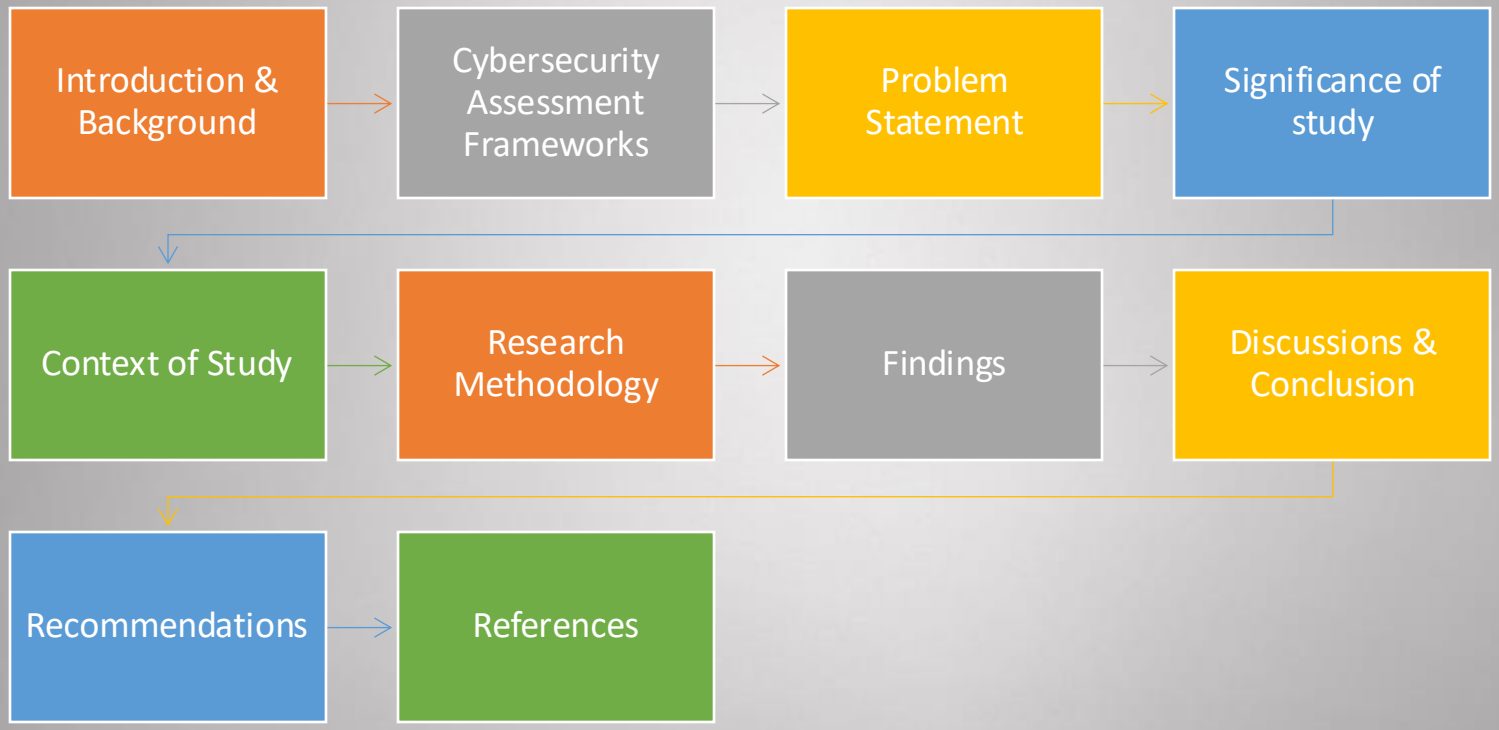
# How Government Agencies Evaluate Cybersecurity Capacity Building Outcomes: A Case of Malawi

ICEGOV 2024 PRETORIA SOUTH AFRICA

**CHIMWEMWE QUEEN MTEGHA**
**WALLACE CHIGONA**
**TEOFELUS TONATENI TUYENI**
UNIVERSITY OF CAPE TOWN

# Outline




Introduction & Background
Cybersecurity Assessment Frameworks
Problem Statement
Significance of study
Context of Study
Research Methodology
Findings
Discussions & Conclusion
Recommendations
References

# Introduction & Background

ICEGOV 2024 PRETORIA SOUTH AFRICA

The internet is a driving tool for economic and social development. It has been estimated that improving the internet penetration by 75%, it would add US$2 trillion to the gross domestic product (World Bank, 2023).

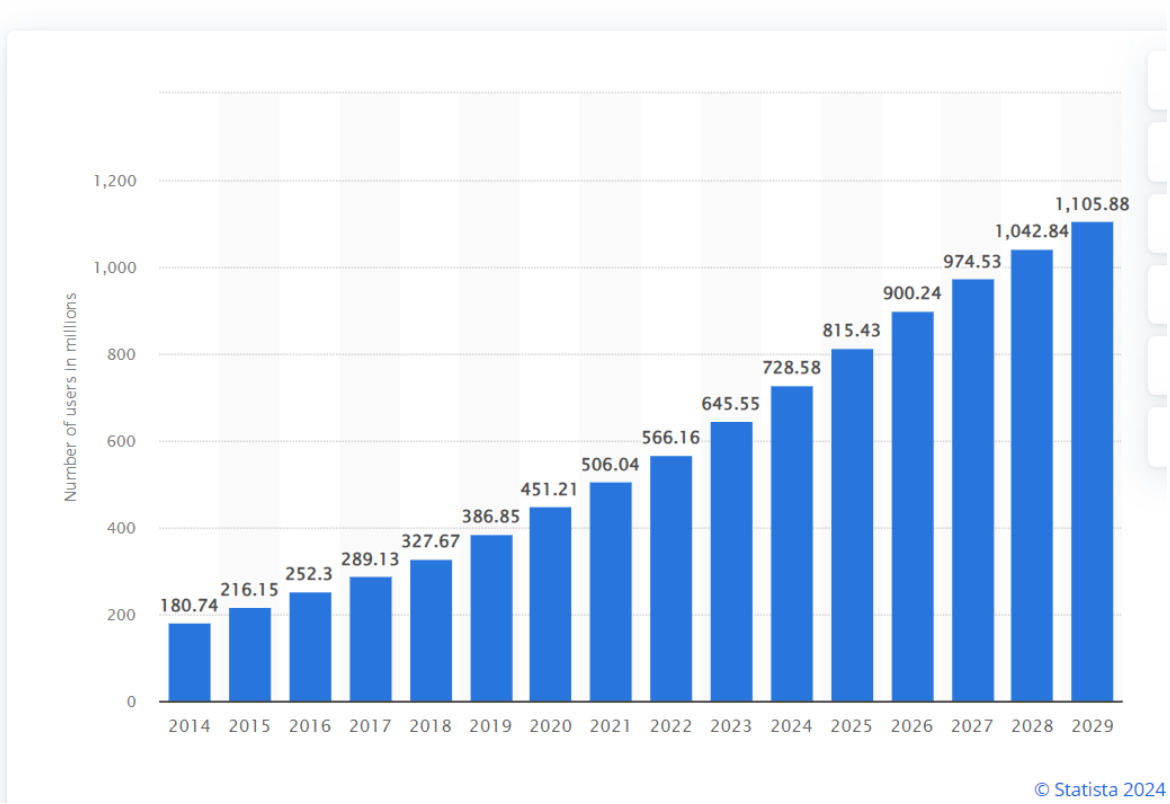
This understanding has increased developmental projects in the global south to enhance internet broadband services to bridge the digital divide of the Sustainable Development Goal (SDG) 9.c (GFCE, 2021).

With the rapid proliferation of the internet, developing countries continue to face challenges in securing digital space.

Africa alone lost US$3.5 billion to cybercrimes (C3SA, 2021).

## Number of internet users in Africa from 2014 to 2029

*(in millions)*



# Introduction & Background

ICEGOV 2024 PRETORIA SOUTH AFRICA

Capacity building has become an essential precautionary measure to enable countries to improve their cybersecurity posture.

Cybersecurity capacity building is “a way to empower individuals, communities and governments to … [reduce] digital risks, security risks, stemming from access and use of information and communication technologies”(Hohmann et al., 2017)

While cybersecurity capacity building is a product of a range of stakeholders, government agencies are a key player in this endeavour.

Government agencies are crucial in determining the cybersecurity posture of the country as they availing resources, implementing policies and regulate sectoral activities (Interpol, 2021; Kshetri, 2019).

It is therefore important to investigate the role of government agencies in evaluating cybersecurity capacity building outcomes.

# Cybersecurity Assessment Frameworks

ICEGOV 2024 PRETORIA SOUTH AFRICA

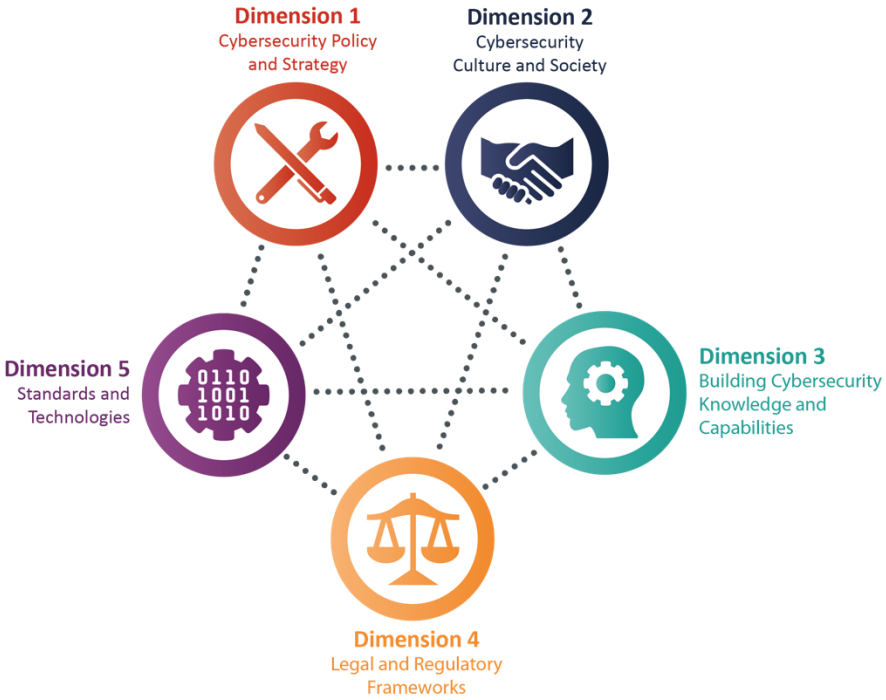
Various cybersecurity assessment frameworks are used to determine cybersecurity posture of a country.

These frameworks highlight achievements, critical gaps, and areas that need prioritisation in building national cybersecurity capacity (Garba et al., 2020; GCSCC, 2021).

Examples of assessment frameworks are the Cybersecurity Maturity Model for Nations (CMM) and the Global Cybersecurity Index (GCI).

The CMM, which was the focus of the current study, is a comprehensive analytical framework that not only identifies the gaps but also recommends actors to carry out the recommendations in building capacity (GCSCC, 2021).

# Cybersecurity Assessment Framework- CMM



# Problem Statement

ICEGOV 2024 PRETORIA SOUTH AFRICA

- CMM has been deployed in more than 70 countries. These include African countries.
- However, it is not known on the cybersecurity capacity building initiatives that are taking shape in the continent.
- Furthermore, it is also essential to understand how government agencies are evaluating cybersecurity capacity building outcomes.

***How do government agencies evaluate the outcomes of cybersecurity capacity building?***

# Significance of the study

ICEGOV 2024 PRETORIA SOUTH AFRICA

- The findings inform policymakers and developmental partners on the impact of the cybersecurity assessment frameworks and possible strategies in making the initiatives more effective in producing intended outcomes.
- Understanding the outcomes of cybersecurity capacity building will assist in informing the effectiveness of the initiatives that are being developed.

# Context of Study – Malawi



- The country located in sub-Saharan Africa, and a member of the Southern African Development Community (SADC).
- Malawi, which was the case for this study, has had two cybersecurity maturity assessments using the CMM (in 2016 and 2020) (Cybil, 2022)
- Further, the GCI highlighted that the country needed cybersecurity capacity building ((ITU, 2018, 2020)
- Therefore, there was a need to investigate how the country has been building cybersecurity capacity.

# Research Methodology

| Research Methodology | Qualitative Methodology |
|---|---|
| Epistemological Stance | Interpretivism |
| Research Contribution | Exploratory |
| Approach to Theory | Inductive |
| Sampled Government Agencies | Eight government agencies |
| Sampling Method | Purposive & Snowball |
| Data Collection | Semi-structured interviews & Desk research |
| Data Analysis | Thematic analysis |

# Research Methodology

| Government Agency | Number of Participants |
|---|---|
| Regulatory Authority | 4 |
| Ministry of Information & Digitalization | 2 |
| Ministry of Education Feature | |
| Research & Development Centre | 2 |
| Higher Learning Institutions | 15 |

The government agencies selected for the study were:

- Malawi Communications Regulatory Authority (MACRA)
- The Ministry of Information and Digitalization
- The Ministry of Education - we selected a research and development centre, and four public and one private higher learning institution in Malawi

# Findings

ICEGOV 2024 PRETORIA SOUTH AFRICA

# Summary of cybersecurity capacity-building initiatives

ICEGOV 2024 PRETORIA SOUTH AFRICA

| Government agencies | Initiatives | Target groups |
|---|---|---|
| MACRA | Training workshops, Cyberdrill, conferences, awareness raising | Law enforcement-judges, police, military, technical experts, women, children, journalists, general public |
| Ministry of Information & Digitalization | Awareness raising, training workshops | Own employees, technical experts in government |
| Higher Learning Institution | Certifications, 1 degree programme in cybersecurity, staff training, skills development | Technical experts, students, technical, lecturers, participation of students in cybersecurity competitions |

- Compared to other government agencies, MACRA conducted the most cybersecurity capacity-building initiatives.
- The reason for the skewed picture could be due to government budgetary allocation-the government agency receives more budgetary support to conduct the initiatives compared to other agencies.
- The unbalanced allocation of budgetary support could be an indication of low maturity levels of cybersecurity in the country, and ICT in the general landscape

# Evaluations of Outcomes

- The findings identified no government institutions that employed evaluation techniques custom-made for cybersecurity capacity building.

| Type of evaluation technique | Examples |
|---|---|
| Generic evaluation techniques | Auditing, tracer studies and stakeholder consultations |
| Informal evaluation techniques | Observation and/or written or verbal communication during meetings or workshops |

# Generic Evaluation Techniques



- The generic evaluation techniques were used by government agencies in their normal course of business to evaluate the capacity-building initiatives
- Such evaluation techniques included an assessment by the audit department, stakeholder consultations, as well as a tracer study by the institutions of higher learning.
- These evaluation techniques are not tailored to assess capacity building and are therefore not as effective as the agencies would like them to be.
- On the other hand, even though the government agencies had these generic evaluations within the institutions, of the eight government agencies, three used the techniques.

***"I think, within the institution, they conduct the evaluations on the programmes but it is done by another department … they deploy staff to check whether the content being taught meets the objective and criteria of the programme."*** [Participant_13]

# Informal Evaluation Techniques



- We found two informal evaluation methods used by agencies to evaluate: observations and communication (either written or verbal).
- Most institutions have challenges in developing evaluation tools that measure change.

***"It's a challenge to quantify the outcomes. … we assess based on what we see. We look at five years ago and see the improvements in terms of how people understand cybersecurity issues now."*** [Participant_1]

- The informal evaluation techniques could have been used because the government agencies felt existing evaluation tools were not sufficient or that there was a lack of skills and motivation to develop the evaluation techniques.

***"When we conduct cybersecurity awareness, we usually monitor the feedback through the engagement of people with the post on the social media platforms. As for radio and television, it is a challenge to engage with the people."*** [Participant_3]

- The current study found that, out of the eight government agencies, **four institutions** used informal evaluation techniques, and **two institutions** used neither informal nor generic assessment tools.
- The use of informal evaluations is an indication of a lack of regulation on the part of those government agencies tasked with the development of cybersecurity capacity-building initiatives.

# Discussions & Conclusion



- No government agency used tailor-made evaluation techniques for cybersecurity capacity-building.
- In comparison, the higher learning institutions conducted more evaluations than the other institutions.
- The reason for the higher propensity for evaluations in higher learning institutions could be the culture of scholarship.
- The culture of scholarships motivates educators to check the progression of their students during their studies and after graduation Taylor-Powell & Boyd, 2008).
- We expected that MACRA, being the Regulatory Authority, could have experienced external pressure to conduct evaluations of their initiatives since the institution is the custodian of the development of most of the cybersecurity capacity-building initiatives and receives most of the funding from other entities.
- We recommend future studies to explore why MACRA got around the expectations to conduct formal evaluations.
- The lack of evaluations could have also been due to a lack of appreciation of the value of evaluations of initiatives (Taylor-Powell & Boyd, 2008).
- There is a need to develop structures using the findings from the evaluations, which could motivate institutions to develop an evaluation-minded culture.

# Recommendations



- We recommend future studies to explore why MACRA got around the expectations to conduct formal evaluations.
- There is a need to develop structures using the findings from the evaluations, which could motivate institutions to develop an evaluation-minded culture.
- This could be achieved by developing mechanisms, for instance, repository hubs for the evaluation findings, so that institutions within the count
- There is a need for institutions to develop a capacity for evaluation (Cousins et al., 2004). This could be achieved by appointing or training dedicated staff in evaluations.
- Furthermore, as a motivation mechanism for government agencies to conduct assessments, institutions should develop incentives to promote evaluations.

# References


Cybil. (2022). *Portal of Cybersecurity Capacity Maturity Model (CMM) Review Reports*. https://cybilportal.org/publications/portal-of-cybersecurity-capacity-maturity-model-cmm-review-reports/

GCSCC. (2021). *Cybersecurity Capacity Maturity Model for Nations (CMM) 2021 Edition*. https://gcscc.ox.ac.uk/files/cmm2021editiondocpdf

GFCE. (2021). *Integrating Cyber Capacity into the Digital Development Agenda*. www.digitaldevelopmentpartnership.org.

Hohmann, M., Pirang, A., & Benner, T. (2017). *Advancing Cybersecurity Capacity Building Implementing a Principle-Based Approach*.

ITU. (2018). *Global Cybersecurity Index (GCI) 2018*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf

ITU. (2020). *Global Cybersecurity Index 2020*. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

mtgchi003@myuct.ac.za

ICEGOV 2024 PRETORIA SOUTH AFRICA