SEPTEMBER 2021

AFICTA THIRD QUARTERLY WEBINAR REPORT

Prepared by: AfICTA Secretariat
03rd October 2021

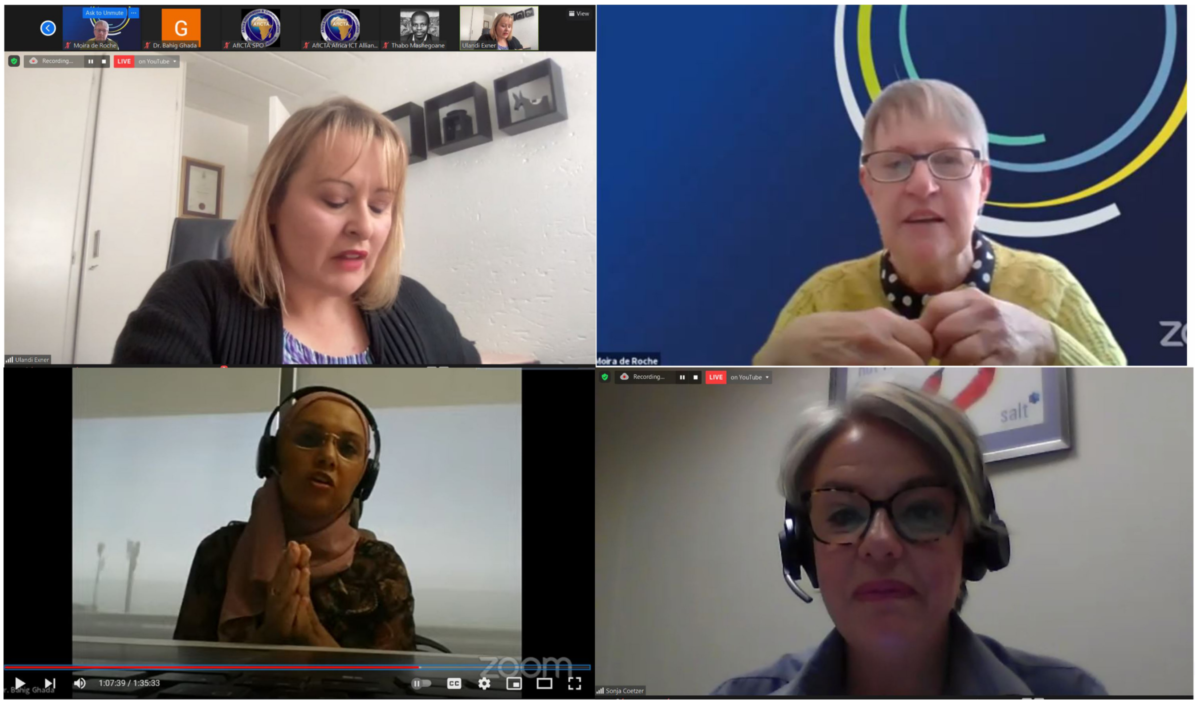
"Data Is the New Oil: The Good, The Bad & The Ugly"

On 29 September 2021, AfICTA in collaboration with the Institute of IT Professional South Africa - IITPSA organized the 3rd edition of its Quarterly webinar series on **"Data is The New Oil: The Good, The Bad & The Ugly"**

It provided a platform for professionals from across Africa to share knowledge on the data regulation policies deployed in African regions and whose duty it is to properly regulate the security of our personal data.

The webinar was a very successful one with panellists and participants from all over Africa online who enriched the collective discourse. Among the highly esteemed panelists were: **Moira de Roche**, Vice-President, IFIP IP3 and Director IITPSA; **Dr. Ghada Bahig**, Engineering Manager, Mentor A Siemens; **Sonja Coetzer**, Managing Director, SALT Essential IT.

Ms Ulandi Exner, Vice-Chairman, Southern Africa AfICTA was the lead facilitator of the webinar. She welcomed all participants to the session and thanked everyone for taking the time to participate in th webinar highlighting that the purpose of the webinar is for knowledge sharing gon mechanism for ensuring data privacy from th perspectives of different regions in the continent. She then welcomed Mr Thabo Madhegoane, Chairman, AfICTA for his opening remarks.



Opening Remarks

Mr Thabo Mashegoane, opened by thanking the panellists for their time and expertise, welcomed the participants and proceeded to buttress the importance of the theme of the webinar which is very imperative as digitalization rapidly increases and the cornerstone for this change is data.

In the aftermath of the proliferation of the use of the Internet across the continent and the globe, we have seen that there is a lot more exploitation of the data available online and the engagement today is organized to raise awareness for better regulation to protect user's information and data online and the speakers would proffer recommendations on best practices that can be replicated across the continent.

He further highlighted that AfICTA as an advocacy group strives to promote the practice of multistakeholderism in all engagement in the ICT ecosystem in the continent hence the reason that people from all stakeholder groups have been invited to benefit from the discourse. He then introduced the moderator for the panel session, Ms Ulandi Exner.

Ms Ulandi introduced all speakers for brief presentations.

Data Security/Privacy in Manufacturing

Dr Ghada Bahig a Research and Technology Director at Siemens delivered a presentation on Data Security/Privacy and its impact in the Manufacturing sector. She began by explaining data privacy and security in a nutshell before giving insights into its implication in the manufacturing sector. Dr Ghada opened by highlighting the difference between data security and data privacy, she explains that data security restricting unauthorized access by third parties to data stored while data privacy connotes the regulation and mechanism in place to properly handle, collate, process, store and use data that doesn't breach any confidentiality or rights as stipulated.

There are 3 pillars of Information security otherwise referred to as the triad which is **Confidentiality, Integrity and Availability**. Confidentiality deals with who accesses the data, Integrity deals with the maintenance of consistencey and accuracy of the data over its lifecycle while availability deals with the readiness to which data can be accessed.

From an organization's perspective, the building blocks for data security is: data encryption, access control, activity monitoring, breach response etc, while data privacy blocks are the discovery and classification of data, data removal mechanisms, 3rd-party management, consent contracts, and policies for regulation.

In the recent past, data networks on manufacturing sites were separated into IT networks which typical controls the data connection over the internet and the operational technology networks that govern the on-site physical data generated and stored physically which are usually air-gapped but the new architecture implemented across the board has seen a shift where both network structures are being merged and what that entails is that there need to be more stringent and meticulous efforts to ensure data security and privacy to prevent downtime in the event of a cyberattack.

According to a Gartner study carried out in 2019, the number one hindrance to industry adoption of AI and industry 4 technologies if the security and privacy concerns hence emphasizing the need for better policies and data security measures implemented in all sectors as we are becoming more digitalized and in conclusion, she stated that "Cybersecurity and data protection is everyone's responsibility and should not be limited to boardrooms". Read More

Data and Trust - The Duty of Care

Moira de Roche the Vice President of IFIP presented on the Data and Trust.

The correlation between trust and data privacy can not be overstated as bad actors tirelessly work to obtain and use peoples data for good, bad and ugly. The bedrock of trust when handling people's data is consent and we must begin to implement consent laws that govern when and how people use and collect data. Trust also encompasses the reliability and integrity of the data collated and to trust anyone or organization collect then there must be set standards that determine how much trust can be afforded to anyone collecting people's data.

Trust is an overarching theme that deals with a few entities namely: Security, privacy, Usability Safety, Reliability Accessibility and a breach in any of these entities will diminish trust thereby dissuading people from using systems/technologies and may also cause financial loss from the perspectives of organizations involved.

The duty of care and its responsibilities is not limited to the systems and technologies in our organizations but we are the last line of defence and we must ensure that so long as we use digital products, then we must ensure we are safe with what, whom we give information to.

Trust is a major issue because trust breeds confidence and if confidence in technologies and products is minimal then it hampers economic growth which in many cases is a function of digital growth. Trust is a multi-disciplinary concept that deals with usability, reliability, security, privacy and safety and data security and privacy are 21st-century soft skills that everyone must have. One of the major challenges of trust is that consumers are unable to evaluate the security of service providers but the questions that need to be asked are: is security built-in at every level of manufacturing of the digital devices and technologies being deployed? In conclusion, she stated that "Trust is a very expensive commodity, it takes years to earn but only seconds to lose it". Read More

Data Security and Privacy... Whose Responsibility is it?

Sonja Coetzer, MD SALT Essential IT gave a presentation on Whose Responsibility is Data Security and Privacy. There is a popular misconception that cybersecurity isn't our responsibility until it hits our doorstep and according to a survey done in 2021. it's estimated that the world would lose 1.5trillion dollars annually to cybercrime and this projection begs the question of whose responsibility cybersecurity data protection is?

The question is are we willing to take the responsibility and ownership of caring about our data protection. Data protection is often bypassed for productivity and efficiency and this practice will prove to be more expensive in th long run. Data privacy laws need to be implemented drastically to ensure that data protection becomes a priority in all organizations.

In an ISACA publication assessing the state of cybersecurity in 2021 and preparing for 2022, Dustin brewer highlights that cybercriminals are working relentlessly to cause business disruption and outage and the same report highlights that the top 5 forms of cyber threats in 2021 are social engineering 14%, advance persistent threats 10%, Ransomware 9%, Unpatched systems 8% DDoS attacks 8%.

Typically the onus of data protection and security is left to trusted technology advisers, experts, service providers and the belief that ICT infrastructure and security of data belongs to the IT department is still held in high regard but truth be told, as cash flow is to bank balances, so is data and the related technology turning data into actionable insights, accelerating innovation and creative technologies to the business.

Since the turn of the century businesses have profit before safety and security same way we have put using data to drive business results before securing data when it is common knowledge that data has now become the most valuable asset both for the business and for cybercriminals.

Data security is more crucial now as it is the heart of any business strategy and as most business functions it should be empowered by the budgetary demands that help accelerate and drive business growth. Global trends suggest that as much as 60% should be put towards a planned, designed, refined and secured ICT environment while empowering the employees, partners and other stakeholders in order to attain business goals and objectives.

In conclusion, until the C-Suite fully understand that data is no longer an enabling tool of the business but rather at the heart of the business then they can begin to treat data privacy and security seriously giving more attention and capital investment in raising awareness among employees on the necessity to be very data security conscious.

What is the approach to securing data in African regions?

South Africa enacted the Protection of Personal Information Act (POPI Act) - POPIA in 2013 and although the policy serves as a guideline to how data and information should be regulated and collected, Moira believes that most people do not really understand the reasoning behind those policies and so more training has to be done to get people more acclimated with the policy on data protection.

Dr Ghada highlights that most countries are now evolving towards creating a data protection law and Egypt in 2020 enacted its data protection law that establishes standards and controls governing the process of handling personal data. It provides the law that grants the binding rights of users to guarantee the protection of personal data and information ranging from rights of consent to rights of what data is collected and by whom. Regulatory bodies are evolving in the right direction towards data privacy in the continent but more needs to be done in other countries as data is proven to be a tool of warfare nowadays.

Sonja Coetzer pointed out that Namibia currently doesn't have a data protection policy and at the beginning of the year there was a multistakeholder forum that sought to begin laying the foundations for a new data protection policy but the electronica bill currently in place is the substitute being used in Namibia now.

Although there are groundwork and isolated data protection laws by CRAN, Bank of Namibia but Namibia is taking insight from the GDPR and POPI Act (Namibia being a child of South Africa) to enact its own. Sonja also suggests that the strive for perfection hinders productivity and so the legislators must ensure they have legislation laid out and work towards perfecting it in the future rather than slow-walk the process trying to achieve perfection.

Ms Ulandi suggested that often than not compliance has become a tick-a-box process and implementation is not fully enforced in totality so we must ensure we hold our regulatory bodies accountable for enforcing legislation.

Data Security in Medicine

Confidentiality is prioritised over security in the medical-practitioning fraternity and it would be prudent that the same level of severity that is attached to breaches in data confidentiality in the medical field be focused on enforcing the data security and protection Act within the medical sector. Sonja held a different perspective that although we try to ensure data privacy and security in the medical field we must ensure we tread the path carefully to prevent overregulation that may hamper the delivery of medical care as this would be disastrous especially in the African regions where urbanization hasn't fully materialized. Instead, we must ensure there sare security measure that aims at the protection of data of technology used to provide care to citizens.

Responsibility of Users in Data Security

Consumers of digital services and technologies have a responsibility to ensure that they apply the same rules of security when it comes to physical entities and universal interactions daily to our engagements online. Online Security cannot be achieved by complete detachment from the virtual world but we must ensure we understand and use the same principles of security taught at homes to the virtual world online. Awareness can not be overemphasized when we are dealing with cybersecurity. As stated earlier, social engineering is the most prevalent cyber threat recorded across the globe and in other to ensure that humans beings are less of the weak links as cybersecurity experts conclude, then we must ensure that awareness on safety online has to be taught and re-thaught at all levels of education.

Impact of COV-19 on data Protection?

Sonja suggested that the COVID-19 crisis which caused the shutdown of physical interaction both socially and in the cooperate sector proved that we as a society and as a continent are not ready for a more digital paradigm and we must not wait for another pandemic/crisis before we begin to set up more proactive measures to mitigate the adverse effect of cyberthreats as we move towards complete digitalization. So although COVID ramped up digitalization it showed the faults and cracks in the cybersecurity and data protection structures and in other for us to move ahead of the curve then we must begin to include data security and protection concerns at board room levels.

Q & A Session

1 What role do you think the AU Cybersecurity and Data Protection Convention can play in safeguarding African data in Industry 4.0?

Sonja Coetzer responded that the AU Cybersecurity and Data protection Convention can play is to help smaller countries within the continent that struggle with data protection legislation by providing a strong baseline off which the regulatory bodies can work to help push their efforts faster. Dr Ghada also responds that the AU like the EU could set up initiatives that push Orgazninzations mostly in the private sectors as they are the front runners of the Industry 4 technologies to come together to enhance the efforts and objectives and concerns of data protection and privacy so that the regulatory bodies can then be brought on board to prepare legislation that suits these concerns.

2 Has IP whitelisting and blacklisting been effective in stemming attack vectors in your organisations?

Sonja Coetzer and Dr Bahig agree that whitelisting and blacklisting IP addresses are to some extent effective but like any other security protocols in real life, the must be several other measures that are being deployed to ensure security within our organization. we must take a deeper look into what whitelisted addresses access regularly and also ensure we are updating the security breacher that bad actors circumvent to connect via IP addresses that are blacklisted by the organizations.

Conclusion

Data privacy and protection has to be elevated on the priority chain in all our organizations and we must also hold forums where all stakeholders are brought together to ensure accountability to regulations on data protection within our countries. Cybersecurity should not be limited to the boardrooms at the organization but we as consumers and users of technologies must ensure we are less susceptible to risks online use to prevent us from being weak links.

Closing Remarks

Mr Thabo Mashegoane, Chairman AfICTA, thanked everyone on the webinar, and commended the organizing team for conveying the very rich discussions, and commended the insights into the necessities for better data privacy and protection regulations and accountability when it comes to enforcing the regulations. On a final note, the Chairman welcomed all the panellists to the 4th Quarterly webinar slated for **November 30th 2021** and the theme for the webinar is ***"Assistive technologies: Towards African Intercontinental orchestrated efforts"***

You can view recording here: https://youtu.be/Fd6Gax8sdYo