MINISTRY
COMMUNICATIONS AND DIGITAL TECHNOLOGIES
REPUBLIC OF SOUTH AFRICA

SPEECH BY MR PHILLY MAPULANE MP, DEPUTY MINISTER OF COMMUNICATIONS AND DIGITAL TECHNOLOGIES AT THE 2023 GOVTECH CONFERENCE, DURBAN ICC, KWAZULU-NATAL, 13 SEPTEMBER 2023

Conference theme: ***Platform Economy for Digital Transformation and Inclusive Growth***

Topic: ***Robust Cybersecurity - a Must for Effective Digital Transformation***

Thank you, Programme Director

The Director-General

Chairpersons and CEOs of SOCs present here today

Esteemed guests

Ladies and gentlemen;

Good morning!

INTRODUCTION

It is my absolute pleasure to be part GovTech 2023. As I said last night at the Gala dinner, this year's GOVTECH is the most well organised of the ones I attended. It is my singular honour to be afforded the opportunity to address you on this important topic of *Cybersecurity in effective Digital Transformation for Inclusive Growth*.

It has been a refreshing and fulfilling experience engaging and interacting with movers and shakers in the ICT sector in this year's conference convened under the theme, "*Platform Economy for Digital Transformation and Inclusive Growth.*"

Ensuring a thriving digital and transformed technological sector is critical to the future of the South African economy. It is critical to growth, to job creation and to raising the productivity of all South Africans, whether it be for citizens in rural or urban communities or SMME's with good products and aspirations for development.

DIGITAL TRANSFORMATION

As we are aware, digital technologies are rapidly changing the world as we know it. Digital transformation is therefore not just a trend, but an imperative for survival, for growth and for innovation.

And so if we are to truly embrace digital transformation, we need to sufficiently interrogate and understand this phenomenon and some of its key drivers, which among others include the following:

1. *Consumer Expectations:* The modern consumer is connected, informed, and always on the move. They demand instant access, personalized experiences, and seamless interactions. Organizations that fail to adapt to this new consumer paradigm risk obsolescence.

2. *Operational Efficiency:* Beyond consumer interaction, digital transformation streamlines operations. Automated processes, data analytics, and integrated systems lead to reduced costs, minimized errors, and faster response times. A digital-first approach allows companies to do more with less, achieving higher productivity levels.

3. *Unlocking New Opportunities:* Digital technologies, from AI to IoT, have paved the way for businesses to enter uncharted territories. Whether it's tapping into new markets, launching innovative products, or identifying unique customer segments, the digital landscape is rife with opportunities that were previously unimaginable.

4. *Competitive Edge:* In many sectors, the difference between leaders and laggards is their degree of digital adoption. Companies that invest in digital tools, technologies, and strategies position themselves at the forefront, often outpacing competitors in capturing market share and driving innovation.

5. *Data-driven Decision Making:* One of the most transformative aspects of digitalization is the power of data. Organizations today have access to vast amounts of data – from customer behaviour to operational metrics. With the right analytical tools, this data can be harnessed to derive insights, forecast trends, and make informed decisions, removing much of the guesswork that once plagued businesses.

6. *Scalability and Agility:* In a traditional setup, scaling often means substantial investments in infrastructure and manpower. Digital platforms, on the other hand, offer elasticity. Businesses can scale up or down based on demand, ensuring agility in response to market fluctuations.

7. *Global Reach:* The digital era has shrunk the world. A start- up in Johannesburg can cater to customers in any part of the world. The barriers of geography are diminishing, allowing businesses of all sizes to operate on a global scale.

Digital transformation offers businesses the tools, strategies, and mindset to not just survive but thrive in an interconnected, digital-first world. While challenges persist, the potential rewards - from growth and efficiency to innovation and global reach - make the journey not just essential, but invaluable.

However, this digital boon is a double-edged sword as with increasing digital footprints, vulnerabilities surface. In the past few years alone, we have witnessed high-profile cyber-attacks on businesses, causing not just financial loss but damaging their reputation and shaking the trust of their customers and stakeholders.

CYBERCRIME

According to reports cybercrime is expected to inflict huge damages annually. And that's not just large corporations at risk; small and medium enterprises are often prime targets due to perceived weaker security postures.

Any individual or organisation doing business on the Internet, - government departments and state-owned enterprises included, can be targeted by cyber criminals. It is therefore critical that digital infrastructure must be protected.

We all know the horror stories that have affected individuals, businesses, and governments across the world, confirming that social networks and mobile device interconnectedness can be a breeding ground for malware, perverts and internet criminals.

The case in point being that of Gerhard Ackerman, a pervert who was found guilty of sexual abuse and trafficking of children, creation and distribution of child pornography and was sentenced to 12 life sentences. Unsurprisingly, the biggest victims of any kind of online abuse are women and children. We need to intensify our efforts to fight online gender-based abuses.

Because we spend an inordinate amount of time on the internet, the risks are higher. In the latest Global Digital Report drawing data from several sources and research groups, it was established that South Africa has the highest screentime worldwide, averaging 10 hours a day. In other words, South Africans are regarded as the biggest internet addicts in the world spending an average of 9 hours and 38 minutes daily connected on any device. This is far higher than the global average of 6 hours and over 2 hours more than the USA.

CYBER ATTACKS

There have been documented attacks in 2021. An attack on the United States' Colonial Pipeline caused it to shut down for several days. President Joe Biden called a state of emergency.

In the United Kingdom, a technology supplier to the country's National Health Service fell victim to a ransomware attack in 2022, disrupting important functions.

In mid-2022, Estonia was the victim of its most intense cyber- attack since 2007. In May last year, a ransomware gang infiltrated Costa Rican government system. Increased internet penetration across our country can give rise to sophisticated attacks on our IT infrastructure.

Here at the home front, Transnet was a victim of cyber-attack. Impact???

Recent malware attacks in the region have put organisations on high alert and, as a result, the network security market is poised for strong growth rates.

CYBERSECURITY – THE BACKBONE OF DIGITAL TRANSFORMATION

Digital transformation without robust cybersecurity is akin to building a skyscraper on a weak foundation. No matter how impressive it looks, it's always at risk of crumbling.

Key elements of cybersecurity in digital transformation are:

- *Trust:* At the heart of any business lies trust. When customers engage with a digital platform, they trust it with their very private and personal data. A single breach can erode years of built trust.

- *Operational Continuity:* Cyber-attacks can disrupt operations. For companies that heavily rely on digital platforms, this could mean significant downtimes, losses, and setbacks in their transformation journey.

- *Legal and Regulatory Compliance:* With regulations like

POPIA, businesses are mandated to ensure data privacy. Non- compliance due to lax cybersecurity can lead to hefty penalties.

STEPS TOWARDS A SECURE DIGITAL FUTURE

While the challenges are manifold, they're not insurmountable. May I at this point proffer a few key points companies need to do to mainstream cybersecurity into their digital business processes:

- *Awareness and Training:* Educate employees about the importance of cybersecurity. Often, human error can be the weakest link.

- *Investment:* View cybersecurity not as a cost, but an investment. This means not only investing in tools and technologies but also in skilled personnel.

- *Regular Audits and Assessments:* Regularly assess and audit your digital infrastructure to uncover and address vulnerabilities.

- *Collaboration:* Cybersecurity is a collective effort. Collaborate with experts, other businesses, and even competitors to share knowledge and best practices.

- *Stay Updated:* The digital landscape is evolving, and so are cyber threats. Staying updated on the latest threats and mitigation techniques is crucial.

Data gathering and tracking of individual behaviours by digital firms has implications for privacy rights, and the PoPIA Act has worked to address this, but we know that more needs to be done, as we mainstream this important concept.

Going forward there must be more investment into our digital transformation drive that ensures that government information assets are always protected, be it, data at rest, data in compute or data in transit.

For government the critical areas in Information and Cybersecurity that is fundamental to protecting the assets of the state, include the need for improved information and cybersecurity skills.

We need purpose-driven initiatives to build local digital transformation skills, Information Security Skills, Cybersecurity Skills, Machine Learning and Artificial Intelligence skills.

As more government services go-online in the digital transformation journey, the one thing we must guard against strenuously is the threat of cyberattacks. Government employees, citizens and all roleplayers must be vigilant and aware of this potential threat through awareness initiatives.

To ensure information and cybersecurity resilience, our government information ecosystem must be designed and maintained for high levels of information and cyber security resilience in this ever-changing landscape**.**

We must collectively as a country use best practices and standards to build in-depth defenses in our digital infrastructure and services.

The POPIA prescripts of sovereignty, i.e. - “data privacy, residence and sovereignty” must be built into the design principle of the government information ecosystem to protect the state and its citizens.

The bottom line is that “we are as strong as our weakest link”. We must build and share people skills, processes, technology in partnerships spanning local and international boundaries. Government and private sector are responsible and accountable to protect and defend government data.

NATIONAL CYBERSECURITY POLICY FRAMEWORK

As a country we have laid a solid foundation with the adoption of the National Cybersecurity Policy Framework in 2015. It provides a holistic approach to the promotion of cyber security measures. It is supported by the National Cybersecurity Implementation Plan, which lays out roles and responsibilities, timeframes, specific performance indicators, and monitoring and evaluation mechanisms.

Amongst others, the Cybercrimes Act 19 of 2020 intends:

- to create offences which have a bearing on cybercrime;
- to criminalise the disclosure of data messages which are harmful and to provide for interim protection orders;
- to further regulate jurisdiction in respect of cybercrimes;
- to further regulate the powers to investigate cybercrimes;
- to further regulate aspects relating to mutual assistance in respect of the investigation of cybercrimes

Some of the new offenses in the Cybercrime Act - are related to data, messages, computers, and networks – and include hacking, unlawful interception of data, ransomware, cyber forgery and uttering, cyber extortion, and malicious communications.

CONCLUSION

Notwithstanding the perils lurking in the dark, the digital space is the best place we can be in at this age and time considering all advantages enjoyed by an inclusive digitally transformed society.

Enhanced cybersecurity frameworks and systems supported by legislation will ensure that we all thrive in digital South Africa

Let us remember that cybersecurity has no boundaries. We can't afford to let our guard down at any time or at any day. As the world changes, we need to engage more to ensure that we remain pro-active and not reactive to cyber threats.

I thank you!

….END