C3SA

Cybersecurity Capacity Centre for Southern Africa

THE GLOBAL CONSTELLATION ANNUAL CONFERENCE ON:

CYBERSECURITY CAPACITY BUILDING

THEME:

Linking Cybersecurity Capacity Research to Development in Africa

VENUE:

Park Inn by Radisson Hotel Newlands

02 - 03 NOVEMBER 2022

TABLE OF CONTENTS

Day 1: Keynote Speaker

Day 1: Panel Discussions

Implementing the Cybersecurity Capacity Maturity Model (CMM): Lessons learnt in African Region

GFCE Cyber Capacity Building Research Agenda - Addressing Knowledge Gaps to support Cyber Capacity Building Efforts

Applying Cyberpsychology to tackle the human factor in cybersecurity vulnerabilities

Cyber Security a National Pandemic: Who is Safe for Cyber Attacks?

Using Cyber maturity methods in practise for capacity building: the case of Botswana

African Lessons in Cyber Strategy

Challenges for engagement in international cyber policy processes for developing countries

Day 1: Research Papers

Cybersecurity Challenges and Consequences of Vehicular Ad-hoc Networks (VANETs) as an Emerging Technology in Africa

Using co-design to craft cybersecurity secure practices for rural communities in Africa: A case study from Northern Namibia

Cybersecurity in the workplace

Exploring the cybersecurity practices of the general members of the public in Cameroon

Distilling the encounters towards building a Namibian cybersecurity awareness Platform

Co-designing a Cybersecurity Citizen Centric Framework for South Africa.

Day 2: Keynote Speaker

Day 2: Panel Discussions

Building cybersecurity culture and capacity for a secured digital transformation

Sustainable approaches for cyber capacity building in practice – experiences from Mauritius

Digital Security in the Media

Interactive Discussion Round: Design and Facilitation of Cybersecurity Policy Exercises

Day 2: Research Papers

Creating a cybersecurity culture in higher education

Multiple key biometric authentication scheme for virtual workspaces

AI Cybersecurity: Ontology as Capacity Creation

Online scams and cybersecurity awareness in Nigeria: A systematic literature review

Privacy And Security Implications Of The Internet Of Everything: A Contactless Payments Perspective During The Covid-19 Pandemic– Literature Review Analysis

DAY 1: KEYNOTE SPEAKER

LUFUNO KHOROMMBI

TOPIC: CYBERLAW IN SOUTH AFRICA

Adv. Lufuno T Khorommbi is an award-winning thought leader with two decades of experience working in a multi-disciplinary Cyber Law space, delivering thought leadership in IT related matters. She holds a Master of Laws (LLM) Degree and a selection of ICT related postgrad qualifications. She is a former public servant who worked in different portfolios; from navigating the regulatory environment to supply chain and procurement to contract management; and was very instrumental in the development of various public sector ICT related policies. As a thought leader, she became the first public servant to successfully spearhead the development and implementation of the pioneered sourcing strategy for ICT procurement; and facilitate the replacement of the evergreen contracts that stifled competition.

She is a former public servant who worked in different portfolios; from navigating the regulatory environment to supply chain and procurement to contract management; and was very instrumental in the development of various public sector ICT related policies. As a thought leader, she became the first public servant to successfully spearhead the development and implementation of the pioneered sourcing strategy for ICT procurement; and facilitate the replacement of the evergreen contracts that stifled competition.

PANEL DISCUSSIONS_ DAY 1

IMPLEMENTING THE CYBERSECURITY CAPACITY MATURITY MODEL (CMM): LESSONS LEARNT IN AFRICAN REGION

Panellist:

Wallace Chigona, Professor of Information Systems, University of Cape Town
Director of the Cybersecurity Capacity Centre for Southern Africa
Daud Suleiman, Director General of Malawi Communication Regulatory Authority
Rajnish Hawabhay, Chief Technical Officer, Ministry of Information Technology, Communication and Innovation, Republic of Mauritius
Bala Fakandu. Office of the National Security Advisor, Federal Republic of Nigeria

Abstract:

The Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the Global Cyber Security Capacity Centre (GCSCC) is one of the well-renowned cybersecurity maturity assessment models. The model employs a systematic assessment of the cyber-maturity across five dimensions. The model has been deployed in 120 countries across the global and over 20 in Africa; these figures are growing. In general countries in Africa have performed poorly on the dimensions. It is, therefore, critical to engage on the experiences of the African countries in regard to the CMM. The panel discussions will unpack the implementation of these CMMs in Africa.

GFCE CYBER CAPACITY BUILDING RESEARCH AGENDA - ADDRESSING KNOWLEDGE GAPS TO SUPPORT CYBER CAPACITY BUILDING EFFORTS

Panellist:

Enrico Calandro, GFCE Research Committee – Chair, Project Lead, Cyber4Dev

Ms. Kathleen Bei (GFCE Secretariat)

Jean-Robert Hountomey (AfricaCERT)

Dr. Andrea Calderaro (GFCE Research Committee – Member) – TBC

Abstract:

Why this track is relevant for cybersecurity capacity: As existing knowledge gaps can be a significant obstacle to the design and delivery of effective cyber capacity building (CCB) projects, the GFCE developed the Global Cyber Capacity Building Research Agenda tool in 2020, with the aim of addressing such gaps in line with the GFCE's global mission of strengthening supporting cyber capacity building efforts The gaps identified are closely connected to the GFCE's thematic focus areas and the subsequent priority list of research topics is presented according to themes: Cyber Security Policy and Strategy, Cyber Incident Management and Critical Infrastructure Protection, Cybercrime and Cyber Security Culture and Skills. In addition, as the GFCE is continuously expanding its efforts to mainstream gender in cyber capacity building, the research priorities also include gender considerations as a priority area and ensure that all research undertaken considers gender perspectives in the various stages. This year's Global Constellation Annual Conference represents a perfect opportunity for the GFCE and its Research Committee to discuss and critically evaluate the progress made on the Research Agenda. The main goal of the session is to raise awareness on how the GFCE supports its community through the Research Agenda tool and how Research on capacity building can add value and increase the effectiveness of global CCB initiatives, for example by providing evidence and data.

APPLYING CYBERPSYCHOLOGY TO TACKLE THE HUMAN FACTOR IN CYBERSECURITY VULNERABILITIES

Panellist:

David Moepeng, Digital Literacy/Cybersecurity Awareness Advocate

Daria J. Kuss, Associate Professor in Psychology, Nottingham Trent University, UK

Hopeton Dunn, Professor of Communications Policy and Digital Media, University of Botswana

Basie Von Solms, Professor of Cyber Security, University of Johannesburg

Abstract:

In the digital era, the use of digital technologies is a significant part of everyday life, and increasingly influences society's socialand cultural evolution. With the use of technology impacting both positively and negatively on society, with the latter effect a result of inappropriate use, researchers are increasingly pointing out the need for user psychological and social well-being to become part of cybersecurity interventions. This is because studies have shown that people's psychological and social habits inform the way they interact with technology, and that inappropriate use of technology can also impact on the psychological and social well-being of users. It is therefore crucial that cybersecurity capacity building measures involve sociological and psychological approaches. Through research and education, universities and research institutions around the world, especially in the developed world are already driving knowledge development in this area. Courses on cyberpsychology, subdiscipline of psychology, are increasingly being introduced in universities in this part of the world. In Africa, however, this is still lacking despite the fact that the use of digital technologies on the continent is rapidly growing, which necessitates research on their effect on user psychological, social and cultural well-being. This is so as to ultimately promote and enable targeted and home-grown interventions. I, David Moepeng, a qualified cyber psychologist with an MSc in Cyberpsychology from Nottingham Trent University in the UK, and probably one of few cyber psychologists in Africa, is advocating for the integration cyberpsychology in to programmes of learning in universities. This, he intends to do through presentations to the cybersecurity and academia community on the continent on why universities should consider introducing cyberpsychology as a course or module for students taking cybersecurity, psychology, education, sociology, media studies and other social sciences.

This is so as to produce professionals knowledgeable in the effect of digital technologies on society to effectively deliver education and interventions against online harms on society. A session is therefore proposed at the Constellation Global Conference in which Cyberpsychologists discuss ways through which the discipline can be integrated in to the different courses listed above as well through research.

CYBER SECURITY A NATIONAL PANDEMIC: WHO IS SAFE FOR CYBER ATTACKS?

Panellist:

Laban Bagui, Senior Researcher & CMM Deployment Lead, C3SA, University of Cape Town

Norbert Rangarirai Jere, Associate Professor, Walter Sisulu University & PAICTA Advisor

Sonwabo Mdwaba, PAICTA President

Nobubele Angel Shozi, CSIR – Data Intensive Research Initiative of South Africa (DIRISA)

Attlee M. Gamundani, Senior Lecturer Computer Science Namibia University of Science and Technology

Tinny Mgabile, Deputy Director: Information Security Department of Corporative Governance Traditional Affairs (COGTA)

Abstract:

The increase in cyber-attacks across all sectors throughout the globe cannot be ignored. Many countries have witnessed high increases in cyber-attacks. South Africa is not spared from these attacks. South Africa holdups behind when it comes to cybersecurity and government face numerous cybersecurity challenges like lack of ICT skills and co-ordination among inter-governmental departments (Fearn, 2017). According to Sutherland (2017) the Protection of Personal Information (POPIA) Act of 2013 in South Africa guarantees data privacy but its policies are only being employed slowly and it has excessively wide exemptions for general security which take in account cybersecurity. Sutherland (2017) further indicate that South Africa lacks government cybersecurity co-ordination between national and municipal levels and with subcontracted sellers (Van Niekerk, B. (2017). More so, there is also a major challenge of raising and upholding cybersecurity culture amongst South Africans and to encourage citizens to accept good practice for cybersecurity (Patrick, 2015).

As a result, the education, retail, banks, Government departments and all citizens have become victims of cyber-attacks. This track proposal is aimed and having an open discussion led by an industry organisation the Pan African Information and Communication Technology supported by two Southern African University researchers. The track proposal aims to engage, discuss and share some experiences and learn from the participants what needs to be done to address the cyber attack pandemic.

The track proposal shall address the following questions:

- How can South African Cybersecurity experts, researchers and stakeholders work together to come up with sustainable cybersecurity solutions to rescue the country?
- What inclusive cybersecurity strategies should be in place to enable the whole nation from industry, government and all citizens in South Africa to be aware and participate in cybersecurity discussions?
- Why are we creating cybersecurity digital divide, yet attacks target all of us?

USING CYBER MATURITY METHODS IN PRACTISE FOR CAPACITY BUILDING: THE CASE OF BOTSWANA

Panellist:
Victoria White, Southern Africa Cyber Lead, British High Commission
Angela Matlapeng, CSIRT Team Leader, Botswana CSIRT (BOCRA)
Don Stikvoort, EU Cyber4Dev, Cybersecurity Expert

Abstract:
Why this track is relevant for cybersecurity capacity: The track will discuss how cyber maturity assessments such as the Security Incident Management Maturity Model (SIM3) and the UK Home Office National Cyber Risk Assessment can be used to devise national needs in terms of cyber capacity and to plan capacity-building activities in an effective and evidence-based way. By discussing the Botswana case from a donor, practitioner and recipient perspectives, panellists will elaborate on how cyber maturity models and risks assessments have been used as a way to:

a) inform cyber resilience programmes;
b) provide evidence-based recommendations for developing national cyber policy and strategies, and
c) plan training and advisory activities to strengthen the operationalisation capacity of CSIRT capacities in Botswana.
Some of the questions the panel discussion aims to answer are:

1. What do SIM3 and the cyber risk assessment measure? How can findings be used to inform national cyber strategy and policy development?
2. What are some of the limits of using such methods to inform cyber capacity-building activities? What else is needed?
3. How can we scale the successful case of Botswana to other African countries that would like to strengthen their cyber resilience?
4. How can countries start using these tools and models independently?

AFRICAN LESSONS IN CYBER STRATEGY

Panellist:

Laban Bagui, Senior Researcher & CMM Deployment Lead, C3SA, University of Cape Town
Nate D.F. Allen, Associate Professor for Africa Center for Strategic Studies / Stellenbosch University
Abdul-Hakeem Ajijola, Chair of the African Union Cyber Security Expert Group (AUCSEG)

Abstract:

The panel discussion will address the following questions:

1. What is the state of the development of Cybersecurity strategy and policy in Africa?
2. What is the state of implementation of Cybersecurity strategy and policy in Africa?
3. What are the challenges that African countries face in the development of national cybersecurity strategy and policy?
4. How can African countries successfully implement national cybersecurity strategy and policy?
5. What areas should be the focus of African NCS and policy with regards to usual social, economic and geopolitical strategic priorities?

CHALLENGES FOR ENGAGEMENT IN INTERNATIONAL CYBER POLICY PROCESSES FOR DEVELOPING COUNTRIES

Panellist:

Moliehi Makumane, Cyber Norms Senior Researcher, UNIDIR

Enrico Calandro, GFCE Research Committee – Chair, Project Lead, Cyber4Dev

Jacco-Pepijn Baljet, Netherlands Ministry of Foreign Affairs

Abstract:

African governments have been largely absent from the evolving international cyber policy processes. In many African countries, cybersecurity was never a top priority, partly because of the specific internet ecosystem of Africa and partly because there were other policy issues that were more important. This situation has translated into limited participation from African stakeholders in UN cybersecurity development processes. Limited internet access, weak institutional capacity (in terms of skills and resources) to meaningfully engage in these international processes, as well as a lack of political will at a decision-making level, are some of the factors resulting in low levels of participation of African countries in international debates on cybersecurity policy development.

However, initiatives such as the pan-African 2014 Malabo Convention on Cybercrime and Data Protection and the 2019 commitment in the African Peace and Security Council to develop a Continental Cyber Security Strategy, together with a growing number of cyber capacity initiatives, suggest a new direction. In the recent round of meetings at the OEWG level, African countries' participation has improved both in terms of quantity and quality of interventions. As more people are getting online, digital safety and security are becoming both priorities and vital elements in the continent’s development

DAY 1: RESEARCH PAPERS

CYBERSECURITY CHALLENGES AND CONSEQUENCES OF VEHICULAR AD-HOC NETWORKS (VANETS) AS AN EMERGING TECHNOLOGY IN AFRICA

Author:

Eunice Naa, Korkoi Hammond & Henry Gidudu, University of Pretoria

Abstract:

The Cybersecurity Capacity Maturity Model for Nations (CMM) developed by the GloIn recent years, we have seen technology evolve, emerge and develop in different facets and industries, and across various regions and nations of the world. This technological evolution and emergence has not excluded the African continent, as the rate at which technology continues to grow and advance, is rapid [1, 2]. Nonetheless, the continent still lags behind, facing many setbacks that affect this advancement and transformation [3]. One example of emerging technologies around the world are Vehicular Adhoc Networks (VANETs), a technological development in the transportation and vehicular space. Vehicular Ad-hoc Networks, or simply VANETs, are systems that allow vehicles to communicate with each other, with infrastructure and with other entities on the road [4, 5]. As an extension of Intelligent Transportation Systems (ITS), a high-level system designed to resolve and improve issues that surround safety and efficiency on roads [6], VANETs are purposed to improve the quality, efficiency and safety of drivers on the road, and particularly while driving [4]. As said, VANETs allow for the communication of various entities on the road which affect or enhance the quality and efficiency of driving. This communication can be grouped into two major groups: Vehicle-to-Vehicle (V2V) or Car-toCar (C2C) communication [4], which facilitate communication between vehicles and Vehicle-to-Infrastructure (V2I) or Car-to-Infrastructure (C2I) communication [7, 8], which facilitates communication between vehicles and infrastructure. Other types of VANET communication include Infrastructure-to-Infrastructure (I2I), representing communication that takes place between infrastructure, and Hybrid Communication, which combines the techniques from V2V & V2I communication [9] respectively. These communication variations all contribute to the purposed efficiency of the system.

USING CO-DESIGN TO CRAFT CYBERSECURITY SECURE PRACTICES FOR RURAL COMMUNITIES IN AFRICA: A CASE STUDY FROM NORTHERN NAMIBIA

Authors:
Gabriel Tuhafeni Nhinda, & Fungai Bhunu Shava, Lecturer Informatics, Namibia University of Science and Technology

Abstract:
With the advent of the COVID-19 pandemic, many services moved onto the internet forcing more people to become first-time internet users, especially on the African continent. This new uptake onto the internet was made possible through mobile computing devices like smartphones. However, the internet is laden with many opportunities and cyber threats. In this abstract, we present our ongoing research utilising co-design to create a cybersecurity secure practices framework for rural and underserved communities in Africa. Co-designing has been used in various areas of research, from Marketing research to Land use planning and human-computer interaction studies.

We report ongoing research in a long term community based qualitative exploratory research project in Northern Namibia, having conducted co-design sessions at 4 villages in the Engela Constituency, Ohangwena Region, Namibia. The Engela Constituency is situated along the border with Angola on the northern side and many of the villages are surrounded by Oshana, which also act as natural border betwixt them. Oshikwanyama is the lingua franca and many residents have little knowledge of English beyond pleasantries, eventhough the official language of Namibia is English. Additionally, due to the proximity with Angola, many youths tend to be more proficient in Portguese than English. We conducted our data collection in a mixture of Oshikwanyama and English.

CYBERSECURITY IN THE WORKPLACE

Authors:
William H. Dutton, Patricia Esteve-Gonzalez, Ioannis Agrafiotis, Sadie Creese, & Michael Goldsmith, TBD, University of Oxford

Abstract:
The present study is anchored in survey research and builds on the natural experiment created by the COVID-19 pandemic. We examine differences in cybersecurity issues across different workplaces, including shifts to and from working at home, the office, hybrid offices, and decentralised work centres over time. This study follows previous research on how cybersecurity has enabled working from home during the pandemic.
In June 2022 we launched a global online survey, asking respondents about their workplaces and cybersecurity issues prior to the COVID-19 pandemic, during the pandemic, and currently. The survey was fielded from mid-June to early September 2022, yielding responses to the survey from 7,330 internet users across 133 countries.

Some of the initial descriptive results show the significant shift towards work from home and hybrid workplaces and away from office and decentralized workplaces, even after the height of the pandemic. Participants perceived more security problems since before the pandemic, such as in being a victim of a scam or fraud online. And most employers have been flexible about workplace choices and have implemented the major cybersecurity measures recommended for security.
We are developing a report on this project and a set of more analytical studies exploring the factors shaping different patterns of working from various locations and their impact on cybersecurity problems. These include the kinds of work people are doing, differences across age and generations, and more.

EXPLORING THE CYBERSECURITY PRACTICES OF THE GENERAL MEMBERS OF THE PUBLIC IN CAMEROON

Author:
Laban Bagui, University of Cape Town

Abstract:
Cameroon is the largest economy in the central African region. The country has seen an important growth in mobile telephony and Internet penetration. Its pyramidal demographics suggests that about 50% of its population is between 15 and 55 years of age. The majority of that population is a user of mobile phones. They use them for business and to connect with friends and family. However, in so doing, they expose themselves to cyber threats and risks lurking online. It is not well known how members of the public in Cameroon protect themselves against these threats and risks. The aim of this study is to explore the cybersecurity practice of general members of the public in the country. This paper accounts of the pilot study conducted in the city of Douala. The study is quantitative and deductive using a combination of the Theory of practice, social cognitive theory, and the human aspects of information Security Questionnaire (HAIS-Q) to assess Cameroon general public cybersecurity practice. Descriptive statistics were used to analyse the data. Findings suggest that over 75% of white collars and educated Cameroonians are aware of cybersecurity threats and risks from personal experiences, national policies, and some awareness campaigns; however, only about 30% have a proactive mindset towards them. They don't know about cybersecurity regulations in the country, are rather conservative in their performance of cybersecurity, avoid reporting incidents, mildly trust traditional media while rather distrusting the internet and government.
Keywords: Cybersecurity practice, Cameroon, human aspects of information Security Questionnaire (HAIS-Q)

DISTILLING THE ENCOUNTERS TOWARDS BUILDING A NAMIBIAN CYBERSECURITY AWARENESS PLATFORM

Author:
Attlee M. Gamundani, Namibia University of Science and Technology

Abstract:
A multi-stakeholder approach towards creating a collaborative national cybersecurity awareness strategy across various domains in Namibia has been a fulfilling journey with a lot of key lessons to highlight. Based on the gains obtained from the journey towards realising a national cybersecurity awareness platform, some of the best practices could be extended to other countries in the region and beyond. Through running a national cybersecurity competition as one such platform, on an annual basis consistently since 2015, the Digital Forensics and Information Security Research Cluster at Namibia University of Science and Technology, successfully managed to build a growing interest from the Namibian private, public, and civil sectors providing a holistic multistakeholder approach in the process. Anchored around the provision of a sustainable open platform for cybersecurity stakeholders to collaborate and secure national assets in line with global Sustainable Development Goals (SDGs), the Namibian cybersecurity awareness platform continue to grow in stature. The same platform provides a collaborative environment that fosters learning, training, and professional growth for both cybersecurity experts and novice cyber users.
The research questions The main driving force behind the initiate of building a national cybersecurity awareness platform was guided by the main key questions thus outlined as:

- How can we create an inclusive awareness platform to sensitize industry, academia, government agencies and other stakeholders on the growing risks associated with cyber systems?
- What are some of the existing best practices around cybersecurity awareness we can borrow towards setting up a national cybersecurity awareness platform?
- What are the key suggestions and implementation solutions to mitigate the national cybersecurity risks?

CO-DESIGNING A CYBERSECURITY CITIZEN CENTRIC FRAMEWORK FOR SOUTH AFRICA

Author:
Norbert Rangarirai Jere, Walter Sisulu University

Abstract:
Grobler & Dlamini, (2012) stated that Cyber trends are a reality through the world notwithstanding of the global innovation and growth ranking of a country, all nations tend to display the same global trends, either on a more or smaller scale. Hence, in terms of phishing attacks South Africa has been categorized between developed countries as one of the greatest attacked countries in the world. Travellers are typically not aware with their surroundings and are regularly carrying their personal documents on them hence they become soft targets for cyber criminals. Moreover, mobile phones have also come to be vital for people's operations hence also becoming attractive targets in South Africa. Deepfake Technology is a technology that operates content like images, videos and voice to make it look as if as if someone is doing, or saying, something yet criminals are applying this technology to upgrade up phishing and voiceattacks, clone websites, and to bully and blackmail targets (Kshetri, 2019). On the other hand, currently the growing trends are likely to offer substantial opportunities for small and large players in the IT sector and this comprise of growth in telecommunications, data center returns and artificial intelligence as well as internet of things where start-ups are predicted to result to innovation. The business is characterized by merging and union of companies within the IT sector and between corporations in the IT and telecommunications sectors. Kritzinger, Bada & Nurse, (2017) specified that in order to advance cyber safety awareness there is a need ensure that a national cyber safety skills and capacity building plan is delivered to all role-players comprising of government employees and teachers. Besides all these efforts, there it seems as if cyber attacks continue to dominate the African. This research paper presents a critical element that could assist in having sustainable cybersecurity solutions for the country. The key research question are: • How can the citizens participate and contribute to cybersecurity awareness and preparedness? • What are the critical cybersecurity skills are required for citizens to fully participate in the cybersecurity discussions? • Who are the key stakeholders in cybersecurity within South Africa and how they engage citizens?

DAY 2: KEYNOTE SPEAKER

SADIE CREESE

TOPIC: BEYOND THE CLASSIC CMM

Sadie Creese is Professor of Cyber Security in the Department of Computer Science at the University of Oxford. She teaches operational aspects of cybersecurity including threat detection, risk assessment and security architectures. In Computer Science she teaches the second year Computer Security course, and the Advanced Security course taken both by BSc undergraduates and MSc graduate students. Sadie is currently Chair of Examiners for the MSc in Computer Science. Elsewhere in Oxford, Sadie is a member of the faculty of the Blavatnik School Executive Public Leaders Programme, where she lectures on cybersecurity topics relevant to senior leaders in public policy from around the world. She also is a regular contributor to the leadership programmes and MBA teaching of the Said Business School.

PANEL DISCUSSIONS_ DAY 2

BUILDING CYBERSECURITY CULTURE AND CAPACITY FOR A SECURED DIGITAL TRANSFORMATION

Panellist:

Adv Lufuno Khorommbi.
Gugu Sema – 4IR Senior Manager: MICTSETA / Matome Madibana – CEO: MICT SETA
Andile Stofile - Government and Corporate Affairs Lead: Microsoft
Sonwabo Mdwaba – President: Pan African Information Communication Technology Association (PAICTA)
Zoran Mitrovic – Professor Specialising in Cybersecurity – DUT and European Commission Research Executive Agency ICT expert

Abstract:

The pandemic forced organizations to shift to remote work, which propelled a rise in the adoption of new technologies. This was when digital transformation shifted from a long term aim to a reality. The increased adoption of digital transformation has changed cybersecurity as we know it. This is because cyberattacks, data breaches, and other cyber events are increasing as the threat surface grows and businesses adopt more digital technologies in various areas of their industry in pursuit of new business models and enhanced customer experiences.

Ponemon's Digital Transformation and Cyber Risk study indicates that 82% of IT security and C-level executives experienced at least one data breach when implementing new technologies and expanding the supply chain. This is increasing the impact of such cyber attacks resulting in huge costs and a considerable impact on business processes.

During lockdown, IT teams were forced to rapidly adapt to remote and hybrid work models. While the effort was challenging, the ability to adapt was a safeguard for most organizations. Unfortunately, increases in remote and hybrid work models resulted in the expansion of the threat landscape. IT teams had to act quickly to deal with an increasingly harsh reality. The sudden expansion of the corporate network, where millions of employees were logging in from their unsecured home offices, led to significant spikes in malicious cyber activity.

Global Threat Landscape Report revealed a tenfold increase in ransomware attacks alone. According to a new Fortinet-sponsored survey, it's clear that many of the challenges organizations face in combating cybercrime are directly related to a lack of qualified cybersecurity professionals.' 2 'Cybersecurity continues to be a significant threat for governments, businesses and individuals around the world. From supply chain disruptions to ransomware attacks, cybercriminals have become increasingly sophisticated and the threat landscape more diverse. These cybersecurity challenges are compounded by a workforce shortage; there simply aren't enough people with the cybersecurity skills needed to fill open jobs. Notably, this is a global problem. According to Cybersecurity Ventures, by 2025, there will be 3.5 million cybersecurity jobs open globally, representing a 350% increase over an eight-year period. In addition, 'a cybersecurity culture is more than physical barriers of entry into a building, multifactor authentication system access or least privilege authorization. It is a collective mindset of the people in the organization working every day to protect the enterprise.

A robust security culture can reduce risk and save enterprises millions of dollars by offsetting the impact of corrupted or lost data, decreased revenue, regulatory fines, and protect the enterprise's reputation. Therefore, 'the stronger your security culture is, the more likely your workforce will exhibit secure behaviors, and as a result your organization will be far more secure. This is critical in today's environment. The 2021 Verizon DBIR identified people were involved in over 85% of all breaches globally. The human element is a risk every organization needs to be actively managing, and a strong security culture creates a safe environment for that to happen.

SUSTAINABLE APPROACHES FOR CYBER CAPACITY BUILDING IN PRACTICE – EXPERIENCES FROM MAURITIUS

Panellist:
Shallen Lusinga, Senior Researcher & CMM Deployment Lead, C3SA, University of Cape Town
Hannes Krause, Cybersecurity Project Coordinator, Mauritius, Cyber4Dev
Mr Rajnish Hawabhay Chief Technology Officer, Ministry of Information Technology, Communication and Innovation, Mauritius

Abstract:
One of the most critical questions in international cyber capacity building has always been how to make programs last after the technical assistance phase is over. To help ensure sustainability, increasing resources are added to cyber capacity-building activities, creating dependency relationships between the donor and recipient communities. This raises important questions about how to sustain the level of competence achieved by trained personnel in the different countries that have benefited from building cybersecurity capacity without counting on external support.
Cyber Resilience for Development (Cyber4Dev) started building cybersecurity capacity in the Republic of Mauritius in 2018, and Mauritius became its priority country in 2019. Since then, Cyber4Dev has done a variety of activities in Mauritius. These include helping with strategy and policy, technical and operational training courses for the national CSIRT, and hands-on help with cybersecurity practice, focusing on cybersecurity exercises for both technical and strategic groups. The last highlight that the Cyber4Dev project did in the country was to host an African Cyber Resilience conference in April 2022. Representatives from 12 different African countries participated in the meeting, which was held in Mauritius.

From the beginning of our work in Mauritius, a central theme in planning activities and in our project itself has been to try to make progress that will last after our project is over. To achieve that, Cyber4Dev has categorised the beneficiary countries so that the most advanced nations (in terms of cyber maturity) get the status of a Cyber4Dev Hub. Such countries have also shown the most initiatives for different kinds of activities and, in the long term, have an opportunity to provide capacity-building activities independently to other regional countries, with or without the support of Cyber4Dev.

Mauritius has been a critical partner for Cyber4Dev, which was quite advanced in its cybersecurity posture before its work with Cyber4Dev started in the country and made a lot of progress in developing its cybersecurity at the time of the COVID restrictions. On that basis, Mauritius received the status of a Cyber4Dev Hub in April 2022, being the second of its kind globally. In its new role, Mauritius has already started to provide opportunities for capacity building to other regional countries and stands ready to increase that activity in years to come.

DIGITAL SECURITY IN THE MEDIA

Panellist:
Brenda Nglazi Zulu, Journalist, Blogger, Online safety trainer and Digital Rights Defender
Yvonne Tshepang Mooka, Journalist, BBC Africa Eye Correspondent
Susan Mwape, Executive Director, Common Cause Zambia
John Tshinseki, President, Zambian Cyber Security Initiative Foundation

Abstract:
Journalists' digital tools are computers, iPads and smartphones. Journalists use telecommunication networks and the internet to communicate with other people. These communications platforms have also made surveillance more prevalent. Without taking extra steps to protect your privacy, every broadcast, every phone call, text message, email, instant message, video and audio chat, and social media message could be vulnerable to eavesdroppers. Journalists also have smartphones which could be tracked for location and turned into tech spy tools for surveillance.

WORKSHOP

INTERACTIVE DISCUSSION ROUND: DESIGN AND FACILITATION OF CYBERSECURITY POLICY EXERCISES

Panellist:
Zainab Ruhwanya, Lecturer in Information Systems & Cybersecurity Researcher, C3SA, University of Cape Town
Lilian Georgieva-Weiche GIZ (Gesellschaft für Internationale Zusammenarbeit)
Rebecca Beigel, Project Manager "International Cybersecurity Policy" Stiftung Neue Verantwortung

Abstract:

The workshop aims to shed light on how different stakeholders use exercises for cyber capacity building by connecting practitioners who are already experienced in designing or implementing exercises while at the same time allowing space for interested participants who are new to the instrument and may want to design or facilitate exercises in the future. For them, the workshop may serve as a possible starting point for using exercises as a tool for cyber capacity building. In the past two years, the workshop facilitators (see below for contact information) have designed and facilitated country-specific cybersecurity policy exercises 3 from 2020 to 2022, among them three exercises with stakeholders from South Africa, Kenya and Rwanda. In the process, they have benefited from exchanging with other stakeholders who have been implementing exercises. In order to lower the entry barrier for the design and facilitation of exercises for others, SNV will publish its learnings in a paper called “Cybersecurity Policy Exercises in Practice” (tentative title) in October. After a brief introduction to cybersecurity policy exercises, the workshop will allow for interactive exchanges among experienced exercise implementers and newcomers to the tool.

CREATING A CYBERSECURITY CULTURE IN HIGHER EDUCATION IGITAL TRANSFORMATION

Author:
Jansen van Vuuren, Tshwane University of Technology

Abstract:
People, processes and technology are the three underlying components of any business architecture or model for an organization. These components are all important and should be treated as such. When dealing with cybersecurity, organizations have focused on technology and, as such, they have directed huge investments in trying to combat all cybersecurity challenges relating to technology. Lot of focus have been directed towards ensuring that there is proper malware and anti-viruses, access control, authentication, cryptography and ensuring end-to-end network security. According (Breda, Barbosa et al. 2017), cybersecurity is more than network security and more attention needs to go towards the non-technical component of the architecture.

There are a number of research articles that attribute this change of focus by cybercriminals to the fact that it has increasingly become difficult to directly penetrate networks across organizations owing to the amount of attention and amount IT controls that have been implemented over the years (Breda, Barbosa et al. 2017). Other researchers highlight the new working from home phenomenon (Borkovich and Skovira 2020). Borkovich and Skoria argue that allowing staff members to work from home have done three things: Firstly, it has attracted the attention of cybercriminals as many staff members are not technical and they are unlikely to put the necessary efforts required to secure their home networks . Secondly, a number of these bad guys are also working from home and, as such, they have lot of time to create malwares and phishing attacks. Lastly, working from home has increase the attack surface for cybercriminals.

The main aim of this research will be to develop a framework for creating a good cybersecurity culture for higher education. This framework will look at both the institution and the staff members and identify all key components to be activated to enable the required institutional culture to combat all social engineering attacks.

MULTIPLE KEY BIOMETRIC AUTHENTICATION SCHEME FOR VIRTUAL WORKSPACES

Author:
Tapiwa Gundu, Nelson Mandela University

Abstract:

The COVID-19 pandemic has fuelled the rapid use of personal computers, smartphones, tablets networks to complete work tasks as well as access company-owned networks, data, and applications remotely from home. This move comes with security risks this study attempts to reduce by proposing a Multiple key biometric authentication scheme for virtual workspaces, which is a key management mechanism. A security mechanism based on a single key is not enough to ensure the secure authentication needs of a home-based employee and remote work server network. In the proposed multiple key authentication scheme, the employee workstation is responsible for supporting three different types of keys. These are group key, pairwise key, and individual key. The group keys are public keys shared with all workstations in the virtual workspace. The pairwise key is used for communication with other workstations. Individual keys are used for communication with the server. This study examined the proposed virtual workspace authentication schemes on numerous attack models. The results demonstrate that multiple key biometric authentication scheme is very effective in protecting against various attacks. The analysis of results suggests that multiple keys are more secure as compared to single keys in virtual workspace authentication.

AI CYBERSECURITY: ONTOLOGY AS CAPACITY CREATION

Author:
Andrew Rens & Mark Gaffley, Research ICT Africa

Abstract:

Methodology: Our research responds to the increasing salience of AI in cybersecurity through constructing a detailed ontology of AI in cybersecurity in Africa. Research question: AI is increasingly salient in cybersecurity, in multiple roles such as threat and target (Creese, 2020). How can AI's polymorphic dynamic in cybersecurity be easily understood by policymakers in Africa? Expected Results: A visual representation of AI in multiple roles across multiple cybersecurity arenas including cyber diplomacy and cybercrime that enables policymakers to intuitively grasp the polymorphic dynamic of AI in cybersecurity, and the ensuing multi-disciplinary capacity requisites.

CYBERSECURITY MATURITY IN LOW-INCOME NATIONS - INTEGRATING CERT SERVICES IN A REGIONAL FRAMEWORK

Author:

Anthony Adams Cybersecurity researcher, Monash University

Abstract:

Cybersecurity resilience acts as a driver of economic growth (Baker, 2014) and national security (Smith and Ingram, 2017), with more than one hundred nations having enacted national cybersecurity policies or strategies (ITU, 2022). A common goal of these policies and strategies is for governments to reinforce their national interests through using cybersecurity response capabilities to protect critical infrastructure and promote local investment. Contemporary (post 2005) academic literature confirms that nations can improve their cybersecurity capability maturity and resilience by collaborating within multi-stakeholder regional frameworks on matters of shared interest while also reinforcing their respective national interests through providing a suite of complementary cybersecurity capabilities (Ferwerda et al., 2010; Dlamini et al., 2011). However, this literature has two general deficiencies that provide an opportunity to research the form and function of a low income/developing nations regional CERT framework, using the Pacific Islands region as the basis for a series of single case studies. First, while much research has been completed into cybersecurity frameworks in high income/developing regions including USA, European Union, OIC and ASEAN, comparatively little research has been conducted into the efficacy of multi-stakeholder cybersecurity resilience frameworks for low income/developing nations. Second, researchers generally address the implementation of cybersecurity frameworks from a high income/developed, rather than low income/developing nations' perspectives. The high income nations perspective assumes that foundation national institutions are established and can be leveraged to drive advantageous outcomes (Choucri et al., 2014), while low income/developing nations often lack mature institutions and may be unable to leverage similar outcomes (Sund, 2007; Baker, 2014).

ONLINE SCAMS AND CYBERSECURITY AWARENESS IN NIGERIA: A SYSTEMATIC LITERATURE REVIEW

Author:
Popyeni Kautondokwa, University of Cape Town

Abstract:

There has been a significant increase in cybersecurity threats on the African continent. Africa is one of the main targets of cybercrime and a haven for cybercriminals. Nigeria in particular, is notorious for cybercrime such as online scams, contributing to a significant number of cybercrimes worldwide. Despite the high prevalence of cybercrime in the continent, cybersecurity remains a low priority for many countries in Africa. Many countries' cybersecurity maturity level in Africa is still at the development stage. Majority of the countries in Africa lack cybersecurity legal and regulatory frameworks, cybersecurity capacity development initiatives and competence. In Nigeria, capacity development is relatively low compared to for instance, cybersecurity legal aspects. Although there has been various research on cybersecurity and cybercrime such as the impact of cybercrime on financial institutions, challenges of cybercrime, socio-technical perspectives in Nigeria, few have focused on online scams and cybersecurity awareness in Nigeria. This study will use a systematic literature review to understand the impact of online scams on cybersecurity awareness in Nigeria. The study seeks to answer the following primary question: How does high prevalence of cybercrime originating from Nigeria impact its cybersecurity awareness?

PRIVACY AND SECURITY IMPLICATIONS OF THE INTERNET OF EVERYTHING: A CONTACTLESS PAYMENTS PERSPECTIVE DURING THE COVID-19 PANDEMIC– LITERATURE REVIEW ANALYSIS

Author:
Nomusa Nomhle Dlamini, University of Cape Town

Abstract:

Background to the study: The Internet of Things (IoT) has gained popularity within many businesses and among individuals over the years. This has opened a world where everything is connected moving from just IoT to the Internet of Everything (IoE) which encompasses the opportunities and new everyday opportunities from personal smart technologies to making our cities and world smarter.

However, as much as interconnectedness is the core and foundational strength of IoE, it also opens a world where the question of security and privacy rises as the technology advances. The challenges emanate from the extension of the internet to encompass IoT as the realm of IoT interconnects heterogeneous devices which create new security challenges as more devices connect. This is more because the connecting devices have their own existing security challenges even before they start connecting with other devices.

Users are said to continue to use technology if they perceive that it offers benefits which are beneficial in their daily lives and “cannot live” without. With this belief users are caught in the entanglement described by Oberländer, et al., (2018), this emanates from socio-economic conditions, sociodemographic conditions as well as culture – we continue to use technology because of influences of these factors. Undeniably, the COVID – 19 pandemic is worth noting as it has altered the way people engage with technology and socially. The pandemic has enabled further technological advancements within many businesses which has in turn accelerated the digitisation of payments leading to the wide use of contactless payment (Renu, 2021). This is a result of the need for social distancing and reducing contact (Zhao & Bacao, 2021). Zhao and Bacao (2021) argued that contactless payment in the face of the COVID-19 pandemic gives users physical and mental sense that they are protected from contact with surfaces that might spread the COVID virus. However, users are still uncomfortable with contactless payments because of privacy and security issues when compared to cash or PIN payments. Security and trust remain the main barriers to adoption of these payments (Karjaluoto, Shaikh, Leppäniemi, & Luomala, 2019). It has been seen that exploitable weakness in contactless payments can come from unencrypted NFC readers that request the data from the payment systems like the card number, cardholder name, expiry date, issue date, etc. (Emms, 2011).

THANK YOU FOR JOINING!