Internet Infrastructure Security Guidelines for Africa

A joint initiative of the Internet Society and the Commission of the African Union

30 May 2017

African Union

About the Internet Society

Founded by Internet pioneers, the Internet Society (ISOC) is a non-profit organization dedicated to ensuring the open development, evolution, and use of the Internet. Working through a global community of chapters and members, the Internet Society collaborates with a broad range of groups to promote the technologies that keep the Internet safe and secure, and advocates for policies that enable universal access. The Internet Society is also the organizational home of the Internet Engineering Task Force (IETF).

About the Commission of the African Union

The African Union (AU) was officially launched in July 2002 in Durban, South Africa, following a decision in September 1999 by its predecessor, the Organisation of African Unity (OAU) which was formed in 1963, to create a new continental organization to build on its work.

A total number of 54 countries joined the new organization, whose headquarters remained in Addis Ababa, Ethiopia.

The Commission of the African Union (AUC) is the secretariat of the AU, entrusted with executive functions, it is composed of ten officials, a Chairperson, a Deputy Chairperson and eight Commissioners.

The structure represents the AU and protects its interests under the auspices of the Assembly of Heads of States and Governments as well as the Executive Committee. The AUC is made up of portfolios which are: Peace and Security, Political Affairs, Trade and Industry, Infrastructure and Energy, Social Affairs, Rural Economy and Agriculture, Human Resources, Science and Technology, and Economic Affairs.

The guiding vision for Agenda 2063 is the AU Vision of: “An integrated, prosperous and peaceful Africa, driven by its own citizens and representing a dynamic force in the global arena”. The mission of the AU Commission is “to become an efficient and value adding institution driving the Africa integration and development process in close collaboration with African Union Member States, the regional economic communities, and African citizens”.

Acknowledgments

We would like to acknowledge the invaluable contributions of Ahmed Hussein (HiLCoE Computer Systems Engineering) and Mulugeta Libsie (Addis Ababa University), who worked on the first draft of the guidelines as well as reviewed the successive drafts based on the input from contributing experts, including: Souhila Amazouz (AUC), Dawit Bekele (ISOC), Abdoullah Cisse (Carapace), Niel Harper (ISOC), Jean-Robert Hountomey (AfricaCERT), Olaf Kolkman (ISOC), Ben Maddison (Workonline), Choolwe Nalubamba (ZICTA), Steve Olshansky (ISOC), Barrack Otieno (AFTLD), Ryan Polk (ISOC), Nii Quaynor (AfNOG), Andrei Robachevsky (ISOC), Bob Rotsted (NSRC), Christine Runnegar (ISOC), Joe St Sauver (Farsight Security, Inc.), and Moctar Yedaly (AUC).

Table of Contents

Executive Summary

In 2014, African Union (AU) members adopted the African Union Convention on Cyber Security and Personal Data Protection ("the Convention").[1]

To facilitate implementation of the Convention, the African Union Commission (AUC) asked the Internet Society (ISOC) to jointly develop Internet Infrastructure Security Guidelines for Africa ("the Guidelines"). The Guidelines were created with contributions from regional and global Internet infrastructure security experts, government and CERT representatives, and network and ccTLD DNS operators.

The Guidelines emphasize the importance of the multistakeholder model and a collaborative security approach in protecting Internet infrastructure. The Guidelines put forward four essential principles of Internet infrastructure security: Awareness, Responsibility, Cooperation, and adherence to Fundamental Rights and Internet Properties.

The Guidelines recommend the most critical actions for various stakeholders to take on Internet infrastructure security. These critical actions are tailored to the African cyber security environment's unique features: a shortage of skilled human resources; limited resources (including financial) for governments and organizations to allocate for cyber security; limited levels of awareness of cyber security issues among stakeholders; and a general lack of awareness of the risks involved in the use of information and communication technologies (ICTs).

Given the broad nature of Internet infrastructure security, a single document is not sufficient, and further work will be needed to complement the Guidelines with specific recommendations addressing particular issues. This set of recommendations is a first, yet significant, step in producing a visible and positive change in the African Internet infrastructure security landscape.

Regional (African Union) Level

- Form an Africa-wide Cyber Security Collaboration and Coordination Committee (ACS3C)
  - The committee would be a multistakeholder group that would advise policymakers of the AUC on regional strategies and capacity building, and facilitate information sharing across the region.

- Engage in Capacity Building and Knowledge Sharing on a pan-African Level
  - The AUC should develop capacity building programs, as advised by the ACS3C, in all areas of Internet infrastructure security.

National Level

- Identify and Protect Critical Internet Infrastructure
  - National governments should take a services-based approach to identifying critical Internet infrastructure for protection.

- Facilitate Information Exchange through a National Multistakeholder Structure
  - National governments should develop multistakeholder structures to advise on cyber security strategy and policy, and to facilitate information sharing.

- Establish and Strengthen National Level Computer Security Incident Response Teams (CSIRTs)
  - National governments working with other stakeholders should establish or support existing national CSIRTs to coordinate security incident response and pre-response.

1 See the Convention at http://www.au.int/en/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf

- Promote Internet Infrastructure Resilience through Internet Exchange Points (IXPs)
    - National governments should promote the use of IXPs, and greater cooperation and connectivity between different African networks to increase the resilience of Internet infrastructure.

- Use Public Institutions to Lead by Example in Cyber Security
    - Governments should adopt and follow cyber security best practices within their own infrastructure and institutions, promoting their use to other stakeholders and sectors.

ISP/Operator Level

- Establish Baseline Security
    - Network operators and service providers should implement essential routing and Domain Name System security measures, network security and other essential security practices to produce a visible and positive change in the African Internet infrastructure security landscape.

- Establish and Maintain Cooperation and Collaboration
    - Network operators and service providers should establish and maintain cooperation and collaboration as an essential component of security solutions.

Organizational Level

- Organizations should implement current best practices and strive to develop a culture of cyber security at all levels of the organization.

1. Introduction

The importance of the Internet and ICTs as effective tools for achieving socio-economic development in developing countries is widely recognized by governments, financial institutions, and development partners. The Internet and ICTs form vital infrastructure for development. They are a new source of growth, and drivers for innovation and social well-being. As the Internet economy grows, stakeholders and the rest of the economy become increasingly reliant on digital infrastructure to perform their essential functions.

The role of the Internet in supporting the economy, delivering information and education, and in enabling creativity is well understood and acknowledged. The Internet economy is a dynamic environment where technologies, applications, uses and markets constantly evolve, often in an unpredictable manner. While the Internet benefits economic growth and innovation, attacks against Internet infrastructure represent a major risk to economic growth and innovation. The joint AUC-Symantec report Cyber Crime & Cyber Security Trends in Africa, published in November 2016, reveals that 24 million malware incidents targeting Africa were observed in 2016.[2] A 2017 report from McAfee finds that, in the fourth quarter of 2016 alone, nearly 12% of their African mobile customers reported malware infections.[3] Vulnerabilities, or exploitable weaknesses, pose a threat to devices, networks and systems, along with those who rely on them. These vulnerabilities are exploited by attackers to attack an increasingly diverse range of industries, organizations and targets.[4]

In light of the threat to socio-economic development posed by attacks on Internet infrastructure, it is the responsibility of all stakeholders, including governments and Internet service providers, to agree upon solutions to ensure the Internet in every country remains safe, secure and resilient. A key aspect of choosing security solutions is to preserve the open nature of the Internet and reinforce trust.

Since the Internet is essential for the economy and for all stakeholders, the consequences of security failures can directly impact society as a whole. Therefore, there has to be a commitment by all stakeholders to secure cyber operations.

The nature of these threats continues to include activities such as theft (of identity, personal data, and secrets of all kinds), infringement of intellectual property rights, denial of service attacks, defacement, and other sources of disruption. However, large-scale distributed denial of service (DDoS) attacks, misuse or breaches of personal data, and the disruption of critical infrastructure should be of the most concern to Africa.

Africa is becoming more and more connected to the Internet. Businesses, infrastructures, governments, citizens and key industries are all becoming linked to the Internet. As the continent increasingly relies upon the Internet, protecting its critical elements becomes vital. African stakeholders in the Internet ecosystem must work together to protect the interconnected Internet infrastructure while preserving the fundamental properties of the Internet[5] and upholding fundamental rights.

Internet infrastructure security is a domain of paramount importance and magnitude. The Guidelines address areas that are relevant and specific to essential current needs in Africa.

---

2 See https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa/documents/publications/2017/03/10/report-cyber-trends-in-africa.

3 See https://www.mcafee.com/ca/security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx

4 See Annex I: Internet and Security-Related Terms for more information concerning threats, threat agents, vulnerabilities, and attacks.

5 See https://www.internetsociety.org/internet-invariants-what-really-matters and http://www.internetsociety.org/policybriefs/internetinvariants

Although the emphasis in the Guidelines is on Internet infrastructure security, it is difficult to differentiate these issues from more general Internet or network security issues. Therefore, some aspects of general network security are also covered in this document or addressed in the annex.[6]

The Guidelines aim to provide recommendations and promote principles and solutions to ensure that African Internet infrastructure security meets the requirements of users at large, and that all stakeholders have clear guidelines for achieving what is expected of them. By ensuring increased security and resiliency, the recommendations will help increase confidence in, and use of, the Internet by the African community. While the recommendations do not cover every issue in Internet infrastructure security, they are an important first step towards a resilient, safe and secure African Internet infrastructure.

1.1 Methodology

The methodology employed in developing the Guidelines included a literature review, and a process for gathering input from experts from inside and outside Africa.

The literature review utilized several different sources including recommendations and best practices published by major Internet-related institutions, organizations, and companies. These included the Internet Corporation for Assigned Names and Numbers (ICANN), the Internet Engineering Task Force (IETF), International Telecommunication Union (ITU), ISOC, the US National Institute of Standards and Technology (NIST), European Union Agency for Network and Information Security (ENISA), and the Organisation for Economic Co-operation and Development (OECD).

Valuable input was obtained in an expert panel discussion on Internet infrastructure security conducted as part of the Africa Internet Summit (AIS) held in Gaborone, Botswana, from 29 May to 10 June 2016.

Selected professionals in the Internet infrastructure field were also interviewed. Finally, draft guidelines were presented at an experts' meeting in Nairobi from 28 to 29 November 2016. During the meeting, comments were collected from participants to improve the final version of this document.

6 See Annex II: Basic Security Principles

1.2 Scope

The scope of the Guidelines is as follows:

- Although the emphasis is on Internet infrastructure security, it is difficult to clearly differentiate between Internet infrastructure security, and network security and traditional information assurance practices.7 They are related areas, whose problems and solutions also highly overlap.

- Solutions in Internet infrastructure security encompass many fields and many stakeholders, including policy-making, enacting and enforcing relevant and appropriate cyber laws, gathering and analyzing threat intelligence, information sharing and collaboration, and employing technical, economic and other solutions.

- The methods and practices concerning physical security are now fairly mature. Therefore, they are not the focus of this document. However, the Guidelines also recognize the importance of protecting physical assets as well as digital assets. The recommendations highlight a number of aspects of physical security for assets such as cables and other physical infrastructures, but the topic is not exhaustively covered in this document.

- As noted earlier, the Guidelines do not encompass all aspects of Internet infrastructure security. However, they are an important first step. Further work will be needed to create additional guidelines addressing particular issues. The Guidelines should only be regarded as a baseline document.

- Also, the research revealed a lack of capacity in Internet infrastructure security in most countries across Africa. As a result, many of the recommendations focus on capacity building at regional, national and institutional or organizational levels. They seek to develop human resources through education and training, cooperation at all levels, capacity building in information sharing, etc.

7 Information assurance are actions to protect and defend information and information systems by guaranteeing their integrity, availability, authentication, non-repudiation and confidentiality.

2. Analysis of Internet Infrastructure Security

2.1 Panel Discussion and Interview Results

On 10 June 2016, as part of the AIS in Gaborone, ISOC and the AUC held a discussion panel on "Internet Infrastructure Security in Africa". Interviews were also conducted with selected experts. The panel discussion and the interviews focused on the following five major topics:

- **What Constitutes Internet Infrastructure and What are Critical Assets**
  Internet connectivity is identified as the most important function of Internet infrastructure. The physical assets that make Internet connectivity possible include network devices such as routers, switches, firewalls, Intrusion Detection Systems, proxy servers, and IXPs. Various virtual, intangible or abstract components are also needed for the Internet to function, such as addressing, routing, application protocols and services, security protocols, and the Domain Name System (DNS).

- **The Security Threat Landscape in Africa**
  At a fundamental level, the nature of cyber threats in Africa is largely similar to elsewhere in the world. However, intermittent connectivity is a serious problem, which distinguishes Africa from much of the rest of the world. Intermittent connectivity is a result of a number of factors such as insufficient resources in terms of bandwidth, the cost of Internet connectivity, frequent power outages and blackouts, a lack of effective maintenance and scheduled patching, a lack of trained workers, natural factors (such as inclement weather), and human factors (fraud, sabotage, theft, fuel shortage, etc.). Intermittent connectivity limits the capability of stakeholders to collaborate to prepare for, or to respond to, an attack.

- **Components of Internet Infrastructure that are Easy Targets of Cyberattacks**
  Many commercial and industrial systems have embedded software that is out-of-date and/or unpatched, and are, therefore, especially vulnerable. For example, many financial systems and public sector networks are dependent on machines running software which is no longer supported by its developers, and for which security upgrades are no longer available. The mobile industry also raises similar concerns. In some instances, mobile devices are being sold with out-of-date or unpatched software. Alongside out-of-date or unsupported software, an inability or unwillingness to upgrade or patch servers and applications on a regular basis makes systems vulnerable to attack.

  Physical attacks on the infrastructure also pose a threat. The attacks could be intentional and motivated by financial reasons, political activism, or even terrorism. Physical damage to infrastructure may also be unintentional, due to factors such as a lack of proper and regular maintenance on the part of the operators, or negligence due to poor operational and management practices.

  Fiber cuts were cited as an example of physical attacks. It may be difficult to totally avoid this problem, but solutions to identify and locate cuts would help mitigate the impact. Information sharing among operators is critical in this regard.

Another problem is a lack of transparency regarding cyberattacks. Some organizations do not report security incidents. This makes it difficult to know the magnitude of the attacks in Africa and to find solutions. Therefore, a trusted ecosystem should be fostered so that everyone (including operators and end users) can learn from cyber incidents. Established practices on responsible disclosure and vulnerability disclosure coordination allow for the provision of information in ways that will not expose infrastructure to further risk, are also important.

- **Measures to Prevent and Mitigate the Risk of Cyberattack**
  Information sharing, effective legislation and enforcement, and recognized best practices were identified as important measures for preventing and mitigating the risk of cyberattacks.

  Information sharing is critical in capacity building, identifying threats, and in developing best practices (whether technical, policy, legal, economic, etc.). Ensuring the right practices are in place to enable relevant stakeholders to share information responsibly is equally important. There are many useful avenues for sharing expertise, including the African Network Operators Group (AfNOG) and the African Peering and Interconnection Forum (AfPIF). Workshops are helpful at the local level to reach the broader operators community.

  Robust legislation and enforcement help deter cybercrime, both locally and internationally. Legal and regulatory frameworks from other continents around the world provide useful starting points for best practices in the African context. National guidelines to measure the effectiveness of security policies, as well as any unintended consequences, should be developed.

  Best practices provide stakeholders with relevant and current information on security methods and threats. Best practices can promote effective network security monitoring activities and encourage operators and service providers to perform and share regular risk analyses.

- **Key stakeholders to improve the security of Internet infrastructure in Africa**
  Capacity needs to be developed in cyber security for all stakeholders in Africa. Among them are governments, the private sector, civil society, academia, and the technical community.

2.2 Core Elements of Internet Infrastructure

Based on the results of the panel discussion, interviews with professionals, and the literature review, the core elements of Internet infrastructure can be broadly categorized into six types: protocols and services, software and hardware, network interconnection, communication infrastructure, information, and human resources.

a. **Protocols and Services**
   A protocol is a standard for computer systems. Protocols allow meaningful communication between different computer systems, making them valuable assets in Internet infrastructure. Protocols can be divided into the Datalink, Internet, Transport, and Application layers.

   A service, in the context of Internet infrastructure, refers to an abstract combination of functionalities utilizing other assets to fulfil a defined task. Without services, the Internet would be of little use. Services can be categorized as Essential Addressing (which is divided into Link Layer addressing, IP addressing, Transport Protocol addressing, and DNS), Routing, Applications (such as electronic mail or file transfer), and Security Services. Attackers will exploit vulnerabilities in services and protocols, so it is important to implement the latest versions of corresponding standards to ensure the greatest security.

b. **Software and Hardware**
   In the context of core Internet infrastructure, software can be broadly categorized as operating systems, device drivers, firmware, and executable programs. Software products have several security vulnerabilities that have to be addressed through regular patching and other methods.

Hardware is a physical component of computer systems such as machines or wiring. For Internet infrastructure, they are grouped into three categories: network devices (such as switches, routers, firewalls, and gateways), servers, and end-user devices (such as personal computers or mobile devices).

c. **Network Interconnection**
As the Internet is a network of different networks, the assets providing interconnection are very valuable. Two examples that facilitate interconnection are Internet Service Providers (ISPs) and IXPs. An ISP provides customers with Internet access using different data transmission technologies. An IXP is the physical location where different IP networks meet to exchange local traffic with each other via a switch.

d. **Communication Infrastructure**
Communication infrastructure are the basic physical structures and facilities (e.g., buildings and cables) needed for the operation of the Internet. In order to build the Internet, supporting infrastructure is crucial. Infrastructure can be grouped as cabling and linking (wireless, such as microwave, radio, and satellite, and wired such as fiber, copper, broadband), buildings (special purpose facilities like landing points for undersea cables or multi-purpose data centres that are used to house all kinds of hardware and infrastructure), power supply, cooling systems, and physical security (fences, walls, doors, etc.).

e. **Information**
Information is derived from the collection of data. Systems (e.g., software, hardware, services) and humans depend on information to make reasonable decisions. In the context of Internet infrastructure, information assets are grouped into four areas, comprising: inventory (of hardware, software, infrastructure, information), network topology, system configuration, and operational information.

f. **Human Resources**
Human resources are personnel considered to be an asset to Internet infrastructure. They include administrators, operators, support team, developers, managers, auditors, and end users.

No matter how much technical security a stakeholder may have, untrained and ineffective human resources are potential vulnerabilities for their systems. Alternatively, well-trained and effective human resources enhance the security of systems. Important features of human resources include: competence, understanding and support from management, staff's discipline to follow procedures, and trustworthiness of staff members.

2.3 National Internet Infrastructure Security Principles

When developing national strategies for Internet infrastructure security, African policymakers should use four essential principles as a guide. These essential principles[8] are awareness, responsibility, cooperation, and fundamental rights and Internet properties.

a. **Awareness:** An understanding of security risks, along with how they can impact others in the Internet infrastructure ecosystem. A preparedness to recognize the risk and manage it, and evaluate the impact of actions on oneself and others in the African Internet infrastructure ecosystem.

b. **Responsibility:** Taking responsibility for the management of security risks. Due to the fundamental nature of the Internet, one should take into account the potential impacts of one's actions, or inactions, on other stakeholders before taking action.

c. **Cooperation:** Engage in an ongoing cyber security dialogue that includes actors across borders to effectively counter new and persisting threats. The security of critical Internet infrastructure cannot be achieved alone. There is a need for cooperation and collective responsibility among all stakeholders, not just the government and a selected number of stakeholders.

d. **Fundamental Rights and Internet Properties:** Actions to manage security risks must adhere to fundamental rights, be transparent, and not infringe upon the fundamental properties of the Internet: voluntary collaboration, open standards, reusable technological building blocks, integrity, permission-free innovation, and global reach.[9]

An effective approach to Internet infrastructure security must not only employ these principles, but empower all other stakeholders to use them. The approach should support conditions for collaborative security[10] and an ongoing security dialogue, encourage transparency, and empower others to safeguard the fundamental properties of the Internet. The approach should improve access and contribute to a more open Internet ecosystem, free of censorship and respectful of privacy.

8 See Annex II for basic security principles.

9 For more information on the fundamental properties of the internet, see the ISOC publication Internet Invariants: What Really Matters https://www.internetsociety.org/internet-invariants-what-really-matters

10 For more information on collaborative security, see the ISOC publication Collaborative Security: An Approach to Tackling Internet Security Issues http://www.internetsociety.org/collaborativesecurity

3. Recommendations

Cyber security is the responsibility of all stakeholders, including governments, the private sector, civil society, academia, and the technical community. Since the Internet is a global network of interconnected networks, no one stakeholder can act alone to successfully ensure the security of the Internet. Not even governments or powerful network operators can secure the Internet, as clearly shown in various major incidents just within the last year.[11] The Internet spans all nations and is made up of thousands of individual networks, each made up of even more users and devices. A trusted Internet infrastructure ecosystem can only be achieved through cooperative efforts among all stakeholders.

Every stakeholder must apply the essential principles of awareness, responsibility, cooperation, and uphold fundamental rights and Internet properties when taking specific actions to protect their systems and the wider Internet ecosystem. Otherwise, the measures that are intended to protect the Internet might end up harming it.

Based on panel discussions, interviews with experts, existing literature, and, in line with the essential principles, this section presents specific recommendations.

Although many cyber security solutions created elsewhere may work for Africa, there are some characteristics that make Africa different. Most African countries differ from the rest of the world (with the exception of some developing countries in other continents) in the following ways:

- Shortages of skilled human resources in the area of cyber security
- Limited resources (including financial resources) available to be allocated by governments, organizations and other stakeholders for cyber security
- Limited levels of awareness of cyber security issues among key stakeholders, such as ICT regulators, law enforcement agencies, the judiciary, information technology professionals, and users
- Lack of awareness of the risks involved in the use of ICTs

These differences are taken into account in these recommendations.

The Guidelines outline the following five dimensions for cyber security solutions:

- Legal and regulatory measures, including legislation and enforcement
- Capacity building, revolving around strategies for enhancing knowledge, expertise and skills to boost cyber security
- Technical and procedural solutions as a way to address vulnerabilities in software and hardware
- Institutional and organizational structures, which aim to create a collaborative environment that is conducive to helping prevent, detect and respond to attacks against critical Internet infrastructure
- Effective global cooperation, focusing on strategies for continued and inclusive collaboration, coordination and information sharing among all stakeholders to reinforce trust in the Internet

However, there are other solutions, such as economic incentives, that could also be used to improve security.

11 For example the Dyn DDoS attack, the US Democratic National Committee hack, and the US Department of Justice attack.

The recommendations in this section address all five dimensions.[12] It has to be noted that some of these recommendations could already be implemented in some countries, while not in others. Although the emphasis is on Internet infrastructure security, it is sometimes difficult to separate it from the general objective of information and network security. Therefore, some recommendations may lie closer to the sphere of general information security.

3.1 Regional (AU Level)

As the Internet is designed as a collection of networks, responsibility for security is shared. Every participant should be conscious that their own security also depends on the security of neighbouring networks and that their security decisions impact others. There is a collective responsibility to implement best practices for Internet security. We recommend establishing a coordination structure at the continental level and engaging in new capacity building initiatives. It should be noted that we have surveyed the existing Africa-wide institutions that are engaged in Internet-related activities to avoid any major duplication of efforts.

3.1.1 Form an Africa-Wide Cyber Security Collaboration and Coordination Committee (ACS3C)

An Africa-Wide Cyber Security Collaboration and Cooperation Committee (ACS3C) would help facilitate coordination and information sharing among stakeholders, help identify cyber security areas where resources are needed, and advise African Union policymakers on regional strategies and capacity building.

The Committee would be an evolving, compact, and trusted network of experts formed by the AUC in collaboration with the African Internet community. The Committee's leadership should be multistakeholder. It should include experts from relevant Africa-wide and national level organizations, and institutions such as AfricaCERT, representatives from academia, the technical community, civil society, regional law enforcement agencies, and some national cyber security multistakeholder structures. Through its multistakeholder network structure, the Committee could more flexibly adapt to the new and emerging security challenges facing Africa. The Committee could be tasked to advise and support the AUC in its cybersecurity activities by:

- Advising the AUC on cyber security issues and policies, such as capacity building initiatives
- Proposing solutions to facilitate the implementation of the Convention
- Sharing best practice recommendations for Internet infrastructure security
- Identifying areas of research needed for the formulation of policies, guidelines, etc., which can be general or sector-specific, for instance, cyber security for smart grid technologies in the electric power industry, for financial systems, and for equipment monitoring tools
- Identifying ways to support Computer Security Incident Response Teams (CSIRTs), including AfricaCERT, in the area of capacity building and information sharing at the regional and African Union level
- Encouraging close collaboration among stakeholders, including in responsible and coordinated disclosure
- Proposing ways to increase the skills of security professionals in Africa (e.g. by fostering trusted certification programs)
- Supporting the AUC in formulating strategies for cyber security and capacity building
- Supporting the AUC and Member States in international cooperation regarding cyber security

The Committee should work in close collaboration with the Communication and Information Communications Technology (ICT) Specialized Technical Committee of the AU.

12 For expanded recommendations on legal measures see, for example, UNECA's "Tackling the challenges of cyber security in Africa", Issue Number NTIS/002/2014.

Details regarding its name, mission, vision, objectives, and detailed activities could be developed by the AUC in collaboration with African Internet community.

3.1.2 Engage in Capacity Building and Knowledge Sharing on a pan-African Level

Capacity building and knowledge sharing are critical to securing Internet infrastructure in Africa. Stakeholders, be they individuals, governments, organizations or others, need to be equipped with the tools necessary to help ensure Internet infrastructure security while preserving economic and social prosperity. This includes current and usable information on threats and security techniques, along with how to implement them. Cyber security research and development in Africa should be improved to create more usable and current tools for African stakeholders. Because of the international nature of the Internet, information needs to be made available to all stakeholders, not only those within a national border.

To achieve these goals, the AUC should create capacity building programs, based on needs assessments, to equip stakeholders with the skills needed to secure Internet infrastructure. These programs will spread state-of-the-art tools, techniques, and practices to other stakeholders through awareness-raising initiatives. The initiatives could take many forms including workshops, training courses, and conferences. All stakeholders should be considered in the needs assessment.

Initiatives would be developed in a multi-step process. First, the ACS3C would identify capacity gaps in cyber security and advise the AUC on how to take action. The AU would develop programs based on the needs identified by ACS3C and implement them in collaboration with partner organizations. Possible partner organizations or institutions include CSIRTs, academic and research institutions, the Internet technical community, the private sector and civil society.

By using an initiative-based approach to capacity building, the AU would be able to tailor its efforts to specific needs and environments within different African countries. Importantly, the initiatives would not be solely technical. Instead, they would provide capacity building in all areas of Internet infrastructure security, including economic and policy dimensions. Importantly, these initiatives will enable capacity building among stakeholders who may not have the resources to allocate towards similar initiatives of their own. The programs would also foster expert organizations that could continue to support capacity building in a particular topic, even after the original initiative is completed.

3.2 National Level

Alongside the role national governments have in facilitating information sharing and promoting best practices, governments hold the unique position of legislator in the Internet infrastructure ecosystem. Therefore, governments should champion awareness and accountability. Governments have the ability to pass laws on Internet infrastructure security. It is important that the laws enacted by governments adhere to the four essential principles of awareness, responsibility, cooperation, and fundamental rights and Internet properties. It is also important that the application and potential impact of new laws are carefully considered before they are enacted. Ratifying and applying the Convention is a strong first step towards creating an African legal context in which a healthy Internet infrastructure security ecosystem could develop. Further, governments should consider using other tools they have available such as the ability to offer economic incentives, driving change through procurement, encouraging industry to self-regulate, and empowering citizens to demand better security solutions. Sometimes these solutions can be more effective than laws.

3.2.1 Identify and Protect Critical Internet Infrastructure

Identifying critical Internet infrastructure is as important as fostering actions for their security. Misclassifying critical Internet infrastructure can undermine other aspects of critical Internet infrastructure protection (CIIP). Misclassified critical Internet infrastructure does not benefit from

policies designed for CIIP. This may result in inadequate security of these assets and services. Likewise, non-critical Internet infrastructure classified as "critical" is impacted by policies created for CIIP, potentially harming its efficiency.

African governments and other stakeholders should take a service-based approach to identifying critical Internet infrastructure. That means that services, such as those vital "for public safety, economic stability, national security, international stability, and for the sustainability and restoration of cyberspace"[13] should be studied to discern the Internet infrastructure essential for the provision of these vital services. This infrastructure is then classified as "critical Internet infrastructure". Alongside services, the identified critical Internet infrastructure should also be examined for dependencies. Integral stakeholders related to critical Internet infrastructure should also be identified.

Prioritizing their importance, conducting risk assessments, and building appropriate security defences around them should be undertaken, while maintaining functionality. Risk assessments are especially important in this context to evaluate what security solutions make sense relative to the specific assets. Given limited resources, it is essential that the steps taken are appropriate to the risk, and neither too little or too much.

Alongside risk assessments and a services-based approach, threat modelling can be a useful method for identifying and protecting critical Internet infrastructure. Threat modelling is a method in which potential threats are identified and prioritized by assuming the attacker's point of view. This method allows defenders to determine the threat vectors likely to be used by attackers and their probable targets.

3.2.2 Facilitate Information Exchange through a National Multistakeholder Structure

Promoting information sharing at the national level is important for developing a healthy Internet infrastructure security ecosystem. National multistakeholder structures should be established to provide an advisory role to the national government on cyber security strategy and policy, and facilitate information sharing among stakeholders.

These structures should be multistakeholder in nature and include stakeholders such as the national CSIRTs, the national government, civil society, academia, the technical community, and private sector. Drawing on the expertise of its stakeholder groups, the network would identify areas where action should be taken on a national level. Examples of advised national actions could be new training programs to alleviate a capacity gap in a specific security area, or adopting a new security practice within government agencies.

3.2.3 Establish and Strengthen National Level Computer Security Incident Response Teams (CSIRTs)

CSIRTs are vital in addressing Internet infrastructure security issues. They perform an important function in identifying security incidents, helping organizations protect themselves against cyberattacks, and in recovery. The frequency and gravity of cyber threats necessitates effective watching, warning and incident response capabilities. Even a well-defended organization will likely experience a cyber incident at some point.

All stakeholders, including the AU, national governments, and the technical community, should work to establish CSIRTs where none exist, and support CSIRTs that promote the principles of awareness, responsibility, cooperation and fundamental rights and Internet properties, along with a free and open Internet.

3.2.4 Promote Internet Infrastructure Resilience through Internet Exchange Points (IXPs)

Governments should promote the use of IXPs and increased cooperation and connectivity between different African networks. IXPs can limit the scope of cyberattacks. Lower traffic loads on international connections make DDoS attacks harder to carry out on those

13 See the African Union Convention on Cyber Security and Personal Data Protection at https://www.au.int/web/en/treaties/african-union-convention-cyber-security-and-personal-data-protection

infrastructures. If an attack makes an international link unavailable, local traffic passing through an IXP is not impacted. IXPs are critical to developing a strong and resilient Internet infrastructure.

There is a need for an increase in cross-border collaboration between IXPs. Therefore, at a regional level, the African IXP Association (AFIX), which was established to coordinate and exchange knowledge among IXPs, should be supported to do more in this area. AFIX is a platform for sharing experiences and learning amongst the IXPs and operators.

3.2.5 Use Public Institutions to Lead by Example in Cyber Security

Governments, as owners and operators of information systems and networks, could lead by example by adopting best practices, using security technologies, satisfying legislative requirements, and through their procurement processes.

It is vital that governments understand the importance of integrating cyber security in their strategic ICT plans, keeping in mind that the overall objective is social and economic prosperity, and confidence in the Internet in Africa. Governments should actively promote the use of security standards and best practices in their own infrastructure, by their agencies, and by third-party suppliers of government services.

Governments can also use their budgets to ensure that appropriate resources, including budget and staff, are allocated to governmental departments and agencies to operate and secure their systems.

3.3 ISP/Operator Level

Network operators have a direct role in securing Internet infrastructure as they operate the networks in Africa. A security weakness in one operator's network not only affects that network, but potentially other networks in Africa, and those across the world.

3.3.1 Establish Baseline Security

Addressing Internet infrastructure security challenges requires collaboration and commitment from all stakeholders. In an interconnected world with dependencies spanning multiple networks, nations and continents, it is very important that all participants adhere to at least a minimum level of security – a baseline level which many will immediately surpass, and from which others can build.

3.3.1.1 Routing and Domain Name System Security

Network operators should prevent propagation of incorrect routing information; prevent traffic with spoofed source IP addresses; facilitate global operational communication and coordination between network operators; and facilitate validation of routing information on a global scale. IP spoofing, or source address forgery, is often used in denial of service attacks to make defensive filtering more difficult.

Network operators should enable DNSSEC validation on their DNS resolvers to ensure the security of DNS. Network operators should also integrate other best current practices related to routing security and resilience in their network management processes.[14]

One of the global initiatives, MANRS, the Mutually Agreed Norms for Routing Security,[15] defines a concise package of minimum but critical measures to meet the above requirements. It also outlines a number of principles and expected actions for network operators to implement to ensure the resilience and security of the global routing system. MANRS was created by members of the network operator community with support from ISOC.

---

14 Deploy 360 is a good source of information for ISPs on routing security and securing the DNS, among others (http://www.internetsociety.org/deploy360/).

15 See https://www.routingmanifesto.org/manrs/

3.3.1.2 Network Security

Securing one's network is necessary to protect the network and others in the Internet ecosystem. This includes filtering spoofed traffic and volumetric attack traffic, both incoming and outgoing, from their networks. Outgoing spoofed and attack traffic may lead to IP address reputation problems for the originating network, but will often lead to more direct negative impacts on other networks in the Internet ecosystem.

ISOC's Anti-Spam Toolkit[16] provides best practices for policymakers, network operators, and users to better secure their networks from the threat of spam. The Toolkit also provides links to outside resources on spam and combating unwanted traffic. M3AAWG's Anti-bot Code of Conduct[17] for Internet service providers advises ISPs to engage in education, detection, notification, remediation, and collaboration. The Code of Conduct promotes the essential principles of awareness, responsibility, cooperation, and upholding the fundamental rights and Internet properties.

3.3.1.3 Essential Security Practices

Secure protocols should be used in products and services supporting Internet infrastructure. For instance, TLS (transport layer security) is a cryptographic protocol that should be employed to protect web services. TLS encrypts data exchanged in an HTTP transaction and cryptographically identifies one or more of the parties engaged in a transaction. Privacy and identity are fundamental elements of secure Internet infrastructure.

Operators must also ensure software critical to Internet infrastructure is being effectively managed for security vulnerabilities. Only software that is being maintained by a vendor or an open source community should be deployed in Internet infrastructure. Operators should employ a patching policy that prioritizes the mitigation of software vulnerabilities, despite the inherent risk to up-time. Operators may also build a software vulnerability management program granting responsibility for the continued mitigation of software vulnerabilities to an individual or institution. A lack of institutional accountability for software vulnerability management is a common reason why many organizations fail to patch appropriately.

3.3.2 Establish and Maintain Cooperation and Collaboration

Beyond their participation in the national multistakeholder structures outlined in Section 3.2.2, ISPs and network operators have a responsibility to coordinate and collaborate with one another, their customer organizations, and other stakeholders. ISPs and network operators should:

- Encourage cooperation and collaboration with customer organizations, local and regional governments, and regulators in preventing, detecting and mitigating routing incidents
- Facilitate global operational communication and coordination between network operators
- Actively participate in ISP associations such as national and regional network operator groups and fora
- Create mechanisms for information sharing with other providers regarding fiber cuts, so as to make quick fixes and speed up maintenance
- Cooperate with law enforcement and regulatory agencies during the investigation and prosecution of cybercrime or other illegal activities

3.4 Institutional/Organizational Level

Executive leadership and accountability for cyber-related issues is required. An executive leader in every organization should be responsible for the information security of the organization. In that role, the executive leader can allocate resources for, and promote, an organizational cyber security culture. Security practices for organizations that utilize ICTs not only have a strong impact on the organizations themselves, but also on the wider Internet ecosystem. It

16 See http://www.internetsociety.org/spamtoolkit
17 See https://www.m3aawg.org/abcs-for-ISP-code

is, therefore, important that these organizations are aware of the impacts of their actions (or inaction) on the security of others. A clear and implemented security policy based on recurring risk assessment and underpinned by organizational commitment should contain, at the minimum, several specific action items. These include: applying basic essential measures for a healthy network; demonstrating an adequate system of controls; having a formalized process and capability to respond to cyber incidents; conducting regular exercises; establishing a disclosure process; and ensuring established relationships with other stakeholders, such as government officials and CSIRT teams.

National governments, and other stakeholders, should empower organizations and institutions to create a culture of cyber security for economic and social prosperity through information sharing, promoting best practices, and leading by example. The necessary organizational structure should be put in place in institutions that are responsible for cyber security initiatives and activities.

Organizations and institutions should implement current best practices and develop a culture of cyber security at the operational, as well as the executive level.

3.5 Global Cooperation

Cyber security threats are global in nature and constantly growing. Adopting technical solutions for prevention, detection, mitigation and recovery is one way to respond to these evolving threats. However, these technological measures have to be accompanied by cross-border collaboration to be effective. Digital boundaries do not coincide with national frontiers, making global collaboration an essential part of the response mechanism. Furthermore, the propagation and implications of threats, such as malware, illustrate that they are no longer an issue for organizations to deal with alone, but are increasingly the responsibility of all stakeholders.

Therefore, the cross-border nature of threats makes it essential to focus on strong international cooperation. This requires major efforts at the national, African, and global level. There needs to be close cooperation with global partners to prevent and to respond to cyber incidents. While formal communication can be helpful, informal trusted communication methods allow for faster responses to threats, closer ties between stakeholders, and stronger cooperation and collaboration.

Developing multiple trusted channels for communication ensures better cooperation and information sharing. Organizations, such as CSIRTs or network operator groups (NOGs), provide good avenues for collaboration. Organizations or networks can be formed geographically or concerning a specific topic or sector. Relationships between network operators, often developed in NOGs, allow for improved security. For example, when spam originates from a network with which there is a relationship, the impacted network operator can inform the operator of the origin network. As that operator is closer to the source of the spam, they are more likely to be able to solve the problem.

The importance of the international dimension of cyber security and the need for better alliances and partnerships with like-minded countries or allies, including capacity building, should not be overlooked.

4. Conclusion

The Internet has become increasingly important for economic and social development in Africa. It is a new source of growth and a driver for innovation, social well-being, national security, governance, media and citizenship. As the Internet economy grows, the entire economy and society, including governments, become increasingly reliant on digital infrastructure to perform their essential functions.

With greater technological exposure and reliance on the Internet, Africa is confronted with many new challenges related to cyber threats. Like elsewhere in the world, cyber threats have become increasingly diverse.

More and more attackers with diverse motivations are attracted by the new opportunities the Internet provides to Africa. Their direct and indirect impact is no longer limited to individual target organizations; they are now also national security concerns. Low levels of cyber security awareness, shortages of funding, the absence of government and other stakeholders' readiness to fight cybercrime and, above all, scarce cyber security skills make Africa particularly vulnerable.

The protection of critical Internet infrastructure in Africa should be both a national and a cross-border priority. Through a multistakeholder approach at regional and national levels, African countries can scale up efforts to mitigate cyber security risks. But, responsibilities must be shared by all stakeholders including governments, the private sector, civil society, academia, and the technical community.

This set of recommendations is a first, yet significant step in creating a visible positive change in the African cyber security landscape. The Internet represents an opportunity for Africa. Unlike the technological revolutions of the past, the digital revolution is well within its reach. With fast Internet adoption rates and a young population, Africa could become a world leader in Internet and other ICTs. By taking the recommended actions and employing essential principles to protect Internet infrastructure, stakeholders can help the continent protect this opportunity and move closer to embracing and leading the digital revolution.

5. Afterword

In the Internet and its related industries, Africa has an opportunity to compete and succeed internationally. With a young population and high Internet adoption rates, Africa is set to catch up to the rest of the world relatively quickly. Africa is deploying infrastructure in a novel way, relying on newer technologies like mobile devices, and 3G and 4G to drive Internet adoption.

While Africa's opportunities are great, it also faces challenges when securing Internet infrastructure. Many people use older hardware that cannot use up-to-date software, putting their systems at risk. Many people use pirated software products, which also present major security risks since they may not be patched to fix vulnerabilities or may contain malware. Many African governments also lack effective legal and regulatory frameworks to support Internet infrastructure security. Some governments negatively impact Internet infrastructure by blocking or restricting the Internet for citizens or stakeholders. Blocking or restricting the Internet limits the capabilities of stakeholders to respond and collaborate to mitigate security threats.

The Guidelines provide the key recommendations for protecting Internet infrastructure security. The recommendations represent the most important actions that need to be taken, and the essential principles to guide them, to create a baseline of Internet infrastructure security in Africa. In order to more thoroughly secure Internet infrastructure, more specific recommendations and best practices should be created by other African organizations such as CSIRTs and the proposed ACS3C. Only with ongoing multistakeholder efforts from the African Internet community can Africa overcome its challenges, embrace its opportunities, and become an Internet world leader.


10/100/1000 PCI-E
eth0
eth1
eth2
LAN

References

African Union. (2014, June, 27). African Union Convention on Cyber Security and Personal Data Protection. Retrieved from https://ccdcoe.org/sites/default/files/documents/AU-270614-CSConvention.pdf

African Union, Symantec Corporation. (2017, November). Cyber Crime & Cyber Security Trends in Africa. (Rep.) Retrieved from https://www.thegfce.com/initiatives/c/cybersecurity-and-cybercrime-trends-in-africa

Arbor Networks, Google Ideas, & Big Picture Group. (2013). What is a DDoS Attack? Retrieved from http://www.digitalattackmap.com/understanding-ddos/

Chatzis, N., Smaragdakis, G., & Feldmann, A. (2013, July 19). On the Importance of Internet eXchange Points for today's Internet Ecosystem [Scholarly project]. In Cornell University Library. Retrieved from https://arxiv.org/abs/1307.5264v2

Crucial Research. (2014, September). People's Role in Cyber Security: Academics' Perspective. [White Paper]. Retrieved from Crucial Research: https://www.crucial.com.au/pdf/Peoples_Role_in_Cyber_Security.pdf

Conrad, D. (2012, January). Towards Improving DNS Security, Stability, and Resiliency (Rep.). Retrieved https://www.internetsociety.org/sites/default/files/bp-dnsresiliency-201201-en_0.pdf

European Network and Information Security Agency. (2012, November). Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime. (Publication). Retrieved https://www.enisa.europa.eu/publications/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_download/fullReport

European Network and Information Security Agency. (2013, October). Cybersecurity cooperation: Defending the digital frontline. (Publication). Retrieved https://www.enisa.europa.eu/publications/cybersecurity-cooperation-defending-the-digital-frontline

European Network and Information Security Agency. (2016, January 27). ENISA Threat Landscape 2015. (Rep.). Retrieved https://www.enisa.europa.eu/publications/etl2015

European Network and Information Security Agency. (2015, January). Threat Landscape and Good Practice Guide for Internet Infrastructure. (Publication). Retrieved https://www.enisa.europa.eu/publications/iitl/at_download/fullReport

The European Union Agency for Network and Information Security. (2015, December). Information sharing and common taxonomies between CSIRTs and Law Enforcement. (Rep.) Retrieved https://www.enisa.europa.eu/publications/information-sharing-and-common-taxonomies-between-csirts-and-law-enforcement

France, Agence Nacionale de la Sécurité des Systèmes d'Information. (2013, January). 40 essential measures for a healthy network. Retrieved from https://www.ssi.gouv.fr/en/actualite/40-essential-measures-for-a-healthy-network/

Information Commissioner's Office, UK. Security Breaches. Licensed under the Open Government Licence. Retrieved from https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/

Internet Corporation for Assigned Names and Numbers. (2009, August). SAC 40 - Measures to Protect Domain Registration Services Against Exploitation or Misuse. (Rep.) Retrieved from https://www.icann.org/en/system/files/files/sac-040-en.pdf

International Organization for Standardization/International Electrotechnical Commission. (2012, July). Information technology - Security techniques - Guidelines for cyber security. (ISO/IEC 27032:2012). Retrieved from https://www.iso.org/standard/44375.html

Internet Society. (2015, April). Collaborative Security: An approach to tackling Internet Security issues. (Publication). Retrieved from http://www.internetsociety.org/collaborativesecurity

Internet Society. (2016, June). A policy framework for an open and trusted Internet. (Publication). Retrieved from http://www.internetsociety.org/doc/policy-framework-open-and-trusted-internet

Internet Society. (2016, February). The Internet Society and African Union Commission Survey on African ICT Policy Makers. (Publication). Retrieved from https://www.internetsociety.org/doc/internet-society-and-african-union-commission-survey-african-ict-policy-makers

Internet Society. (2012, February). Internet Invariants: What Really Matters. (Publication). Retrieved from https://www.internetsociety.org/internet-invariants-what-really-matters

Internet Society. (2016, October). Policy Brief: Internet Invariants. (Brief). Retrieved from http://www.internetsociety.org/policybriefs/internetinvariants

Internet Society. (2011). Deploy 360. Retrieved from http://www.internetsociety.org/deploy360/

Internet Society. (2015). Anti-Spam Toolkit. Retrieved from https://www.internetsociety.org/spamtoolkit

International Telecommunications Union. (2011, September). The ITU National Cybersecurity Strategy Guide (Publication). Retrieved from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITUNationalCybersecurityStrategyGuide.pdf

International Telecommunications Union, World Telecommunication Standards Assembly. Resolution 58, Encourage the creation of national Computer Incident Response Teams, particularly for developing countries (20-29, November, 2012) Retrieved from https://www.itu.int/en/ITU-T/wtsa12/Documents/resolutions/Resolution%2058.pdf

International Telecommunications Union, Plenipotentiary Conference of the International Telecommunication Union. Resolution 130, Strengthening the role of ITU in building confidence and security in the use of information and communication technologies. (2014). Retrieved from https://www.itu.int/en/action/cybersecurity/Documents/Resolutions/pp-14_Res.%20130.pdf

International Telecommunications Union Development Sector. (2009, April). Understanding Cybercrime: A Guide for Developing Countries, ICT Applications and Cybersecurity Division, Policies and Strategies Department. (Rep.) Retrieved from https://www.itu.int/ITU-D/cyb/cybersecurity/docs/itu-understanding-cybercrime-guide.pdf

Krebs, B. (2016, October). Hacked Cameras, DVRs Powered Today's Massive Internet Outage. Retrieved from https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

MANRS. (2014). Mutually Agreed Norms for Routing Security https://www.routingmanifesto.org/

McAfee. (2017, April). McAfee Labs Threat Report: April 2017 (Rep.) Retrieved from https://www.mcafee.com/ca/security-awareness/articles/mcafee-labs-threats-report-mar-2017.aspx

Messaging, Malware and Mobile Anti-Abuse Working Group. (2012, March). The Anti-Bot Code of Conduct for Internet Service Providers: A Voluntary Industry Code to Help Reduce End-User Bots. (Publication). Retrieved from https://www.m3aawg.org/abcs-for-ISP-code

Michael, C. (2009, August). Computer Viruses Slow African Expansion. Guardian. Retrieved from https://www.theguardian.com/technology/2009/aug/12/ethiopia-computer-virus

Nakashima, E. (2016, October), US government officially accuses Russia of hacking campaign to interfere with elections. Washington Post. Retrieved from https://www.washingtonpost.com/world/national-security/us-government-officially-accuses-russia-of-hacking-campaign-to-influence-elections/2016/10/07/4e0b9654-8cbf-11e6-875e-2c1bfe943b66_story.html?utm_term=.9961e9ff4fb3

Wilson, M., & Hash, J. (2003, October). Building an Information Technology Security Awareness and Training Program (United States, National Institute of Standards and Technology). Retrieved from http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-50.pdf

Organisation for Economic Co-operation and Development. Ministerial Meeting on the Future of the Internet Economy (2008, June). OECD Recommendation of the Council on the Protection of Critical Information Infrastructures OECD Ministerial Meeting on the Future of the Internet Economy.

Schumann, R., & Kende, M. (2013, May). Lifting barriers to Internet development in Africa: Suggestions for improving connectivity. (Rep.) Retrieved from http://www.internetsociety.org/doc/lifting-barriers-internet-development-africa-suggestions-improving-connectivity

SANS Institute. (2015, December). Infrastructure Security Architecture for Effective Security Monitoring. (Publication) Retrieved from https://www.sans.org/reading-room/whitepapers/bestprac/infrastructure-security-architecture-effective-security-monitoring-36512

SSAC (ICANN Security and Stability Advisory Committee). (2009). SAC 40: Measures to Protect Domain Registration Services Against Exploitation or Misuse. (Publication) Retrieved from https://www.icann.org/en/system/files/files/sac-040-en.pdf

Storm, D. (2016 February). Hackers Breach DOJ, dump details of 9,000 DHS employees, plan to leak 20,000 from FBI. Computerworld. Retrieved from http://www.computerworld.com/article/3030983/security/hackers-breach-doj-dump-details-of-9-000-dhs-employees-plan-to-leak-20-000-from-fbi.html

Symantec. (2016). Internet Security Report (21 vol.). Symantec. Retrieved from https://www.symantec.com/content/dam/symantec/docs/reports/istr-21-2016-en.pdf

Symantec. (2013, April). Internet Security Threat Report (18 vol.). Symantec. Retrieved from http://www.symantec.com/about/news/resources/press_kits/detail.jsp?pkid=istr-18

United Nations Economic Commission for Africa (2014), Tackling the challenges of cyber security in Africa. (Publication) Retrieved from http://www.uneca.org/sites/default/files/PublicationFiles/ntis_policy_brief_1.pdf

United States National Institute of Standards and Technology. (2014, February, 12). Framework for Improving Critical Infrastructure Cybersecurity. (United States, National Institute of Standards and Technology). Retrieved from https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf

Annexes

The following annexes include definitions to help explain the concepts and terminology found in the Guidelines for audiences that may not be familiar with the terms. The definitions do not form a complete glossary, nor are they the authoritative definitions on these subjects. They are intended to provide a simple introduction to the terms.

Annex I: Internet and Security-Related Terms

a. **Attacks and Attack Vectors**
   - Attackers may use a variety of tools, scripts, and programs to launch attacks against networks and network devices, and to deceive or otherwise compromise staff or vendors with access to the network – whether on-site or remotely. Typically, the network devices under attack are the endpoints, such as servers and desktop computers. A cyberattack occurs if an attacker successfully breaches security controls.

   - An attack vector is a means by which an attacker can gain access to a network in order to deliver a payload with malware. Attack vectors enable attackers to exploit system vulnerabilities. The major attack vectors are botnets, DNS attacks, phishing (including targeted or "spear phishing"), and routing table poisoning attacks.

b. **Best Practices**
   - A method or practice which is generally accepted as the preferred way to achieve the desired outcome.

c. **Breaches of Personal Data**
   - In the context of networks, "a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision" [18] of an electronic communications service.

d. **Collaborative Security Approach**
   - The collaborative security approach to Internet security recognizes that people are what ultimately hold the Internet together. The Internet's development has been based on voluntary cooperation and collaboration. Cooperation and collaboration remain the essential factors for its prosperity and potential. The approach emphasizes five principles: preserving opportunities and building confidence; collective responsibility; security solutions fully integrated with rights and the open Internet; security solutions grounded in experience, developed by consensus and evolutionary in outlook; and targeting the point of maximum impact – think globally, act locally.[19]

e. **Computer Security Incident Response Team (CSIRT)**
   - An organization or community of experts that receives, reviews, and responds to computer security incidents. They may be geographically or sector specific, and led by the public and/or private sector. CSIRTs provide a critical knowledge sharing function to ensure security.

18 See https://ico.org.uk/for-organisations/guide-to-pecr/communications-networks-and-services/security-breaches/.
19 See http://www.internetsociety.org/collaborativesecurity

f. **Critical Internet Infrastructure**
   - Interconnected systems and networks, the disruption or destruction of which would have a serious impact on the health, safety, security, or economic well-being of citizens, the provision of essential services, or the effective functioning of government or economy.

g. **Distributed Denial of Service (DDoS) Attacks**
   - A DDoS attack "is an attempt to make an online service unavailable by overwhelming it with traffic from multiple sources"[20].

h. **Domain Name System (DNS):**
   - A distributed database that allows human-readable names to be translated into IP addresses which are used to identify Internet-connected devices or systems. A query of a DNS server will match a domain name to the IP address required by the computer to route the traffic to its intended destination.

i. **Fundamental Properties of the Internet (or Internet Invariants)**
   - "Characteristics which have enabled the Internet to serve as a platform for seemingly limitless innovation, outline not only its technology, but also its shape in terms of global impact and social structures"[21]. These identified characteristics are: voluntary collaboration, open standards, reusable technological building blocks, integrity, permission-free innovation, and global reach.

j. **Internet Exchange Point (IXP)**
   - A system that allows many Internet-based networks to exchange traffic with each other at a common meeting point, thus eliminating the need to build separate bilateral links with each local network.

k. **Internet Infrastructure**
   - The elements which make up and enable the movement of usable data across an interconnected network of networks. These elements include protocols and services, software and hardware, network interconnection, communication infrastructure, information, and human resources.

l. **Internet Service Provider (ISP)**
   - A company or organization that provides individuals, organizations, enterprises and others with access to the Internet. Aside from connecting users, ISPs often provide other services such as email and hosting of websites for their customers.

m. **Routing**
   - Routing determines how traffic will travel from one point in the network(s) to another. Network nodes that make routing decisions are called routers. Reachability information (i.e. whether a particular network can be reached through a node) is exchanged among the Internet routers. The two types of protocols used to exchange this information are Interior Gateway Protocol used between the routers inside a network (such as OSPF, IS-IS or RIP) and exterior gateway protocol used between networks, or autonomous systems (AS), which is Border Gateway Protocol. One of the vulnerabilities of BGP is that it does not provide means to check the validity of the information exchanged. Such validation requires use of additional tools and practices.

n. **Stakeholders**
   - The individuals, groups, organizations, entities or communities which have an interest or stake in the Internet. Stakeholders include governments, the private sector, civil society, academia, and the technical community.

---

20 See http://www.digitalattackmap.com/understanding-ddos/
21 See https://www.internetsociety.org/internet-invariants-what-really-matters

o. Threats

- A threat is a potential event that can take advantage of a vulnerabilities (weaknesses in systems, networks and devices) and cause a negative impact on the network, system, or organization. A threat is the possible event, while an attack is the incidence of such an event. Threats can be accidental or intentional. Accidental threats do not have premeditated intent. Examples are potential system or software malfunctions, misconfigurations, or accidental disclosure of sensitive or private information. Intentional threats are possible deliberate acts against the security of an asset. Intentional threats range from potential casual examination of a computer network using easily available monitoring tools, to sophisticated deliberate attacks using special system knowledge.

- Threats to the network need to be identified, and the related vulnerabilities need to be addressed to minimize the risk of the threats. The major cyber threats are malware, web-based attacks, web application attacks, denial of service, phishing, and identity theft. Insider threats are just as dangerous as those coming from outside the network.

p. Threat Agents

- It is customary to use the term attacker to refer to any individual attacking a computer system. "Threat agent" is a more inclusive term, referring to individuals who are attacking or have attacked a network, system or organization, alongside those who would capitalize upon a vulnerability (either intentionally or accidentally) and cause a negative impact upon the network, system or organization.

- Risk assessment techniques require that a threat assessment be performed to identify the threats a system faces, and the actors or the sources behind them. Though it is possible to identify a threat and the corresponding attack vectors employed, identifying the threat agent is not straightforward. Collecting and analyzing event logs through specialized systems such as Intrusion Detection System (IDS) or even Security Information and Event Management (SIEM) systems could easily reveal the attempted or successful threats that took place, but threat agent identification and analyzing their attributes requires further investigation and expertise beyond the scope of a pure cyber security domain. Threat agent identification should also encompass attributes such as motivation, capability, opportunity exploited, and potential impact to the target system. Log analysis is a useful and necessary approach, but it can be challenging to find the important information hidden in very large amounts of collected data. The logs themselves can also be used by attackers to obtain important information about the network and its defenses, and this means the logs must be protected as well.

- The major threat agents are insider threats, malicious attackers and hacktivists, cyber criminals, cyber spies, and cyber terrorists. Any of these may be independent, or may be acting for or on behalf of nations (e.g. national security agencies, military, law enforcement) or commercial entities (in the case of industrial espionage or attacks).

q. Vulnerabilities

- Vulnerabilities are the weaknesses in systems, networks and devices that can be potentially exploited by threat agents to carry out an attack. Vulnerabilities can be present in communication protocols, operating systems and application software running on devices that connect to networks including routers, switches, servers, user devices, and even security devices themselves. Vulnerabilities may be introduced by poor configuration and persist due to lack of software patching.

- In general, network systems may have one or all of the following vulnerabilities or weaknesses:
    - Inherent technological weaknesses, or bugs
    - Configuration weaknesses
    - Security policy weaknesses
    - Insufficient end user training, end user carelessness and intentional end user acts.

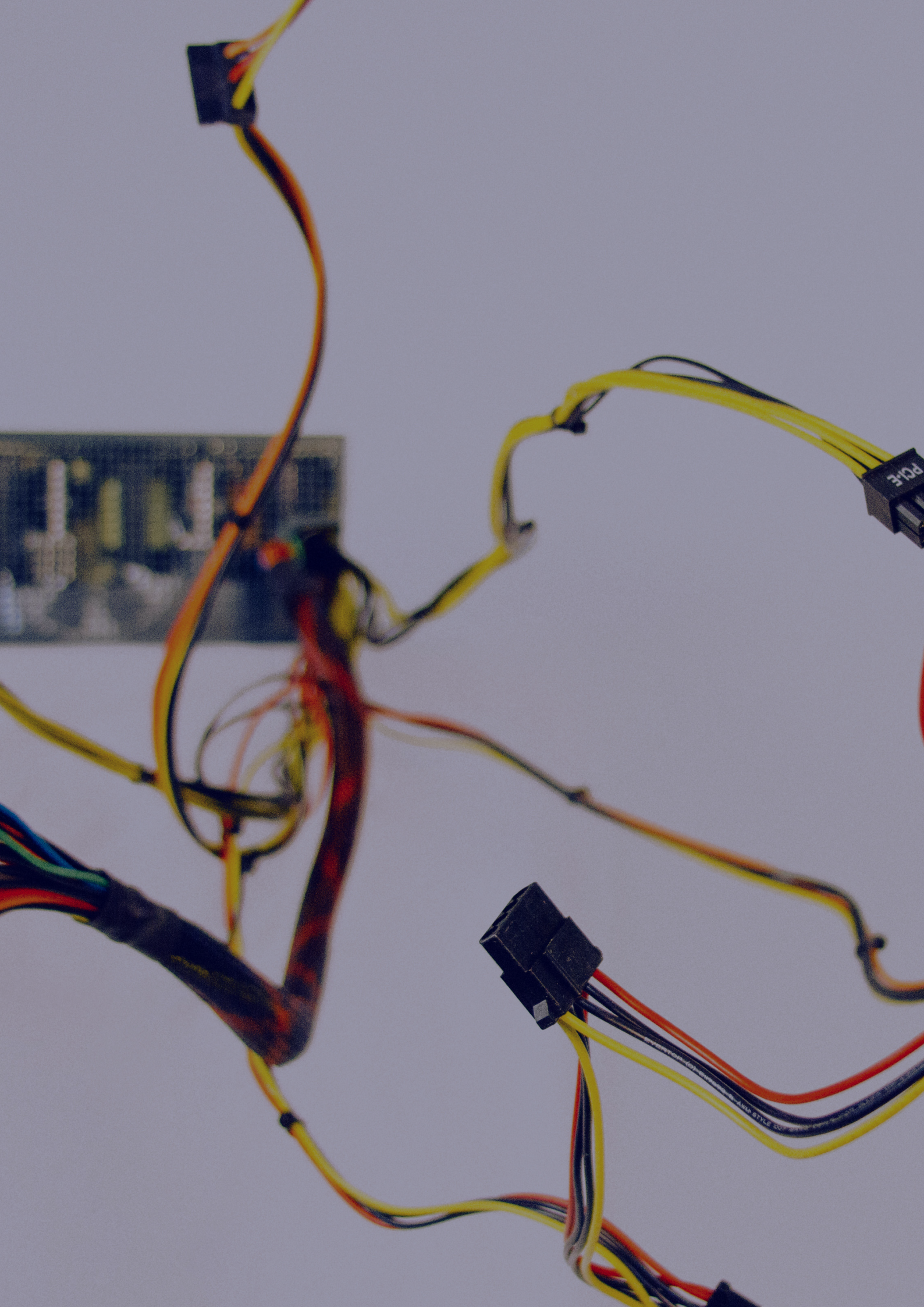
Annex II: Basic Security Principles

All stakeholders must understand the procedures for protecting Internet infrastructure assets and handling the different types of threats and weaknesses that might have an impact on the security of an organization or a country at large.

a. **Basic Protection Principles**
Once assets are identified and their vulnerabilities assessed, protection has four stages: defence/prevention, detection, reaction, and deterrence.
   - Prevention refers to taking measures to prevent the attack.
   - Detection requires developing and implementing appropriate mechanisms to quickly identify the occurrence of a security event.
   - Response means developing and implementing the appropriate actions necessary to thwart and possibly contain a detected security event.
   - Deterrence increases and signals the costs of breaking into a system, keeping potential intruders from even trying due to the very low probability of successfully breaking into the system relative to the very high costs of doing so.

b. **Least Privilege Principle**
The principle of least privilege requires that a particular user be given no more privilege to perform actions or access information than is necessary to perform their function or job. Moreover, the principle also dictates that users use the lowest level of their privileges whenever possible.

c. **Defence in Depth Principle**
No single security control can protect an organization. Defence in depth is a layered approach to address or protect against threats, or to reduce vulnerability. For instance, perimeter security controls such as firewalls, intrusion detection/prevention systems or network access controls should be complemented with endpoint security controls such as anti-malware and host intrusion detection systems. The use of layered and complementary controls will increase the effort an attacker must expend to successfully attack the system, offering deterrence.


PCI-E