishment, by the Authority, of an early warning system in respect of human initiated risks that are likely to undermine the cybersecurity of the country.

Part VII contains miscellaneous provisions. Specifically, the Part gives the Minister the power to make regulations, on the advice of the Authority, for carrying out or giving effect to the provisions of the Act and for such matters as are envisaged by the provisions of the Act or as the Authority may deem necessary.

CYBERSECURITY BILL, 2023

ARRANGEMENT OF SECTIONS

SECTION

A BILL

entitled

An Act to make provision for the establishment of the Malawi Computer Emergency Response Team; for the appointment of cyber inspectors; for the development and enforcement of cybersecurity standards; for the designation and registration of critical information infrastructure; for the reporting of cybersecurity incidents; and for matters ancillary thereto or connected therewith.

ENACTED by the Parliament of Malawi as follows —

PART I — PRELIMINARY

Short title and commencement

1. This Act may be cited as the Cybersecurity Act, 2023, and shall come into force on such date as the Minister may appoint by notice published in the Gazette.

Interpretation

2. In this Act, unless the context otherwise requires —

Cap. 68:01

"Authority" has the meaning ascribed thereto in the Communications Act;

"classified information" means any information whose unauthorized disclosure would prejudice national security, and includes information on strategy, doctrine, capability, capacity and deployment;

"Computer Emergency Response Team (in this Act otherwise referred to as "CERT")" means a group of information security experts responsible for preventing, responding to, managing, and mitigating cybersecurity incidents;

“computer network” means interconnected computer systems, devices or nodes, that are linked together to transmit and share resources through various means such as wired or wireless connections;

“computer system” means a set of integrated devices that input, output, process, and store data and information including internet;

“critical data” means data which is declared by the Minister in accordance with this Act, to be of importance to the protection of national security of the country or the economic and social wellbeing of its citizens;

"critical information infrastructure" means any information system, networks or services, including databases containing critical data which if disrupted or destroyed would have a serious negative impact on the health, security or economic and social wellbeing of the citizens of Malawi and the efficient functioning of the Malawi Government;

“cyber incident” means any event in a system that compromises or has an adverse effect on the security of the system, the data processed therein, or services offered through the system;

“cybersecurity” means the ability of systems to resist, at a given level of confidence, any event that may compromise the availability, integrity or confidentiality of data, computer systems or of services offered via these systems;

“cyber threat” means any potential circumstance, event or action that could damage, disrupt or otherwise adversely impact computer systems, the users of such systems and other persons;

“data” means electronic presentation of information in any form;

"incident handling" means a systematic approach to effectively manage and respond to security incidents or disruptions in information technology systems or infrastructure;

"information system" means a system for generating, sending, receiving, storing, displaying or otherwise processing data and electronic messages, including internet;

"owner" in relation to critical information infrastructure includes a person who operates or exercises control of the critical information infrastructure;

"proactive services" means a systematic approach of identifying potential cybersecurity issues or needs before they become significant problems for individuals or organizations;

"reactive services" means a response to, and mitigation of, cybersecurity incidents that have already occurred;

"sectoral CERT" means a specialized group or organization that is responsible for handling and responding to cybersecurity incidents within a specific sector or industry; and

"vulnerability" means a weakness, susceptibility or flaw of an information and communication technology product or service that can be exploited by a cyber threat.

Objectives of this Act

3. – (1) The objectives of this Act are to set up a responsive information and communication technology legal framework that shall ensure the security of information and information communication and technology infrastructure.

(2) Without prejudice to the generality of subsection (1), the objectives of this Act shall include -

(a) the regulation of cybersecurity activities in Malawi;

(b) the prevention, management and response to cybersecurity threats and cybersecurity incidents;

(c) the protection of the confidentiality, integrity and availability of computer systems, programs and data;

(d) the regulation of owners of critical information infrastructure in respect of cybersecurity activities, cybersecurity service providers and practitioners in the country;

(e) the promotion of the development of cybersecurity in the country to ensure a secured and resilient digital ecosystem;

(f) the establishment of a platform for cross-sector engagement on matters of cybersecurity for effective co-ordination and co-operation between key public institutions and the private sector;

(g) the creation of awareness of cybersecurity matters; and

(h) the collaboration with international agencies to promote the cybersecurity of the country.

Principles of this Act

4. The following principles shall be adhered to in the implementation and application of this Act -

(a) respect for fundamental rights and freedoms, and in particular, the –

(i) right to respect for private life and communications;

(ii) protection of personal data;

(iii) freedom to conduct business;

(iv) right to property;

(v) right to an effective remedy before a court of law; and

(vi) right to be heard;

(b) risk management;

(c) assistance and cooperation; and

(d) minimizing harmful effect.

Application of this Act

5. This Act shall not apply to -

(a) personal data protection;

(b) cybercrime offences and criminal procedural powers;

(c) electronic identity;

(d) electronic commerce; and

(e) classified information and its processing.

PART II — CYBERSECURITY GOVERNANCE

Establishment of Malawi CERT

6. - (1) There is hereby established the Malawi CERT which shall be a unit under the Authority.

(2) The Malawi CERT shall take charge of its information infrastructure protection actions and serve as a base for national coordination to respond to information and communication technology security threats.

(3) The Authority shall ensure that the Malawi CERT is capable of providing reactive and proactive services, communicating timely information on recent relevant threats and, whenever necessary, assist in responding to cyber incidents.

Functions of Malawi CERT

7. – (1) The Malawi CERT shall carry out the following functions –

(a) advising Government Ministries, Departments and Agencies on all matters related to cybersecurity in Malawi;

(b) promoting the security of computers and computer systems in Malawi;

(c) monitoring cybersecurity threats within and outside Malawi;

(d) establishing codes of practice and standards for cybersecurity, and monitoring compliance with the codes of practice and standards by the public and private sector owners of critical information infrastructure;

(e) in consultation with the Malawi Bureau of Standards, establishing standards for certifying cybersecurity products or services;

(f) certifying cybersecurity products or services in accordance with the standards established pursuant to paragraph (e);

(g) accrediting sectoral CERTS and overseeing their operations;

(h) taking measures in response to cybersecurity incidents that occur within and outside Malawi which may threaten -

(i) the national security of Malawi;

(ii) the economy of Malawi;

(iii) international relations between Malawi and other countries;

(iv) health of the public;

(v) the safety of life and property;

(vi) vital installations and classified information; and

(vii) any other sector of the country likely to be affected by a cybersecurity incident;

(i) identifying and designating critical information infrastructure and advising the Minister on the regulation of owners of critical information infrastructure to protect the critical information infrastructure of the country, in accordance with international best practices;

(j) providing technical support for law enforcement agencies and security agencies to investigate and prosecute cyber offenders;

(k) promoting the protection of children online;

(l) maintaining a register of providers of cybersecurity services;

(m) establishing standards for the provision of cybersecurity services;

(n) supporting technological advances and research and development in cybersecurity to ensure a resilient and sustainable digital ecosystem;

(o) deploying strategies to implement research findings towards the promotion of the cybersecurity in Malawi;

(p) establishing and maintaining a framework for disseminating information on cybersecurity;

(q) submitting periodic reports to the Minister on the state of cybersecurity in Malawi;

(r) building the capacity of persons in the public or private sector in matters related to cybersecurity;

(s) collaborating with law enforcement agencies to intercept or disable a digital technology service or product whose operation undermines the cybersecurity in Malawi;

(t) establishing and maintaining a national register of -

(i) identified and potential risks;

(ii) the levels and impact of risks;

(iii) owners of critical information infrastructure; and

(iv) any other persons licensed or accredited to carry out cybersecurity activities;

(u) periodically reviewing cybersecurity risk assessments and continuity plans;

(v) contributing to cybersecurity policy development and overseeing policy implementation;

(w) overseeing and monitoring the implementation of cybersecurity measures, regulations, and standards to ensure effective protection of critical information infrastructure and information system;

(x) coordinating with relevant national and international actors as the primary point of contact for cross-sectoral and cross-border cooperation in addressing cybersecurity threats and incidents; and

(y) performing any other functions which are ancillary to the objectives of the Malawi CERT.

(2) The Authority shall initiate the periodic review and update of the national cybersecurity policies, strategies, and measures, to ensure their continued effectiveness and adaptability to emerging threats and challenges.

(3) The Authority shall ensure that the Malawi CERT is provided with adequate funds, resources, and well-trained staff to effectively deliver proactive and reactive services at all times.

(4) To ensure availability, the Malawi CERT shall maintain multiple communication channels and make them known to its partners.

(5) The Malawi CERT shall utilize an appropriate system for managing and routing requests.

(6) The Authority shall charge fees for services provided by the Malawi CERT as determined by the Authority.

Classification of incidents

8. The Malawi CERT may prescribe standardized practices and classification schemes, related to incident handling, crisis management, and coordinated vulnerability disclosure.

Sectoral CERTS

9. - (1) For purposes of achieving effective cybersecurity incident coordination, the Malawi CERT shall facilitate the establishment of a sectoral CERT.

(2) When facilitating the establishment of a sectoral CERT, the Malawi CERT shall -

(a) consider -

(i) the needs and criticality of a sector; and

(ii) developments in respect of cybersecurity in Malawi;

(b) prescribe –

(i) the reporting obligation of the sectoral CERT;

(ii) the penalty for non-compliance to the reporting obligation; and

(iii) the need to adhere to risk management protocols.

(3) A sector shall be responsible for the cost of establishing its sectoral CERT and for the operational costs of the sectoral CERT.

Functions of a sectoral CERT

10. - (1) A sectoral CERT shall -

(a) collect and collate cybersecurity incidents within its sector and, within five days, report the incidents to the Malawi CERT;

(b) co-ordinate responses to cybersecurity incidents within its sector;

(c) in coordination with the Malawi CERT, promote cybersecurity within its sector;

(d) act as the focal point of contact within its sector;

(e) provide the first response to sector specific cyber security incidents; and

(f) carry out other responsibilities as provided under this Act.

(2) A sectoral CERT shall, through its administrative head, submit a monthly report to the Malawi CERT covering the operations of the sectoral CERT, in a manner and form prescribed by the Malawi CERT.

(3) A sectoral CERT that fails to comply with directives of the Malawi CERT commits an offence and shall be liable to an administrative penalty prescribed by the Authority.

Interagency coordination

11. - (1) The Malawi CERT shall cooperate with public authorities and other relevant stakeholders at the national level.

(2) In pursuance of the cooperation in subsection (1), the Malawi CERT shall establish cooperation relationships with critical information infrastructure owners and operators, private sector, academia, civil society actors, or any other relevant stakeholder, for the purpose of achieving the objectives of this Act.

(3) Where appropriate, the Malawi CERT may exchange relevant information with sectoral or cross-sectoral stakeholders.

(4) For the purpose of achieving effective incident coordination, a sectoral CERT or an owner of a critical information infrastructure shall designate a person to be a contact point for incident reporting.

International cooperation

12. – (1) For the purpose of cybersecurity assistance and the effective, efficient and secure exchange of information, the Malawi CERT may establish bilateral or multilateral cooperation relationships with relevant cybersecurity bodies in other countries.

(2) The Malawi CERT may participate in international cooperation networks and exchange relevant information with the national CERTs of other countries or entities similar to the Malawi CERT.

(3) Where the Malawi CERT engages in exchange of information, it shall use internationally recognized information-sharing protocols and adhere to personal data protection principles.

PART III - CYBER INSPECTION

Appointment of cyber inspectors

13. - (1) The Authority shall appoint cyber inspectors on terms and conditions determined by the Authority.

(2) A person may be appointed as a cyber inspector if he -

(a) is a citizen of Malawi;

(b) is resident in Malawi; and

(b) possesses qualifications, expertise and experience in any of the following areas –

(i) information and communications technology;

(ii) law;

(iii) economics;

(iv) finance; or

(v) law enforcement.

(3) A person shall be disqualified from being appointed as a cyber inspector if he -

(a) is a Member of Parliament;

(b) is a Minister or Deputy Minister; or

(c) holds a position in a political party or is actively involved in politics.

(4) The Authority shall provide any person appointed as a cyber inspector with a certificate of appointment.

(5) A cyber inspector shall, in performing any function under this Act, carry his identity card and shall, upon request by a person who is a subject of an investigation or the person's employee, show the identity card to the person or the employee, as the case may be.

Functions and powers of a cyber inspector

14. - (1) A cyber inspector shall monitor, audit and inspect critical information infrastructure for the purpose of ensuring compliance with this Act.

(2) Notwithstanding the generality of subsection (1), a cyber inspector may, with a search or seizure warrant -

(a) enter and inspect the premises of an owner of critical information infrastructure, if there are reasonable grounds to believe that the owner has contravened the provisions of this Act;

(b) search any person, premises or systems holding critical information infrastructure;

(c) take extracts from, or make copies of, any book, document, record or any element that is in the premises or system and has a bearing on an investigation;

(d) demand the production of, and inspect, relevant authorizations, declarations and certificates;

(e) require the person by whom, or on whose behalf, the cyber inspector has reasonable cause to suspect that a computer or information system is or has been used, or require any person in control of, or otherwise involved with the operation of the computer or information system, to provide the cyber inspector with such reasonable technical and other assistance as the cyber inspector may require for the purposes of this Act; and

No. … of 2023

(f) exercise any other procedural investigative powers under the Cybercrimes Act.

Hindering, obstruction, etc, of a cyber inspector

15. - (1) A person who -

(a) hinders or obstructs a cyber inspector in the performance of his functions and powers under this Act;

(b) refuses to co-operate with the cyber inspector; or

(c) falsely holds himself out as a cyber inspector,

commits an offence and shall, upon conviction, be liable to a fine of K10,000,000 and imprisonment for seven years.

(2) For the proper performance of his functions and powers under this Act, a cyber inspector may be accompanied by a police officer.

PART IV - CYBERSECURITY STANDARDS AND ENFORCEMENT

Cybersecurity standards

16. - (1) The Authority shall develop, establish and adopt standards in the cybersecurity space for governance and risk management and any other relevant area that the Authority may determine in accordance with international best practices.

(2) The Authority shall publish on its website the standards developed and promote their adoption by the public and private sectors.

(3) The Authority shall take the necessary measures to enforce the cybersecurity standards adopted and monitor compliance by the public and private sectors.

(4) A person who fails to comply with the cybersecurity standards is liable to pay to the Authority the administrative penalty specified in the Schedule.

Certificate of compliance

17. A cyber inspector shall issue a certificate of compliance where he is satisfied that the standards set by the Authority from time to time have been met.

PART V - CRITICAL INFORMATION INFRASTRUCTURE

Designation of critical information infrastructure

18. - (1) The Minister may, on the advice of the Authority, designate a computer system or computer network as a critical information infrastructure if the Minister considers that the computer system or computer network is essential for –

(a) national security, or

(b) the economic and social wellbeing of citizens.

(2) Where the Minister designates a computer system or computer network as a critical information infrastructure under subsection (1), the Minister shall publish the designation in the Gazette.

(3) The Minister shall, in designating a computer system or computer network as a critical information infrastructure under subsection (1), consider if the computer system or computer network is necessary for –

(a) the security, defence or international relations of the country;

(b) the production, preservation or identity of a confidential source of information related to the enforcement of criminal law;

(c) the provision of services directly related to –

(i) communication and telecommunication infrastructure;

(ii) banking and financial services;

(iii) public utilities;

(iv) public transportation; and

(v) public key infrastructure;

(d) the protection of public safety and public health, including systems related to essential emergency services;

(e) an international business or communication affecting a citizen of Malawi or any other international business in which a citizen of Malawi or the Government has an interest; or

(f) the functions of the Legislature, Executive, Judiciary or security agencies.

(4) The Minister shall establish a procedure for the regulation of critical information infrastructure.

(5) Where the Minister establishes a procedure for the regulation of critical information infrastructure under subsection (4), the Minister shall publish the procedure in the Gazette.

Registration of critical information infrastructure

19. – (1) An owner of critical information infrastructure shall register with the Authority.

(2) An owner of critical information infrastructure operating in Malawi prior to the commencement of this Act shall, within six months from the commencement of this Act, register with the Authority.

(3) When registering critical information infrastructure under subsection (1), the owner shall provide the following information –

(a) his name or the name of the person who is in control of the critical information infrastructure;
(b) the nature and type of the critical information infrastructure;
(c) the use or function of the critical information infrastructure; and
(d) any other information that the Authority may deem necessary.

(4) Any change in the legal ownership of a registered critical information infrastructure shall be subject to the approval of the Authority.

(5) An owner of a registered critical information infrastructure who contravenes subsection (2) is liable to pay to the Authority the administrative penalty specified in the Schedule.

Withdrawal of designation of critical information infrastructure

20. – (1) The Minister may, on the advice of the Authority, withdraw the designation of a critical information infrastructure at any time if the Minister considers that the computer system or computer network no longer satisfies the criteria of a critical information infrastructure.

(2) Where the Minister withdraws a designation of critical information infrastructure under subsection (1), the Minister shall publish the withdrawal in the Gazette.

Duty of owner of critical information infrastructure

21. - (1) An owner of critical information infrastructure shall –

(a) within twenty four hours after a cybersecurity incident is detected, report the incident to –

(i) the relevant sectoral CERT; or

(ii) the Malawi CERT, if the critical information infrastructure does not belong to any sectoral CERT;

(b) cause an audit to be conducted on the critical information infrastructure; and

(c) submit a copy of the audit report to the Authority.

(2) An owner of critical information infrastructure who fails to comply with subsection (1) is liable to pay to the Authority the administrative penalty specified in the Schedule.

Access to critical information infrastructure

22. - (1) A person shall not, without authorization –

(a) secure access; or

(b) attempt to secure access,

to a computer system or a computer network designated as a critical information infrastructure.

(2) A person shall not, without lawful justification, block –

(a) access to critical information infrastructure; or

(c) access to a site that is hosting critical information infrastructure.

(3) A person who contravenes subsections (1) and (2) commits an offence and shall, upon conviction, be liable to a fine of K5,000,000 and to imprisonment for five years.

(4) Where the offence committed under subsections (1) and (2) –

(a) results in a serious bodily injury, or financial loss or damage to the computer system or computer network designated as a critical information infrastructure, the person who committed the offence shall, upon conviction –

(i) in the case of an individual, be liable to a fine of K15,000,000 and imprisonment for fifteen years; and

(ii) in the case of a body corporate, a partnership or a firm, be liable to a fine of K25,000,000; and

(b) is deemed to be a terrorist act, the person who committed the offence shall, upon conviction, be liable to imprisonment for twenty five years.

(5) In addition to the penalty provided under subsection (4) (a) (ii), every director or officer of the body corporate, or member of the partnership, or any other person concerned with the management of the firm, shall be deemed to have committed the same offence and shall, upon summary conviction, be liable to a fine of K10,000,000.

(6) A person shall not be convicted of an offence by virtue of subsection (5) if it is proved that –

(a) due diligence was exercised on the part of the person to prevent the commission of the offence; or

(b) the offence was committed without the knowledge, consent or connivance of the person.

Localization of critical data

23. - (1) An owner of critical data shall store all critical data on a server or data center that is located within Malawi.

(2) Notwithstanding subsection (1), the Minister may authorize an owner of critical data to externalize the critical data outside Malawi.

(3) In the event that the purpose for which the critical data was collected expires, or the data controller ceases to exist, the critical data shall be surrendered to the Authority.

PART VI - CYBERSECURITY INCIDENT REPORTING

Duty to report cybersecurity incident

24. - (1) Where a particular sector has experienced a cybersecurity incident, the relevant sectoral CERT shall report to the Malawi CERT on the occurrence of the incident.

(2) A sectoral CERT shall, within thirty days, submit to the Malawi CERT a monthly report covering the operations of that CERT, including a report of a cybersecurity incident.

(3) The Malawi CERT shall establish a cybersecurity incident reporting and information sharing platform to enable a sectoral CERT, an owner of critical information infrastructure, individuals and any other relevant institution, report a cybersecurity incident.

(4) The Malawi CERT shall, upon receipt of information in respect of a cybersecurity incident, circulate the information to the relevant sectoral CERT, the owner of critical information infrastructure, individual and any other relevant institution.

(5) A person in charge of an institution shall report a cybersecurity incident to the relevant sectoral CERT and to the Malawi CERT within twenty four hours after the incident is detected.

(6) A person who contravenes subsection (5) is liable to pay to the Authority the administrative penalty specified in the Schedule.

Cybersecurity incident point of contact

25. - (1) The Malawi CERT shall establish a cybersecurity incident point of contact to facilitate –

(a) the reporting of a cybersecurity incident by the general public; and

(b) international co-operation in cybersecurity matters.

(2) An institution that is not affiliated to a designated sectoral CERT shall report a cybersecurity incident to the Malawi CERT through the cybersecurity incident point of contact established under subsection (1).

(3) An individual may report a cybersecurity incident to the Malawi CERT through the cybersecurity incident point of contact established under subsection (1).

Early warning system

26. - (1) The Authority shall establish an early warning system in respect of human initiated risks that are likely to undermine the cybersecurity of the country.

(2) The Authority shall implement the early warning system in order to advise the public on cybersecurity matters.

PART VII — MISCELLANEOUS

Regulations

27. The Minister may, on the advice of the Authority, make regulations for carrying out or giving effect to the provisions of this Act and for such matters as are envisaged by the provisions of this Act or as the Authority may deem necessary.

SCHEDULE (sections 16, 19, 21 and 24)

ADMINISTRATIVE PENALTIES

OBJECTS AND REASONS