7th National ICT Summit Windhoek 2023

Theme: "Re-Thinking Cybersecurity investment to secure the digital economy and its opportunities"

About the Presenter

Iyaloo Ndapandula Waiganjo

- ✓IT Lecturer with 9 years of experience, specializing in cybersecurity and law at the International University of Management.
- ✓Senior Cybersecurity Consultant for 3 years at Waigaz Cybersecurity Consultancy.
- ✓Pursuing a PhD in Informatics at the Namibian University of Technology and Science, focusing on Cybersecurity Policies and Compliance.
- ✓Contacts:+264814256609/ in11waiganjo@gmail.com

Cybersecurity awareness strategy which organizations could implement to create a cybersecurity Awareness culture in the digital world

Outline:

- Introduction to Cybersecurity Investment
- Problem Statement: Cybersecurity Challenges in Namibia
- The Behavioral Aspect of Cybersecurity
- National Cybersecurity Strategy 2022-2027
- Steps for Implementing Cybersecurity Training and Awareness strategy
- Conclusion
- Call to Action
- Reference List

Introduction to Cybersecurity Investment

- The theme of this summit emphasizes the critical need for a paradigm shift in our approach to cybersecurity investment.
- In today's rapidly evolving digital landscape, securing our digital economy and its vast opportunities requires a re-thinking of our strategies and resources.

Problem Statement: Cybersecurity Challenges in Namibia

- Rapid Digitalization and System Interconnectivity
- High Internet Usage (52% internet users,) (NCS & awareness plan 2022-2027, 2023)
- In 2017, it ranked 151 out of 165 globally and in 2018 ranked 35 out of 42 in Africa for low commitment to cybersecurity awareness and controls. (Global Cybersecurity Index, 2017 ; Global Cybersecurity Index, 2018)
- Weak security practices have resulted in cyber-attacks.
- In 2020, Namibia was ranked 119 globally for cyberattacks. (Kaspersky, 2020)

Problem Statement: Cybersecurity Challenges in Namibia

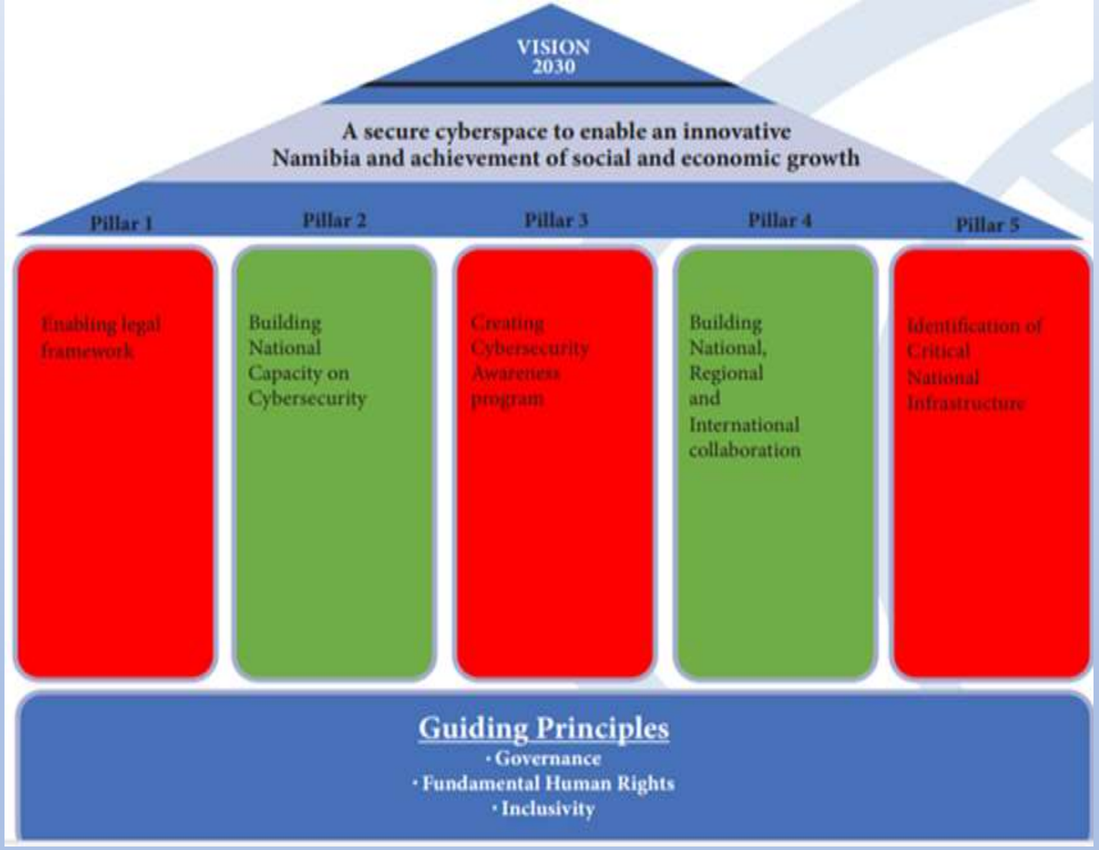
- In 2021, Namibian organizations faced 49% of cyber-attacks, averaging 1,382 per week. (Xinhua, 2021)
- Namibian banks ranked third globally for malware attacks. (Kaspersky, 2020)
- Government offices in Namibia also faced cyber-attacks.
- Cybercrimes include Social Engineering, IT outages, ransomware attacks, data breaches, and more.
- Harmful cybercrimes such as obscene materials, defamation, cyberbullying, hate speech, and privacy breaches are prevalent. (Shipena,2020)

The Behavioral Aspect of Cybersecurity

- Cybersecurity attacks often result from employee behaviors.
- When employees lack empowerment and adequate knowledge about securing the organization, it compromises its security .
- The behavioral aspect of cybersecurity is a critical component of overall security efforts.
- Empowering employees with knowledge and awareness is key to mitigating cyber threats.

National Cybersecurity Strategy & Awareness Raising Plan 2022 - 2027

“A step towards Cyber resilience & Digital Security”


VISION
2030
A secure cyberspace to enable an innovative
Namibia and achievement of social and economic growth
Pillar 1
Pillar 2
Pillar 3
Pillar 4
Pillar 5
Enabling legal framework
Building National Capacity on Cybersecurity
Creating Cybersecurity Awareness program
Building National, Regional and International collaboration
Identification of Critical National Infrastructure
Guiding Principles
• Governance
• Fundamental Human Rights
• Inclusivity

Source: (NCS & awareness plan 2022-2027, 2023)

Strategic Objectives:

1. Develop and/or review the necessary legislation, policies, and regulations

2. To have recognized and functional National Cybersecurity structures

3. Create and promote awareness among internet users and promote cyber hygiene.

4. Establish and coordinate national, sub-regional, continental, and international collaborations on cybersecurity

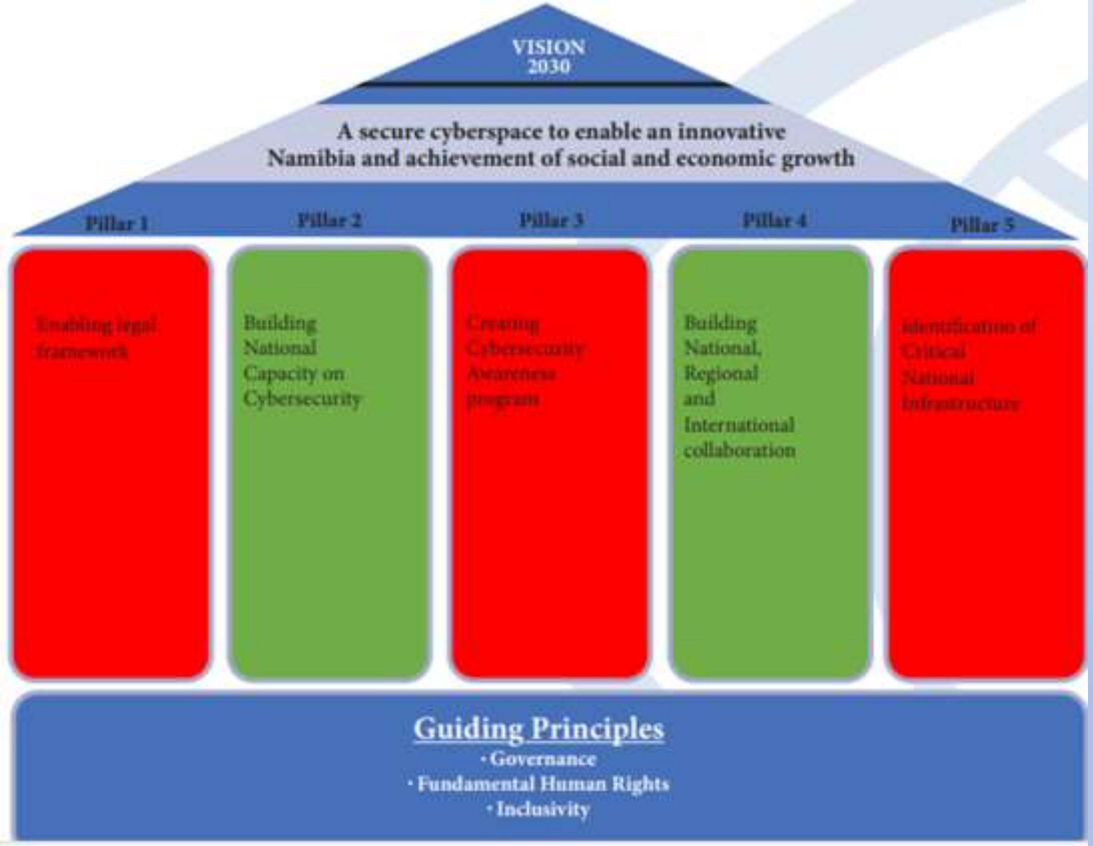
- Define cyber defense, mitigation, and incident response strategies for government and non-governmental institutions, as well as netizens;

5. Safeguard Critical National Infrastructure (CNIs) and Critical National Information Infrastructure (CNIIs)

National Cybersecurity Strategy & Awareness Raising Plan 2022 - 2027

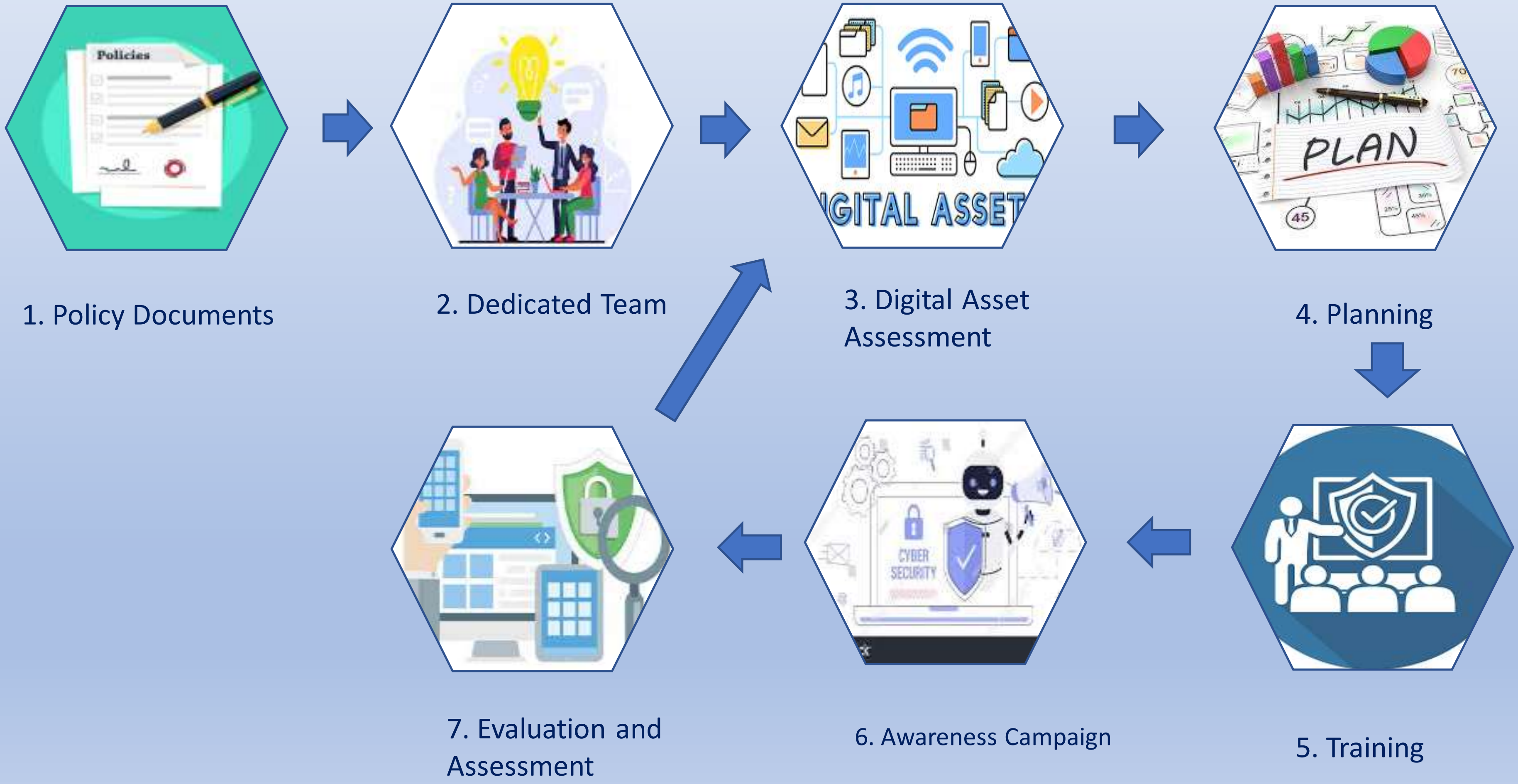
“A step towards Cyber resilience & Digital Security”

- To support the government's Strategic Objective 3: “promoting awareness and cyber hygiene among internet users” under pillar 3 as outlined in the National Cybersecurity Strategy and Awareness Creation Plan 2022-2027, every organization in Namibia should invest in the implementation of a cybersecurity awareness strategy.


VISION
2030
A secure cyberspace to enable an innovative Namibia and achievement of social and economic growth
Pillar 1
Pillar 2
Pillar 3
Pillar 4
Pillar 5
Enabling legal framework
Building National Capacity on Cybersecurity
Creating Cybersecurity Awareness program
Building National, Regional and International collaboration
Identification of Critical National Infrastructure
Guiding Principles
· Governance
· Fundamental Human Rights
· Inclusivity

Source: (NCS & awareness plan 2022-2027, 2023)

7 Steps for Implementing Cybersecurity Training and Awareness strategy



1. Policy Documents

2. Dedicated Team

3. Digital Asset Assessment

4. Planning

5. Training

6. Awareness Campaign

7. Evaluation and Assessment

Conclusion

- In closing, it is clear that cybersecurity is not merely a technological issue, but a behavioral one as well. Empowering and equipping our staff with the knowledge and tools to safeguard our organization is paramount (Zwilling et al., 2022; Goode, 2018).
- Effective awareness strategy must be designed with the intention of influencing behavioral change (Sabillon et al., 2021)
- By following the steps outlined, from establishing robust policies to conducting thorough assessments and implementing effective training, we can significantly enhance our cybersecurity posture.

Call to Action

- Namibia, like many other nations, faces challenges in building a culture of cybersecurity awareness. However, with dedicated efforts and a strategic approach, we can contribute to the realization of our government's cybersecurity objectives and ultimately safeguard the digital landscape of our nation.
- I encourage each organization to take proactive steps in implementing these strategies. Together, we can fortify our collective defense against cyber threats and ensure a secure digital future.

Reference List

- Global Cybersecurity Index 2017 Report: Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-PDF-E.pdf
- Global Cybersecurity Index 2018 Report: Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf
- Goode, J. (2018). Comparing Training Methodologies on Employee's Cybersecurity Countermeasures Awareness and Skills in Traditional vs. Socio-Technical Programs. Doctoral dissertation. Nova Southeastern University. Retrieved from NSUWorks, College of Engineering and Computing. (1045) https://nsuworks.nova.edu/gscis_etd/1045.
- Kaspersky (2020). Kaspersky Security Bulletin 2020. Statistics. Retrieved from: https://go.kaspersky.com/rs/802-IJN-240/images/KSB_statistics_2020_en.pdf
- Sabillon, R., Serra-Ruiz, J., Cavaller, V., Jeimy J. & Cano M. (2021). An Effective Cybersecurity Training Model to Support an Organizational Awareness Program: The Cybersecurity Awareness TRAining Model (CATRAM). A Case Study in Canada. Research Anthology on Artificial Intelligence Applications in Security. DOI: 10.4018/978-1-7998-7705-9.ch008
- Shipena, D. (2020). Towards a strategy for social media implications on human security in Namibia: Case study of Windhoek. [Master's thesis, University of Namibia]. URI: http://hdl.handle.net/11070/2999
- Xinhua. (2022, February). Namibian businesses more prone to cyberthreats: research firm. Retrieved From: https://english.news.cn/africa/20220224/2977c610ad814697b80861f4d6280f4f/c.html
- Zwilling, M., Klien, G., Lesjak, D., Wiechetek, L., Cetin, F & Basim, H. N. (2022). Cyber Security Awareness, Knowledge and Behavior: A Comparative Study. Journal of Computer Information Systems. 62(1). 82-97. doi:10.1080/08874417.2020.1712269

thank you