# CRAN

Communications Regulatory Authority of Namibia

# 7th NATIONAL ICT SUMMIT 2023 – NAM-CSIRT

**By Elton Witbooi**
**Executive: Cybersecurity & ICT - CRAN**

CRAN

# Talking Points

- Introduction - Speaker
- The Digital Economy & Cybersecurity
- Country Profile - Namibia
- Cybersecurity & NAM-CSIRT Background
- CIRT Activities
- Country Profile
- Awareness: Cyber Hygiene

# The Digital Economy & Cybersecurity

- The Digital Economy refers to activity resulting from online **connections** among people, business, devices, data, and processes. The backbone of the digital economy is **interconnectedness**.. (Delloite, 2023)
- Widespread cybercrime and cyber insecurity is now considered among the top ten global risks for the short and long term. (WEF, 2023)
- The technology sector will be among the central targets of stronger industrial policies and enhanced state intervention. (WEF, 2023)
- Trust is critical for increasing online economic activity, hence the need for improved cybersecurity.

# Cybersecurity & NAM-CSIRT Background

- The Malabo Convention – 2014 -(Electronic Transactions, Data Protection, Cybersecurity & Cybercrime)
- The Readiness Report for CIRT Establishment – (ITU, 2017) – Recommendation to establish CIRT
- National Cybersecurity Strategy & Awareness Raising Plan 2022-2027
  - 5 Pillars
  - Enabling Legal Framework & Enforcement – Cyber Crime Bill
  - Building National Capacity on Cybersecurity – NAM-CSIRT
  - Cybersecurity Awareness
  - National & International Cooperation
- CRAN NAM-CSIRT Initiatives
  - NSCIRT Implementation Plan 2020 (revised in 2023)
  - Phase Zero
    - Published RFC2350
    - Identified Alert sources – Shadowserver
    - Budget & Funding Request
    - Job Descriptions (Manager, Incident Handler & Vulnerability Analyst)
    - Relationships with other CIRTS
    - Cooperation/Coordination Agreements with neighbouring countries (Botswana & RSA)
    - Capacity Building - Cyberdrills

# Cybersecurity & NAM-CSIRT Background

- CRAN NAM-CSIRT Preparatory Work
  - Appoint Manager
  - Identify Office Space
  - Identify Hardware & Software
  - Engagements with industry experts (Cyber4Dev)
  - Stakeholder engagements to develop Constituency
  - Participation in the development of the Cybercrime law.

# Cybersecurity & NAM-CSIRT Background

- **Gap**
  - **Finalisation of Law**
  - **Human Resource Capacity Building for NAM-CSIRT**
  - **Develop Regulatory Instruments: Policies, Regulations, and guidelines for enhancing cybersecurity.**
  - **Develop Constituency: owners and operators of Critical Infrastructure & Critical Information Infrastructure. A multi-stakeholder approach.**
  - **Awareness Campaigns (ongoing)**

# CIRT Activities

- Benefits
  - Build Confidence in the Digital Economy
  - Protecting CI & CII
  - Improve National Cyber Resilience
  - Improve Global Cybersecurity through Local & Int'l Collaboration
- Activities & Services
  - Awareness Campaigns
  - Announcements (alerts, vulnerability warnings)
  - Technology Watch (trend analysis, cooperation with Int'l CIRTs)
  - Development of Technical Capacity
  - Constituency Development – A Multi-stakeholder Approach
  - Incident Handling/Management
    - Coordinating actions
    - Technical Remediation (in limited cases).
    - Documentation for lessons learned

# Country Profile – ITU 2020

**Namibia (Republic of)**


**Development Level:**
Developing Country

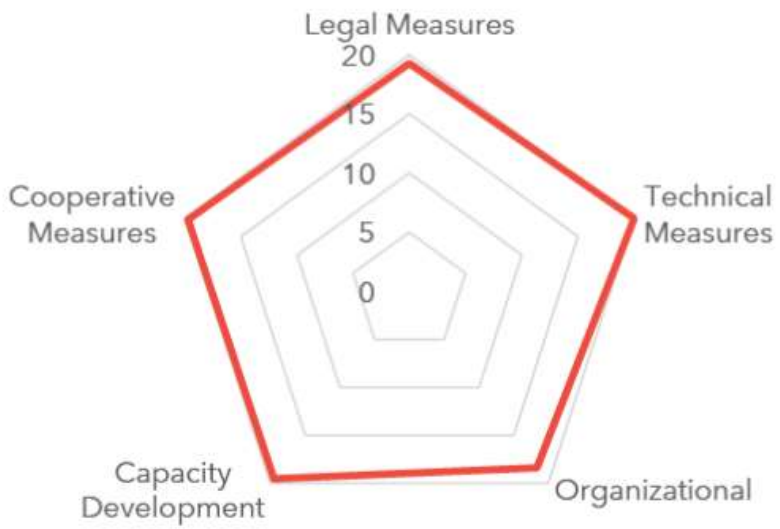
**Area(s) of Relative Strength**
Cooperative Measures
**Area(s) of Potential Growth**
Technical, Organizational Measures

| Overall Score | Legal Measures | Technical Measures | Organizational Measures | Capacity Development | Cooperative Measures |
|---|---|---|---|---|---|
| 11.47 | 2.84 | 0.00 | 0.00 | 2.34 | 6.30 |

Source: ITU Global Cybersecurity Index v4, 2020

# Country Profile – Mauritius Comparison – ITU 2020

**Mauritius (Republic of)**




**Development Level:**
Developing Country, Small Island Developing States (SIDS)

**Area(s) of Relative Strength**
Technical, Cooperative, Capacity Development Measures

**Area(s) of Potential Growth**
Organizational Measures

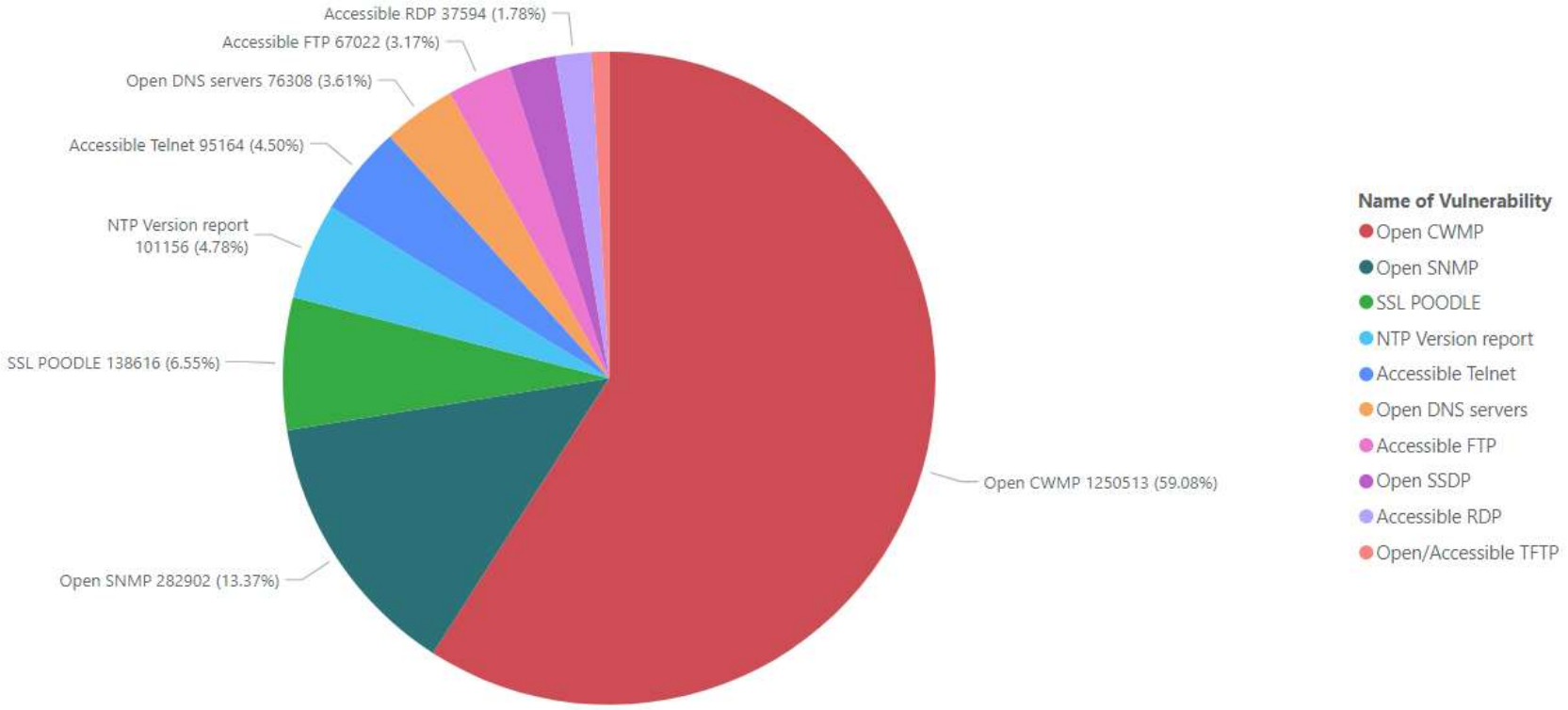
| Overall Score | Legal Measures | Technical Measures | Organizational Measures | Capacity Development | Cooperative Measures |
|---|---|---|---|---|---|
| 96.89 | 19.27 | 20.00 | 18.38 | 19.54 | 19.70 |

Source: ITU Global Cybersecurity Index v4, 2020

CRAN

1/1/2023 10/4/2023

## Top 10 Cyber Vulnerabilities



# Awarenesss – Cyber Hygiene

- Governance & Auditing - Establish a robust Security Policy to embed good security practices by IT department and employees. Periodic auditing of security.
- Secure your Perimeter network by using a mix of traditional and other controls, e.g. firewall, VPN, zero trust controls (never trust, always validate, least privilege, device health).
- User Awareness and IT Staff Development
- Cryptography – encrypting network traffic (SSL), encrypting data at rest.
- Secure Software Development Practices – security-by-design, hardcoding secrets, not hashing passwords, simplistic access to persistence stores, unencrypted communication between system components
- Keep Up to date with CVE Publications e.g. https://www.cvedetails.com/
- Keep systems up-to-date
- Good Password & Identity management Practices & Multi-Factor Authentication, Biometrics.
- Supplier/Third Party Access Management
- Change system defaults (default passwords, autoplay for USB drives, Bluetooth discovery, etc.)

# *THE END*