1st AfICTA Quarterly Webinar: "Insider Risks: Secure Digital Identity & Solving the Challenges of Modern Remote Access in the Post COVID-19 World"

Webinar Report

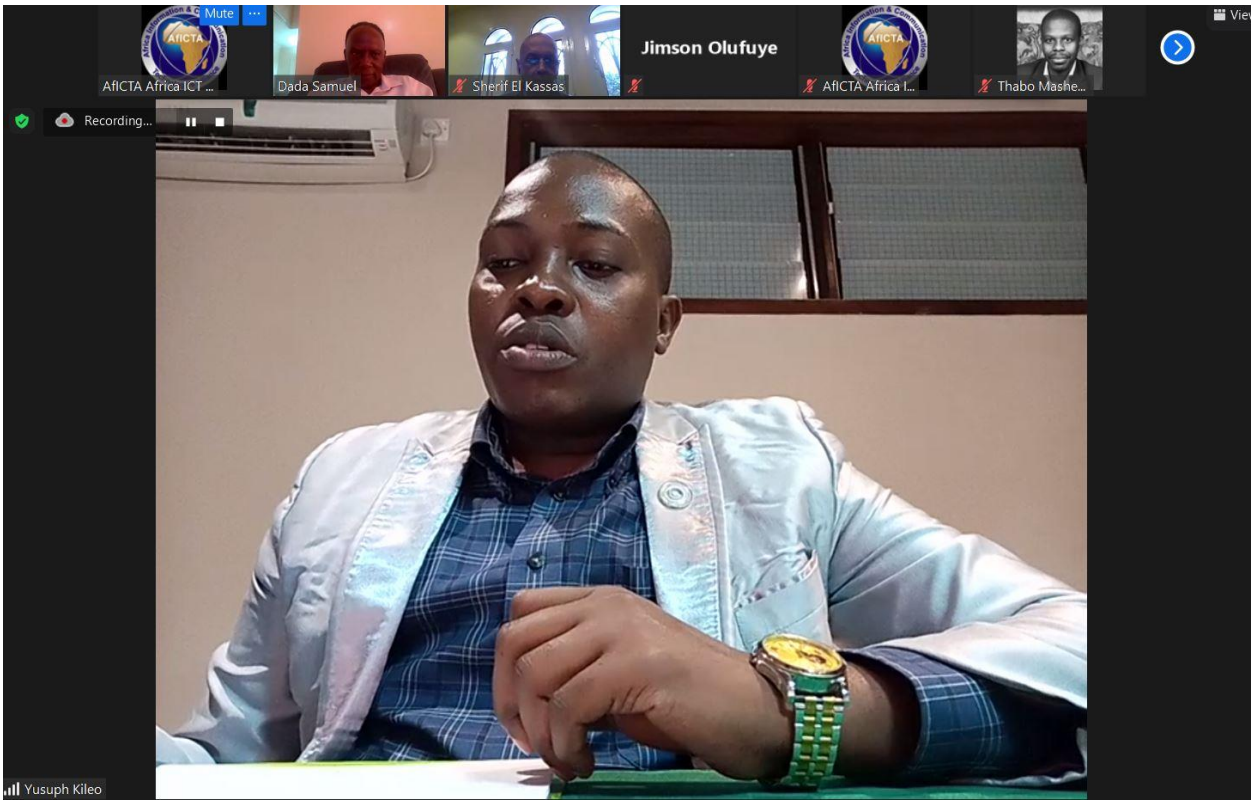
Introduction:

On 18 March July 2021, AfICTA in collaboration with Computer Society Kenya organized the 1st edition of its Quarterly webinar series on "**Insider Risks: Secure Digital Identity & Solving the Challenges of Modern Remote Access in the Post COVID-19**"

It provided a platform for professionals from across Africa to share knowledge on ways to protect and secure our digital identity.

The webinar was very successful boasting of 4 panellists and participants from all over Africa online who enriched the collective dialogue.

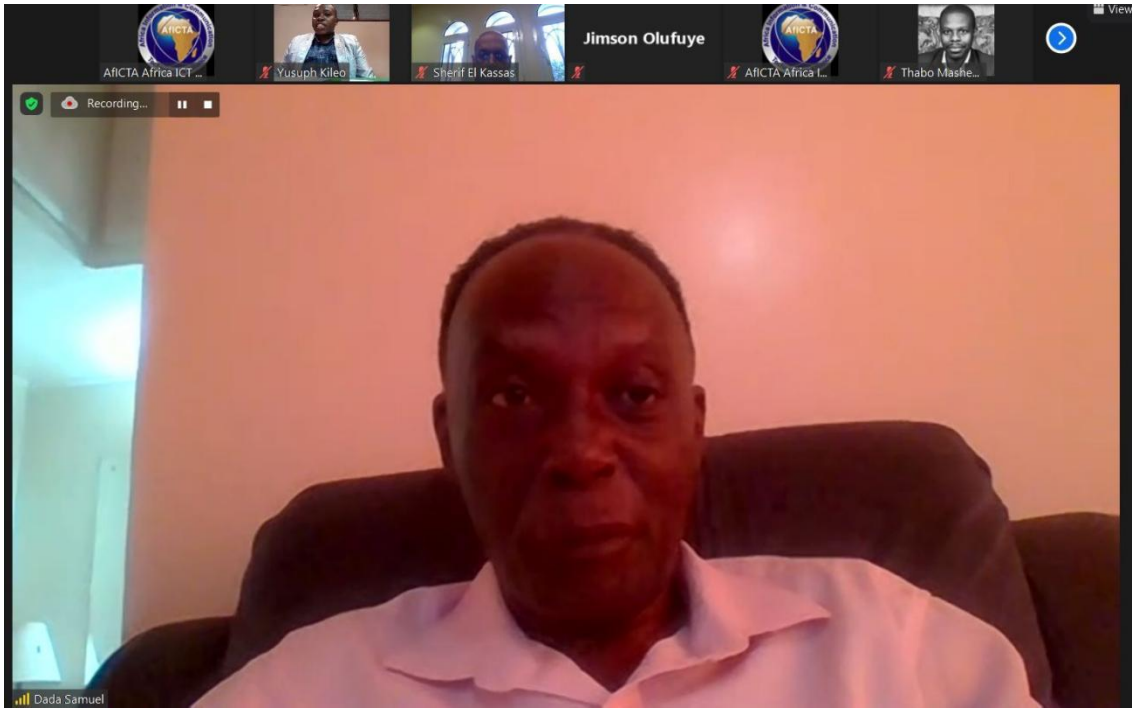
Mr Yusuph Kileo, Cybersecurity expert and board member at AfICTA was the lead facilitator of the webinar. He welcomed all participants to the session and thanked everyone for taking the time to partake in the webinar. He also announced all the speakers on the call before introducing the Vice-Chairman East Africa Region, AfICTA and host of the webinar to give an opening remark.



Mr Kileo said that it would be advisable that we be more prudent with the information we share about ourselves on social media platforms or other online tools we make use of as they generally could become ammunition for cyber attackers to infringe on our privacy and put us at risk. Mr Kileo also highlighted one of the overlooked practices in our organizations that may create the perfect conditions for insider threats which is the Bring Your Own Devices (BYOD) policy, he suggested that we would have to create security and authentication policies to validate these devices for access to critical organization information and prevent compromises that could be detrimental the organization.

Opening Remarks:

Dr Waudo Siganga, VC EA host & President of CSK opened the session by offering his condolences to the Tanzanian people over the loss of their beloved president, **John Pombe Magufuli** before welcoming all the participants and panelists who have taken the time out to join the session as it would be a very informative one considering that we are still in recovery over the pandemic.



Part 1: Presentations by Speakers

Cybersecurity, Trust, and the connected world

Prof Sheriff El-kassas, Professor from the American University Cairo delivered a presentation on Cybersecurity, Trust and the Connected World. He opened by sending condolences to the people of Tanzania empathizing with them over the loss of their leader in these trying times.

Dr Sheriff began by providing insight on some of the massive data breaches that have occurred over research done in recent years. The key takeaway from this research clearly points out that supply chain attacks are the prevalent forms of cyber threats currently. This begs the question of trust and dependability in the cyberspace ecosystem. Perhaps it's noteworthy to highlight that cyber attacks are not a purely technical issue but more socio-technical in the sense that cyber-attacks are not always caused by breaches in the technical systems and infrastructure but could also be as a result of misplaced trust by

end-users. Prof Sherif refers to the Saltzer & Schroeder Designs Principle emphasizing that a critical look at the principles of this design proves that most of the principles are not purely technical and the best way to increase the efficiency of this principle is through constant oversight and scrutiny.

The issues of trust between end-user and service providers can be a very complex issue when security motives are completely diametrical nonetheless, the best answer here lies in constant oversight, regulation and effective liabilities exemplary in the work done on privacy protection carried out by the EU with the GDPR.

In conclusion, Cyber Security is a socio-technical and physical problem and we would need to tackle it through robust risk and trust management, we would also need reliable regulations that prioritize the protection of end-user data. Finally, we would need more comprehensive Research and development programs that aims at developing more reliable systems. Read More

Part 2: Panel Session on Insider Threats

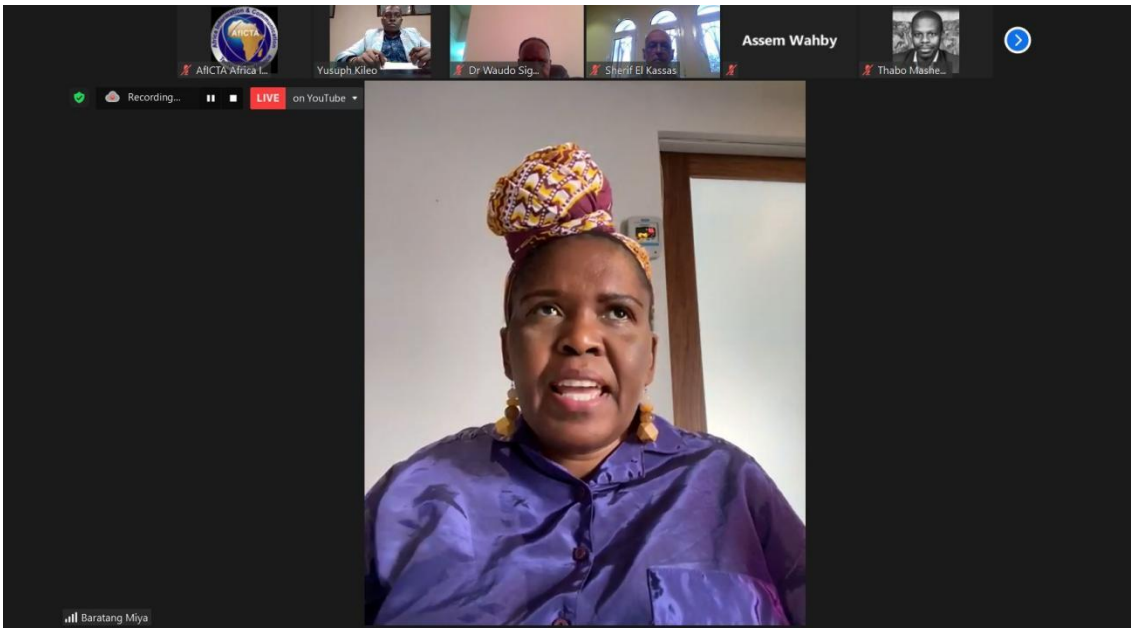
1. Risks in today's Remote workforce

Prof Sheriff El-kassas was asked the question: what are the risks in today's remote workforce to which he responded:

Traditionally, an organization builds its system defence mechanism around zonal compartments based on the level of information in question, but with the explosion of the remote workforce due to COVID, we have seen a situation where information zones are no longer in compartments but are rather in a mesh connection through the number of devices holding and accessing critical information. This creates the necessity for the Zero trust architecture that tries to build trust based on each interaction of devices, this

means that within each interaction between entities there is no room for assumption on security risks and eligibility so we ensure there is complete scrutiny and authentication requires for sensitive information to be shared on any interaction level. It is impossible to ignore the cost factor associated with this architecture but we have to begin to look at the issues of trust from not just the point of view of protection of assist but as a matter of security as well.

2. Securing Digital Identity

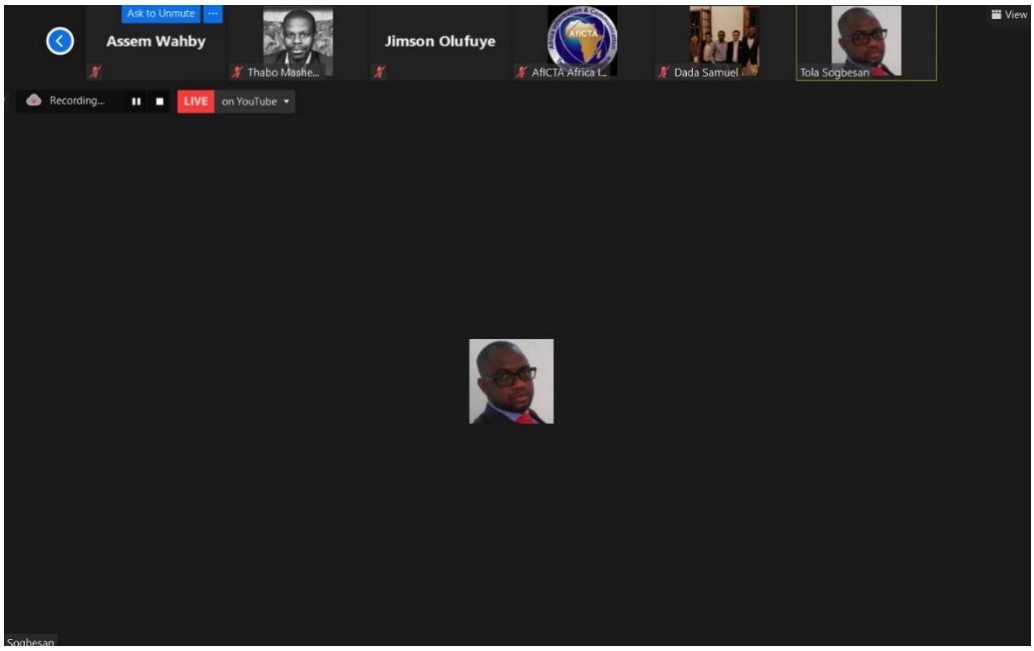


Individually we should be responsible for determining who we entrust with our digital data online but from an infrastructural standpoint, it becomes very hard to carry out accountability assessments on devices/systems used to process our data because most of these devices are made externally. We must begin to invest and employ homegrown solutions so that we can reduce the biases that come with external manufactures of these solutions. Although the onus of securing digital identity lies majorly on the manufacturers of the devices and the proper regulators that make the standards for best practices among the vendors. It's also important that we carry out end-user awareness schemes to get people informed on the ways to be more digitally safe and cyber vigilant. Cyber education in schools needs to be a prerequisite as most of the adopters of these new technologies are the youth and its necessary that they are more knowledgeable on ways to ensure their digital identity are managed properly and are safe.

3. Readiness for future Shutdown Contingencies.

Mr Tola Sogbesan, CEO of Axiom Consulting stated that our preparedness for any future shutdown contingencies should anchor on the Zero Trust Network access architecture. In other words, to increase the readiness index for any shutdown that results in digital/remote operations, we need to know what kind of devices would be used for digital access, we need to know the security standard for access online, we need to know the types of data requested from any vendor or company. It’s important for end-users

to minimize the amount of information they provide online and who gets consent to their data, it's also important that we raise awareness on risk assessment for any digital interaction we carry out online.



4. Policy considerations for Cybersecurity in the Post COVID era

Prof Sheriff when asked what policies should be considered in the aftermath of the COVID-19 pandemic, he stated that there is no one-size-fits-all policy to combat cybersecurity threats, so the more feasible approach would be to develop policy strategies that are tailored specifically to industries that make use and manage people's data online be it the medical industry, the financial industry, government and private sector. It's also noteworthy to mention that we need to migrate from the current identity management system of providing all our identity and data to a single entity relying on single systems that can be easily breached, we need to make a shift to self-sovereign identity practices where users have controls over which aspects of their data and identity is being accessed by who. To implement this structure, we would need to have set down a framework and regulations that engender this architecture and are acceptable to vendors.

Conclusion:

Although there is no guarantee of total security online, we need to strive as much as possible to ensure we are more aware and cyber conscious. The current landscape of cybersecurity proves that we can't rely solely on just passwords to secure our identities online so we should employ multi-factor authentication techniques in all layers of access to crucial and important data online. Cybersecurity policies such as the GDPR and other privacy laws help to maintain some form of privacy for individual digital identity but the major challenge facing such law is the enforcing of them. African countries need to work together to ensure cross-border collaboration and jurisdictional persecution of bad actors. Finally, the problems of enforcing prosecution on culprits would require access to the WHOIS database so its easier to carry out an investigation.

Closing Remarks:

Mr Thabo Mashegoane, Chairman AfICTA and President IITPSA, thanked everyone on the webinar, and commended the organizing team for conveying the very rich discussions, and commended the insights into ways to secure our Digital Identity, he appreciated the recommendations for more awareness on cybersecurity and the need for more scrutiny and risk analysis. On a final note, he suggests that in Africa, as we rapidly adopt digitalization, it would be prudent that we take Cyber awareness and security more seriously than we do in the more customary physical structure.

This report is a summary of events at the AfICTA 1st Quarterly webinar. You can explore more on www.aficta.africa

The digital recording of this event can be accessed here.