BYTES.za

The Department of Communications and Digital Technologies Report

IN THIS ISSUE

[] WHAT TO KNOW ABOUT RANSOMWARE ATTACKS (AND HOW TO STOP THEM) **[P6]**

[] WHY CYBER RISK IS EVERYONE'S BUSINESS **[P8]**

[] ARE YOU SECURE ON THE EDGE? **[P11]**

[] BUILDING RELEVANT ICT SKILLS FOR THE DIGITAL TRANSFORMATION ERA **[P13]**

[] WHY CYBER SECURITY MATTERS IN THE AGE OF DIGITAL TRANSFORMATION **[P15]**

[] CREATING INCLUSION IN CYBERSECURITY **[17]**

[] TOGETHER WE AMPLIFY **[P19]**

[] TRANSFORMING CYBERSECURITY PROCUREMENT SPEND IN THE PUBLIC SECTOR **[P21]**

[] SOUTH AFRICA'S CYBERINFRASTRUCTURE: THE CHALLENGES, THE OPPORTUNITIES **[P23]**

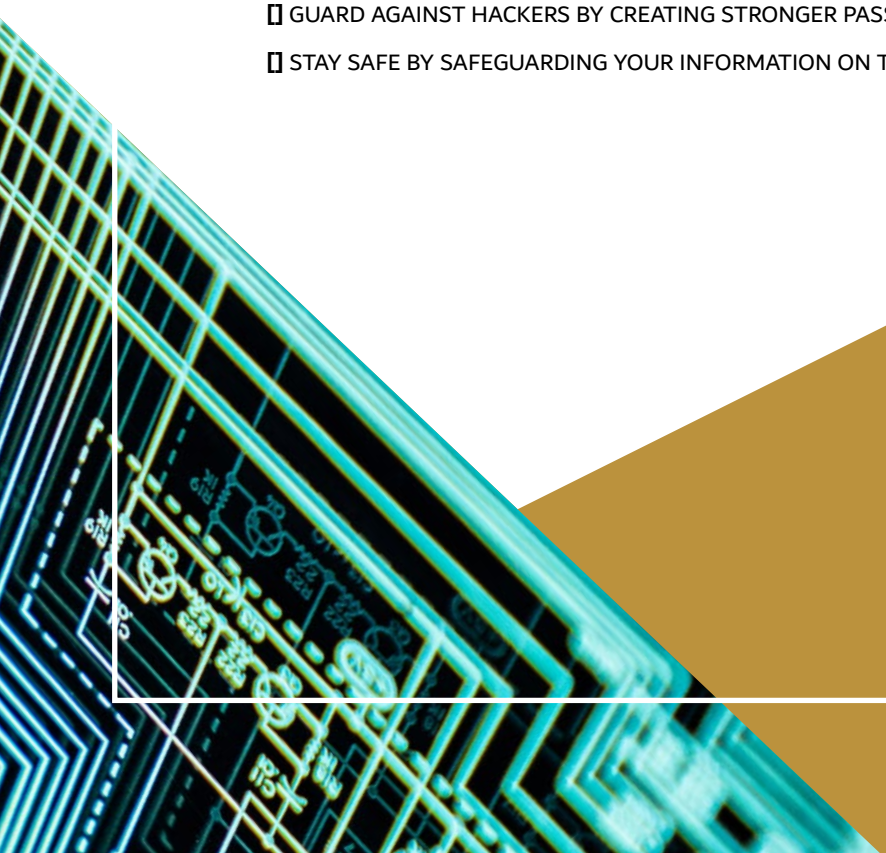
[] EDUCATE A GIRL CHILD ABOUT CYBER SECURITY **[P24]**

[] DEFENDING AGAINST RANSOMWARE **[P26]**

[] CYBERSECURITY ON A SMALL BUSINESS BUDGET **[P27]**

[] GUARD AGAINST HACKERS BY CREATING STRONGER PASSWORDS FOR SYSTEMS **[P28]**

[] STAY SAFE BY SAFEGUARDING YOUR INFORMATION ON THE NET **[P30]**



“The five most efficient cyber defenders are: Anticipation, Education, Detection, Reaction and Resilience. Do remember: “Cybersecurity is much more than an IT topic.” ~ Stephane Nappo

Hon. Khumbudzo Ntshavheni
Minister of Communications and Digital Technologies

Hon. Philly Mapulane
Deputy Minister of Communications and Digital Technologies

What to Know About RansomWare and Stopping Them

Mr. Thomas Mangwiro:
cybersecurity expert at Mimecast

Even as the world remains in the grip of a global pandemic that is showing no signs of abating, another threat is vying for the crown of number one risk to the global economy.

In scenes reminiscent of action thrillers, high-tech criminal organisations are targeting high-value organisations and critical national infrastructure. Data is being locked away in encrypted formats and criminals are demanding ransoms for millions in exchange for the release of data or, in some cases, the promise to not release sensitive customer and company information such as passwords and ID numbers publicly (in what is known as double extortion attacks).

These ransomware attacks are forcing organisations offline, which can lead to major disruption of an organisation and its supply chains.

Downtime means organisations are unable to deliver services which could be catastrophic when it affects critical national infrastructure.

Following a series of highly publicised ransomware attacks on businesses and critical US infrastructure, the US Department of Justice has announced it is elevating investigations of ransomware attacks to a similar priority level as terrorism. Recently, a successful ransomware attack on a US IT management software firm, Kaseya, put more than 1 000 businesses - all customers of the firm - at risk. What distinguished the perpetrators of this latest attack from historic ransomware attackers is that they offer ransomware-as-a-service, suggesting that anyone who was willing to pay it for its services could launch similar attacks against businesses or critical infrastructure. In fact, one report found that nearly two-thirds of ransomware attacks in 2020 employed a ransomware-as-a-service model.

Local organisations targeted

In South Africa, organisations face the dual challenge of securing against ransomware attacks and avoiding regulatory penalties should they fail to take all reasonable steps to protect against data breaches.

The Protection of Personal Information Act has raised the stakes for businesses who already face a growing volume of increasingly sophisticated attacks.

In Mimecast's State of Email Security 2021 Report, 47% of South African respondents stated their organisations were hit by a ransomware attack in the past 12 months, with seven days being the average amount of downtime.

Common consequences for affected organisations include data loss (66%), business disruption (53%), damage to their reputation (45%), loss of productivity (38%), financial losses (38%) and negative impact on regulatory compliance (30%).

Recent research by the Ponemon Institute also brings into stark relief the cost of data breaches to local organisations. According to the latest data, it took South African organisations an average of 177 days to identify a data breach and 51 days to contain it, costing them on average $2.14-million, or around R30-million, per breach.

Organisations, desperate to get their data back and avoid downtime as well as damage to their customers and reputations, are paying huge sums to these criminal organisations.

Mimecast research found that 53% of South African organisations that suffered a ransomware attack paid the ransom, but only 60% actually recovered their data. Forty percent never got their data back despite paying the ransom.

However, in a twist of irony, ransom payments are playing into the hands of criminals. When an organisation suffers a ransomware attack and makes the payment, they become prime targets for future attacks.

And cyber insurance is no longer the silver bullet: many insurance firms no longer cover the cost of ransomware payments.

A layered security strategy approach for best protection

What can organisations do in response to the growing threat of ransomware attacks?

1. Harden the email perimeter. Email remains the most attractive attack vector. Using a mature, cloud-based secure email gateway with advanced inbound and outbound scanning remains the most effective way to do that.

2. Deploy a layered email security strategy to augment the built-in email security of solutions such as Microsoft 365.

Recent Mimecast research found that 95% of South African IT decision-makers use additional third-party solutions to better secure their business email platforms.

Forty seven percent of respondents identified ransomware as a reason for deploying third-party solutions for email security, while nearly a third (31%) said ransomware was one of the primary reasons.

Thirty eight percent suggested their email platform's built-in security does not have adequate ransomware tools.

3. Protect and preserve corporate data by archiving to an independent, separately secured environment.

This allows organisations to recover their data in the event of a successful ransomware attack while also maintaining a lean amount of data that reduces the organisation's exposure and attack surface.

Our research found that 45% of respondents deployed third party solutions for email as they required reliable and robust back-up solutions in the event of a breach.

4. Establish an email continuity plan that allows you to continue operating in the event of a cyberattack or other disruption.

As the lifeblood of modern business productivity, email is essential to keeping the business running in the wake of a disruptive event, including ransomware attacks.

5. Support end-users by empowering them with regular and effective cybersecurity awareness training.

This helps strengthen overall organisational defences and removes opportunities for threat actors to breach the perimeter due to human error or negligence.

6. Employ new technologies such as AI and machine learning to bolster the capabilities of security teams.

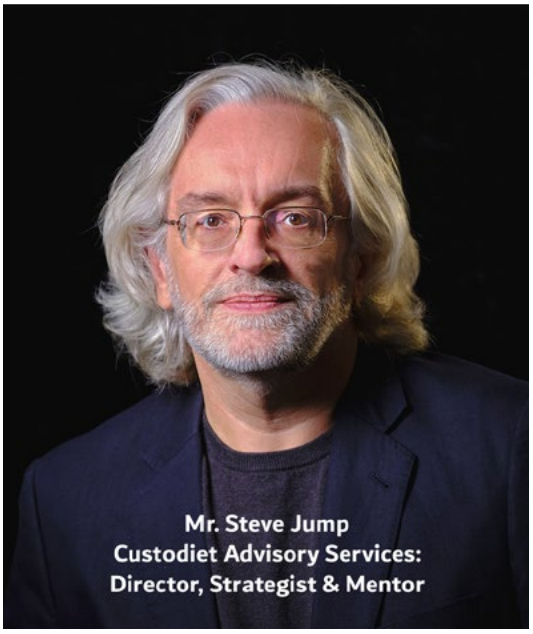
Such tools can be invaluable in helping recognise patterns for detecting threats or vulnerabilities, equipping security teams with greater visibility over potential risk areas.

7. Finally, organisations must monitor and control shadow IT. With the rise of the hybrid digital workplace, the lines between employees personal and professional lives are increasingly blurred.

Unsecured Wi-Fi, public file sharing services and insecure website access all increase the risk to the user and, by effect, the organisation.

By gaining greater visibility over applications, security teams are better able to monitor which apps are being used and block those that pose a risk to organisational defences.

Why Cyber Risk is Everyone's Business



Once upon a time, computers were huge, heavy, and expensive and only available to a very few companies. Businesses that had access to a computer soon found out that they could outperform their competition with ease. That meant that soon everyone wanted a computer, office by office, and desk by desk, computers started to be used in every part of every business.

But computers are complicated, and businesses found out that they needed new skills to keep their computers working to ensure their businesses benefited from the new information technology (IT).

When computers broke, or could not be maintained, businesses quickly realized that they lost money, so they invested in making their computers more reliable and keeping their systems more available than their competitors. Just keeping IT working well is an immensely difficult thing to do, but companies that could afford to do it stayed in business longer than those that could not. For these businesses IT reliability became a business risk and hence it became good business practice for it to be managed just like any other commercial threat.

And then, as computers started to be connected to other computers the internet arrived. Businesses that could "get online" could now conduct their business directly between computers, the opportunities were immense and so were the profits. Of course whenever there are people who work at making a profit there are always people who want the profit without the work, and so digital crime became a problem too.

So in addition to the IT risk businesses had learned to manage, preventing losses from the growing rise in theft and fraud using computers became just another risk for businesses to manage. It was in this era, almost 30 years ago, that the term password began to appear as a common business term. Even then it's use was often mistakenly assumed to infer a sense of security by those using it.

Just keeping an IT system working is a difficult enough task. For your infrastructure to be reliable always available, but only to authorized users and cost-effective, a business needs to take special effort to ensure that this can happen.

Businesses that chose to use cheap IT always found out that too cheap was always more expensive. But that is a different story about business economics. Our story though really begins in the early years of the 21st-century as the cost of electronics fell and allowed the creation of small portable electronic devices. Initially these devices were expensive mobile phones and portable laptops only accessible to business. But within the first ten years of the new century as technology costs continued to fall, battery capacity improved, and mobile communications became affordable the smart phone became a thing.

A pocket sized internet connected computer that everybody reading this tale owns at least one of. Almost at the speed of thought a connected customer became able contact retailers and suppliers, designers could commission designs, orders, payments, and banking could happen in seconds, businesses became able to scale as fast as they could connect customers to new internet services. Online assessment and comparison allowed instant value, both for the vendor and the customer. Every element of a commercial transaction had become a data element. But within that digitalisation of value came a subtle evolution in the way every business operated.

As data became business and business became data, the use and enrichment of that data became a business in its own right. Data had always represented an object with value, but now data itself had value in and of itself. Applications and application software became the vehicle through which data was collected, enriched, manipulated, presented and traded. The better, more intelligent, more usable the software, the more profitable the business.

As years of IT experience had taught many businesses some software was better written than others, and the better written the software, the greater the benefit, and the less risk to a business of using it. But the ease and speed with which anyone, or any organisation, could now become an online presence, or engage with their customers, partners or even citizens online allowed any type of software to be written or copied and an internet presence to be created in an instant, allowing almost any kind of data to be collected and manipulated.

Unfortunately as with anything of value, data itself now became a target of criminals seeking to steal its value, or to sufficiently damage it so others could benefit from its loss of value. This type of digitally enabled criminality earned its own new name “Cyber Crime”. Which in turn gave rise to the field of Cyber Security, which focussed on the technology and processes required to protect a business and prevent losses through cyber crime. Cyber Security itself is a highly complex function, and although its objectives are massively different to IT, its technical components often lead to it being placed within the IT department, sometime even being called IT Security.

Already stretched IT departments struggle to face up to the demands of cyber security, some are able to, but many in spite of massive investment in cyber security systems are not. As cyber breaches continue to make headlines, and companies both large and small have their customer data stolen, or become victims to massive ransomware attacks. As the personal and private data of citizens and businesses alike continue to be stolen, compromised, and used for identity theft and fraud.

As critical national infrastructure and healthcare facilities are taken offline, or even destroyed, and as even the regulators themselves fall victim to such attacks, questions are being asked as to why many businesses remain able to safely conduct business even as they endure targeted cyber attacks, but others that invest just as much, or more, appear to have no effective defences and fall prey to even the simplest cyber threat?

When examined more closely certain trends do reveal themselves. Cyber Risk is globally recognised as a fundamental threat to both business and social growth and represents a major threat to stable economies. Almost every business, small or large, has some level of risk reporting that now includes Cyber Risk as a business affecting element. Not surprisingly how and where cyber risk is reported, how it is measured and where the responsibility for it’s management resides has a massive affect on how well active cyber threats can actually be managed.

Unlike most of the other operational risks a business faces Cyber risk is subtly different. Whereas many risks are based on opportunity, environmental circumstances, availability of finance, use of technology, and other competitive factors that may happen to prevent achievement of business objectives; Cyber Risk is unique in that it is an adversarial risk - in that someone is actively trying to destroy, steal or damage your business.

Regardless of what your business does, whether you make or sell goods, provide social services to those in need, operate a national energy service, run a hospital, or simply teach in a university; a cyber criminal will still attack you.
So why is cyber risk different? As businesses have digitalised the risk management processes and procedures that they have built though the ages have become part of larger software based business process systems. This process virtualisation is often implemented for efficiency and expediency, the reasons and errors that exist in any active business system can often become hidden, or masked. Almost every business process is monitored in terms of how well is it working, how often does it fail, and how can it be improved. The measurements and controls to do this are under the control of the business itself. Cyber threats though are often not even considered when such business processes are being drawn up, if considered at all they are often left up to IT to manage and to report on under IT risk and hence appear as an unwelcome surprise to business when they actually happen.

Before digitalization the owner or manager of a physical business never actually needed to know how to design a factory or build a warehouse. But they did know that there were good and bad business choices to be made in terms of design and location.

Such decisions were readily delegated to people who knew about the business benefits of construction, skills to build, access to materials, power and water, and the cost of operations, security, and maintenance. As these are critical business decisions, not just in terms of cash flow and profitability, there are often severe penalties if regulations were broken, the owner or manager would always be an active participant in reviewing and approving them.

In a digitalised business every data collection, processing and manipulation that is required to be delivered by IT to produce value to a business has an equivalent cyber threat that can destroy that value and more. This cyber risk is of equivalence to every other risk that a business faces, and is readily recognised and addressed as a business threat in the normal daily function and operation of a business.

In a new warehouse project a CEO would never accept the project viability risk assessment being signed off by a technical specialist such as a senior electrician alone, no matter how experienced they may be. But when launching a software based online store that signs up and collects customer data, processes sales, enables payments and delivers goods that might double a company’s sales, the web site may be approved only by a senior graphics designer.

All software is prone to bugs, that is why code is tested all through development until ready for the application or web site to be launched. More importantly after it has been launched it is fully understood that any internet facing software is automatically subject to continuous scanning and attack by potential cyber criminals throughout its entire fifecycle. This requires that the business itself must be continually testing and fixing its own systems and assets for as long as they are online, and disconnecting them immediately they are no longer needed. Such testing and repair does not happen for free, it is a cost of business that must have been factored in to the initial design and lifecycle costing.

Why do some organisations then appear to be managing cyber crime, whilst others do not? Where cyber risk is managed alongside IT risk and the function of a software system is clearly defined and owned by the business function that will not only derive the benefit from its operation, but will be held accountable in case of any breach or failure, a more resilient and reliable system is built. Such systems do still suffer from cyber attacks, but the effect of the attack is rarely news worthy, or even reportable. In organizations such as this cyber risk is considered to be a responsibility of every department, who in turn ensure that the IT and cyber security teams understand each business units specific cyber threats and are then able to affordably prevent the cyber risks that would damage their functions the most.

Where cyber risk is delegated entirely under IT Risk, or perhaps not even addressed as a business risk, the additional expense of secure design and continued secure operations and maintenance is often factored simply as additional, non-value generating cost. Even the time to perform testing and cyber vulnerability assessment is often denied as interruptive and unaffordable. If normal IT systems struggle to remain functional and fight for maintenance budget every year it is unlikely that the secure design and security systems required for cyber risk management will be getting enough attention.

Wherever software is used to manage customer records, store personal identities and banking details, provide access to retail products, or simply enable social engagement and entertainment, its presence and use should not harm it's users. Recent legislation in South Africa and around the world is passing that accountability back on to the owners of such systems, by allowing victims of cyber crime due to negligence of a provider to sue the provider, and in certain cases open the management of the provider to criminal liabilities if negligence is proven. This accountability is clearly a business risk.

As business continues to evolve and grow within the digital and our existence increasingly depends on reliable, resilient and provably secure business systems it has become obvious that Cyber Risk is a subject that needs to be taken seriously by every business itself and every designer and user of such systems. Cyber security is too important to be delegated to the technical delivery side of your business. Cyber risk reduction is the responsibility of every business owner that derives benefit from any and every software enabled function or service.

As that business owner, the person who funds the idea, you own the risk that your solution may encounter, it is therefore up to you to make sure that the IT and technical specialists that design, build and maintain your systems know how to do so securely (1. Ask them), understand which threats matter most to your business (2. Tell them), and find the funding to keep doing so for as long as your business needs the service to exist (3. Support them). You don't need to do it yourself, but you do need to make sure it is done, and be able to prove it!
When you next hear of a massive data breach of sensitive information or a destructive cyber attack that shut down a business, it is almost guaranteed that at least one of these three business actions had not been taken to combat the cyber risk.

Are you secure on the Edge?

Ms. Sindisiwe Chuma: Entrepreneur and ICT Technologist

South Africa is seeing a surge in the adoption of Internet of Things (IoT) technologies in the services market. The constant exponential rise is expected to continue until 2027. This is because of national lockdowns due to the COVID-19 Pandemic are driving the adoption and utilization of digital channels as a means of communication, accessing information and working remotely by the state, private sector and civil society.

Constant access to digital platforms and the need to be easily reached in the shortest time permissible by the information and communication Infrastructure has made edge computing the mostly used initial point of contact to the outside world. Edge computing brings data storage closer to all users at improved response times, makes it easier to stay connected online while making the most of the resources available on limited spectrum that is overly currently utilized.

On the other end of the spectrum, increased adoption and roll-out of distributed computing has increased the threat-surface of cyber-crime. These are attacks are fuelled by poor public knowledge of cyber threats, limited investment in cyber security and cyber-crime legislation to regulate dynamic technological environments.

As a result, malicious users are able eavesdrop on communication devices and monitor networks they are not authorised to be on with no consequences. They send Denial of Service (DoS) attacks, tamper with data in local storage of the device being used to communicate and are able to conduct unauthorized activities and steal valuable private information where possible. These attacks are due to privacy and security problems as a result of ignorance and/or not being diligent enough to implement strong credentials, secure communication between devices, implement security patches and software updates in a timely manner, exercise selective data access etc.

Businesses that have invested millions on securing data on the digital infrastructure are not immune to threats mentioned above. A lot of investment has been made in end point security such as passwords not protection of company data that is on connected IoT devices or edge computing devices. Edge computing devices exposes company Intellectual Property (IP) and customer data especially when the device is access by an unauthorized person increasing potential attacks on the company, employees, infrastructure and data. Fortunately, there is a solution to the problems mentioned and it is empowering users of the edge computing devices with skills and information to prevent and be proactive in avoiding these attacks.

In 2019, the Statistics South Africa Household Survey reported that 63,3% of households in South Africa had a member that had access to the internet. These statistics are an indication that government, civil society and the private Sector must work together now in ensuring empowerment of South African Citizens in taking the responsibility to using the internet safely.

South Africa is gearing up on increasing initiatives to minimize the digital divide though Broadband Connectivity to connect rural and semi-rural areas such as Broadband Connect and others. This means more people will need to be educated on navigating the web safely and responsibly.

Education should be inclusive, alternative ways of getting the message in way that is easily understood should be exercised. In South Africa this means education on these new innovations that are posing cyber security threats should not only be conducted in English. Education should be in all eleven official languages and must be localized based on the linguistic requirements of each province to ensure understanding and constant training uptake of cyber security education.

In addition, education on responsible conduct on digital platforms should start early as primary school and young people must grow up knowing how to keep themselves safe and those around them from harm on the internet. Digital etiquette should be normalized and must made be an expectation from each individual that is interacting with others online.

Teaching of these principles is a responsibility of each and everyone of us especially to those that have not been exposed to them. Let's all go back to communities and families we belong to and part knowledge or learn together. It's not the government or private sectors responsibility to ensure safe and responsible conduct online.

It is our responsibility let's own it. A simple online search on the ABCs of cyber security and an application of the information learned is a great way to start before advancing to beginner, intermediate and advanced courses.

The Media, Information and Communication Technologies Sector in Education and Training Authority (MICT SETA) with the assistance of the Quality Council for Trades and Occupations has developed eleven new qualifications.

Cyber Security and Cloud Computing are in the list of the recently gazetted qualifications. These qualifications will aid the scarce skills crises we currently face in a shortage of the workforce knowledgeable in security on cloud computing technologies by preparing potential employees in institutions of higher learning.

The empowerment of the workforce on responsible online conduct will have a positive effect in business and will alleviate the huge burden for business to invest time and money on empowering employees in protecting themselves and company assets online. As a result, available options to direct more resources to innovate can be directed improving company compliance and security.

Managing security risk through compliance ensures detection, protection, prevention and security of company assets. Securing information and infrastructure through latest tools and technologies doesn't offer optimum security unless controls defined through compliance are used in the configuration and deployment of tools.

This means security is most likely to be effective when compliant controls in place are used. To manage complexity brought by increasing redundant processes can be managed though automation. Automation minimizes time spent, improved traceability and configuration, reduced human errors, consistent change management and configuration.

Building Relevant ICT Skills for the Digital Transformation Era

Dr Jabu Mtsweni
Centre Manager: CSIR Information and Cybersecurity Centre

The advent and adoption of Information and Communication Technologies (ICTs) in South Africa has led to several initiatives that attempt to eradicate a myriad of socio-economic challenges, such as access to education, financial services, information, health, and employment, to name but just a few.

It has also been observed throughout Africa that ICTs are becoming critical in contributing towards socio-economic development, and the mass adoption of mobile devices including mobile-enabled innovations across the different sectors cannot be disputed. However, it is also critical to note that technology is not a one size fits all, as context always plays a very huge role in the effective and efficient adoption and use of technology to address social problems and bring about the much-needed development in our communities.

The South African government has long acknowledged, through various strategic plans and initiatives such as the National Development Plan 2030 and recently 4IR Presidential Commission, that digital technologies and connectivity are core to the development of a modern knowledge economy and information-centric society. However, full implementation of these initiatives has always been lacking and lagging. As a result, South Africa has slowly dropped in the ICT Development Index and Global Cybersecurity Index over the past few years with ICT education and training, particularly in secondary and tertiary environments remaining stagnant and in other instances declining.

Nevertheless, the noticeable progress in the South Africa's digital transformation landscape cannot be ignored. South Africa has made steady progress in ICT development with an increasing number of households having computers and broadband internet, which are the enablers of technological innovations, information-centric society, and knowledge economy. Over 100 million mobile connections have been recorded in South Africa by January 2021 surpassing the population by over 168% and smart phone users almost at 100%.

The Internet users are at an estimated 64% of the population and active social media users are growing at a very fast pace, now seating at over 25 million .

The use of instant messaging platforms such as WhatsApp has changed the way citizens and governments communicate, engage, disseminate information and even provide online government services.

The reliance on digital technologies for virtual meetings and interactions has skyrocketed since 2020 due to the COVID-19 national lockdown, and clearly demonstrating that technology has a huge role to play in realizing the aspirations set out in the NDP 2030.

The implementation of 4G and 5G internet services across the country both in urban and rural communities continues to revolutionize the ICT arena, opening opportunities for the poor, small businesses, and previously disadvantaged.

The deployment of the fibre networks across the country has also made a positive impact, and this also saw a large demand during the COVID-19 pandemic including reduction of costs to some limited extent.

The innovative use of mobile banking and cash transfers without the need to have a bank account has forever changed the South Africa's economic landscape, and access to banking services even for the deep rural citizens. Access to online news media and shopping has seen considerable growth even before the COVID-19 pandemic demonstrating that digital divide is turning into digital difference where in Africa mobile technologies are driving information access and connectivity.

On the flip side, the wide adoption disruptive technologies, such as Internet of Things (IoTs), Big Data, and Artificial Intelligence (AI) introduces unintended and adverse consequences and challenges. Today, due to increased interconnectedness and digital advancements, cybersecurity incidents are also growing at a sophisticated pace all over the world, and they affect all organizations of different sectors and size.

As opined by (Tuteja, 2020) at the World Economic Forum, "our digital future depends on cybersecurity". In South Africa, we have seen an increase in reported cyber incidents over the past few months suggesting that there more we are connected, more risks and threats are introduced which we need to prepare for and deal with them systematically.

Cybersecurity has a particularly important role to play in the successful realisation of the NDP and 4IR via the safeguarding of the country's critical information and services including building cyber savvy citizenry, thereby improving the trust in and adoption of these services by the greater populous.

There is also a worldwide gap in skills needed to deal with digital transformation and cybersecurity. In the context of the 4IR and its disruptive effect on all economies, the development of digital skills is paramount. According to the ISC2's Cybersecurity Workforce Study of 2019, there are 3 million unfilled cybersecurity workforce positions across the globe.

This also calls for serious interventions in building advanced skills to prepare for an inclusive national participation in the 4IR. It is therefore paramount that organizations including our government start increasing their investments in developing relevant 4IR and cybersecurity capabilities to drive digital transformation, innovation, including protecting and securing their systems and data.

Although a view is that skills development for 4IR will take a concerted effort to rectify, it presents an opportunity for IT professionals, academics, researchers, university students, and other aspirants to take-up human capital development opportunities that may drive job creation and business opportunities. This also present opportunities for institutions of higher learning or re-engineer their curriculums such that South Africans are prepare for the Futures of Work.

Industry partnerships are also critical including collaborating in technology development initiatives with SMEs, collaborating with technology transfer offices at universities and research institutions to drive digital transformation capability development through grass-root level innovations, technology prototyping, development, and commercialization. This is expected to increase capacity and aligned workforce to respond to 4IR digital transformation imperatives, home-grown capabilities to respond to the fast-changing digital landscape.

Strategic approaches that could aid and guide seamless adoption and application of ICTs in building smarter and socially relevant communities that are citizen-focused, proactive, collaborative, corroborative, and impactful could also be useful.

Why Cyber Security Matters in the Age of Digital Transformation

According to the World Economic Forum, one of the top 10 risks facing the world today is Cyber Attacks as shown in the chart below. This risk has accelerated in the last 10 months as companies accelerate their digital transformation to meet the needs of customers and staff in the post pandemic world.

A cyberattack can impact a business in many ways, including:

- Loss or Damage to Electronic Data
- An attack can damage electronic data
- Loss of brand value
- Loss of Income due to downtime
- Privacy Lawsuits. (Compliance Risk)
- Extortion Losses.
- Notification Costs.
- Damage to Business Reputation.

Image: Catherine Weetman – using data from World Economic Forum (2020), Global Risks Perception Survey 2019-20 (available from: www.weforum.org/reports/the-global-risks-report-2020)

All industries face greater exposure to cyberthreats due to increasing digitisation. For example, in the airline industry, digital innovation across the value chain — combined with the sheer volume of customer data airlines possess — has made them a hot target for cybercriminals.

Various cyber incidents have demonstrated the need for airlines to upgrade IT and operational technology systems to reduce risk and build resiliency into their heavily digitized operating models.

The timelines below show Cyber Attacks for Ukraine's Power Grid & Anthem Data Breach. Both graphs highlight impact of Cyber Security in the Age of Digital Transformation.

Ms. Mamela Luthuli
CEO of TakenoteIT

UKRAINE'S POWER GRID AND CYBERWARFARE

2015

23 DECEMBER 2015:
Hackers manage to access and take control of three Ukrainian power distribution control centers, cutting off the power supply to 30 substations in several regions of Ukraine, which leaves about 230,000 residents without electricity for between one and six hours.

JUNE – JULY 2015:
Hackers send spear-phishing emails to staff that work for multiple power distribution centers, and begin mapping the network in preparation for the attack in December.

2015

DECEMBER 2015 – FEBRUARY 2016:
Several agencies, including the FBI and the US Department of Homeland Security (DHS), help the Ukrainian government during investigations into the attack.

FEBRUARY 2016:
Sixteen Ukrainian substations have to be manually operated due to slow recovery from the malicious firmware installed on the system.

17 DECEMBER 2016:
A second cyberattack on a Ukrainian power grid occurs; however, this attack only affects the country's capital, Kiev. A fifth of its power supply is cut off for just over an hour.

ANTHEM AND THE IMPORTANCE OF PROTECTING SENSITIVE DATA

2014

APRIL 2014:
The hackers gain access to Anthem's database.

18 FEBRUARY 2014:
An employee in one of Anthem's ancillary companies becomes a victim of a simple spear-phishing attack when they open an email containing malicious software.

10 DECEMBER 2014 – 27 JANUARY 2015:
Suspicious database queries are detected and continue until 27 January 2015.

2015

29 JANUARY 2015:
Anthem confirms the breach and alerts the necessary federal authorities and other key stakeholders of the breach.

4 FEBRUARY 2015:
Anthem publicly announces the breach.

FEBRUARY 2015:
The FBI and an independent state insurance commission prepare to investigate the breach. Anthem also begins an internal forensic investigation.

The response to COVID-19 has increased cyber risks:

Physical distancing means many workers are staying home and making greater use of services such as video conferencing, collaboration platforms, and other digital tools to do business.

In their free time, they are also going online more frequently to shop, read, chat, play, and stream. All these behaviours put immense stress on cybersecurity controls and operations.

Several major vulnerabilities stand out for us:

First, a broad shift toward work-from-home arrangements has amplified long-standing cybersecurity challenges and opened multiple vectors for cyberattacks (Exhibit 3).

Second, social-engineering ploys to gain information, money, or access to protected systems are on the rise, such as attackers posing as help-desk teams, health workers, or investors in virus-related response activities.

Finally, cyber attackers are using websites with weak security to deliver malware, in some instances using domains and websites created to spread information and resources to combat COVID-19.

As the COVID-19 outbreak progresses and alters the functioning of our socioeconomic systems, cyber attackers will continue their efforts to exploit our fears and our digital vulnerabilities. To remain vigilant and effective, CISOs will need new tactics, particularly in two areas: (1) securing work-from-home arrangements at scale; and (2) supporting high levels of consumer-facing network traffic.
Assess your vulnerabilities by performing a detailed quantitative risk analysis:

Cybersecurity should be central to every strategic decision and an essential component of every IT product in any organisation. Cybersecurity initiatives should be prioritised based on business-risk scenarios. By looking across the business through a cybersecurity lens, companies can transform their decision making and make wiser investments based on risk. Reviewing potential attack vectors from a risk perspective and evaluating the effectiveness of current cybersecurity activities could help identify areas that put the company at risk but are not yet covered by existing cyber activities.

We recommend that cybersecurity leaders assess their organization's current vulnerability through a security assessment including patch management practices; and build metrics and a dashboard to report regularly on the identified vulnerabilities and patch releases to the CISO.

Keitumetsi Tsotetsi: Senior specialist in governance, risk and control at Vodacom

Creating Inclusion in Cybersecurity

The beauty of being a disruptor is the ability to apply fast paced innovation. Technology is currently the backbone of business services across all industries. Technology is an industry that is developing faster than it is being discovered. This creates opportunity but also poses a risk because solutions are being implemented and replaced faster than they can be managed and legislated. A lot of technology operates over the internet. We must however remember that the internet was designed to be redundant and is not inherently secure.

Cyber security is aimed at protecting systems, networks and programmes against criminals. The cyber space is anticipated to be the one of the most high risk/high accountability careers because of the challenges that digitisation has brought forward. The cyber space brings great prospects for the global learning landscape through problem solving not only to protect companies and their assets but also to protect people and their identities.

Working from home has forced companies to digitise faster than they would have originally anticipated. This has produced great strides in productivity but has also increased the playing ground for cyber criminals. There has been a significant increase in cyber threats through phishing, social engineering, ransomware and malicious or insecure applications and services. The whole world is learning about new problems and resolving them as we go along.

No society exists without women, as such, industries should be a reflection of the societies they operate in. There is a discrepancy in the number of women who graduate in IT courses and how that translates to the number of women working in the industry. Organisations have openly mentioned that the lack of women in certain roles is not due to lack of trying.

Are women simply not picking IT and cyber security as career choices?

A lot of women are not in the cyber security space largely because of the limited exposure they have to the opportunities and success stories that are available in the industry. The need for diversity in the workplace goes without saying. Putting women in positions and not offering support in order to tick the “black female” quota is not going to do the industry any justice.

We need to build and upskill a capable workforce. Although there are a number of women in cyber security and leadership roles, we still have a long way to go. There are many women have led us all with their courage and perseverance and cleared the path for all of us. It is our responsibility to pass the baton on. Success, to me, means bringing other people along and giving them the capabilities to be self-sufficient.

Many of the opportunities that have been presented to me are a result of other women putting my name forward and having the confidence that I would deliver. We inherently have a “lift as we rise” mentality. I believe many people misconstrue us wanting gender diversity and equality to us saying we bring the same things to the table when what it actually means is that our different strengths are equally important.

There is lack of visibility of women in these roles which further feeds the imposter syndrome that women already feel going into a male dominated space. There's a boost of confidence that comes with the silent nods we give each other as women when we enter the room. For the youth, not being exposed to something as a reality may limit their perception of considering it a possibility.

There are many forums and organisations that are dedicated to enabling women in cyber security. Recent movements/trends such as #Infosecbikini and #DevsPelades were empowering non-men to bring their whole selves to work and spoke out against leaving certain parts of yourself outside of work to seem "more professional". The trends spoke out against sexism experienced by women in the industry (Riggins, 2021).

There is a lot of opportunity in cyber security ranging from tech, business innovation, academia, the legislative environment, research and development etc. There are also various roles that one can specialize in. Cyber security jobs are not limited to ethical hacking. In fact, there's a great need for people in "blue teams" who would be defenders of the systems. Members of the ISC(2) leadership team states "the cybersecurity skills shortage is expected to result in 3.5 million unfilled positions by 2021" (Morgan, 2021). Now THAT is opportunity. We need to find innovative ways to teach and learn cyber skills because the threat landscape is getting broader. There is a huge impact to business and potentially society as a whole if this is not addressed.

Although the frameworks of implementation vary, the requirement to embed digital literacy needed in the mainstream curriculum and upskilling programmes is agreed. The ability to protect, access, manage, deploy and generate information requires critical thinking and functional skills which prove to be a challenge in the South African context. The responsibility to address the challenge of digital inclusion cannot fall to one group. Private and public organisations need to work with local governments to create a global framework of cooperation to close the digital divide.

The cyber skills gap can be closed through formal higher learning but also with informal learning through events such as hackathons. Another consideration to make is to start teaching security at a basic level as soon as a child is starting to use technology because that's where the risk exposure starts. Organisations are furthermore doing their part in providing more entry level jobs and cyber security internships to enable learning and employment opportunities.

When we talk about resilience, it's not about how quickly you can bounce back from an attack, but looking at how efficiently you're able to continue operating during an attack. This applies to both cyber security and real life. Even though it might be a rocky road, what you are born to do comes with the grace to do it.

There are many women whose names we might not always remember but who have fundamentally changed the industry (e.g. Dr. Shirley Ann Jackson, Navy lieutenant Judy Parsons, Renee Guttmann). You don't always have to do things to be remembered. They do them because they have a positive impact on people's lives.

"Hackers don't break in, they log in."- Bret Arsenault

Together we AMPlify

Women in Cybersecurity and their Allies

Ms. Ranisha Reddy
Cybersecurity Specialist at Cisco

Representation of women in the cybersecurity industry has grown over the past years and, while this is positive, there is still room for improvement. Growth and success in this area requires that everyone work together to amplify but this is easier said than done.

How can those interested in cybersecurity further develop their careers? What can those who would like to be an ally do? To answer this, we asked a couple of women on the Cisco cybersecurity team across Africa to share their journey and experiences and a few common themes stood out.

Interestingly, not everyone in cybersecurity started with a technical background. Some of the women currently in cybersecurity started in non-stem-related courses.

Cybersecurity was also seen as a growing industry with a choice of job opportunities and diverse career paths to pursue, including engineering, consultation, leadership, and entrepreneurial opportunities. There was one bright spot that all the women we spoke to highlighted and this was the importance of having allies at different stages of their journey.

Allies, people who support and advocate towards a common purpose of growing representation in cybersecurity, advocating for women's representation in cybersecurity are not just women and not just people in cybersecurity. It is anyone who can contribute towards the common purpose of representation of more women in the industry.

Here are some tips and best practices for developing within cybersecurity as well as becoming an ally.

Developing Your Career in Cybersecurity:

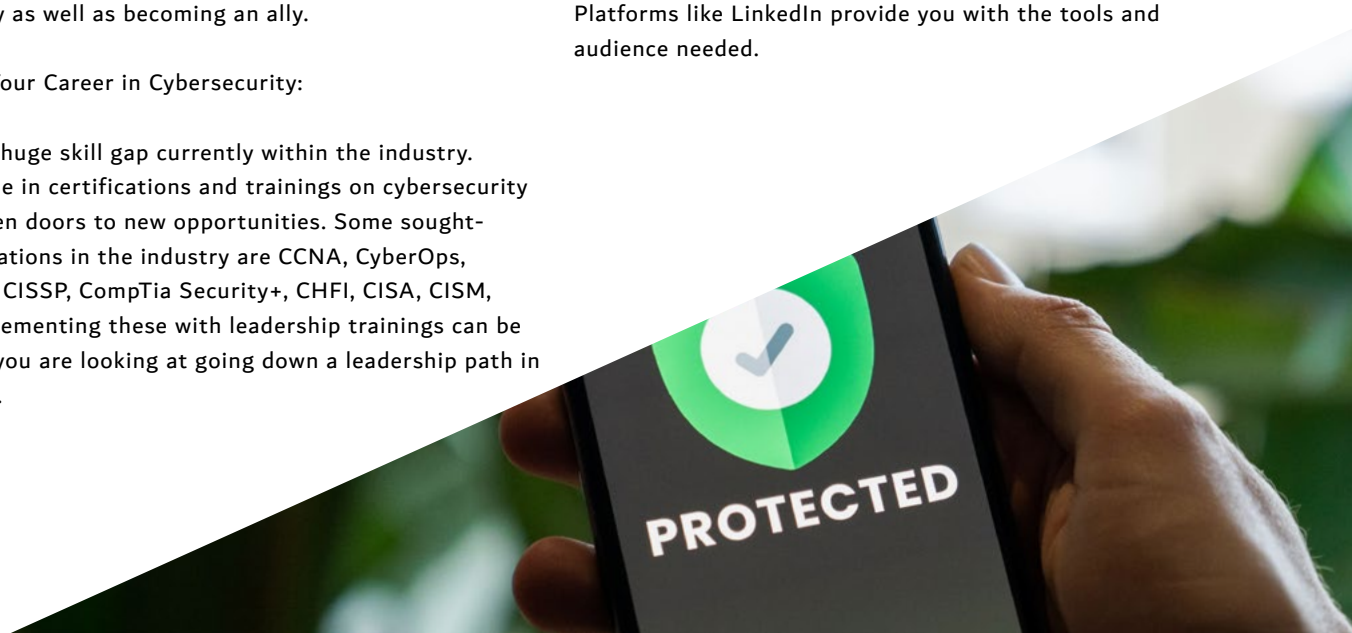
1. There is a huge skill gap currently within the industry. Investing time in certifications and trainings on cybersecurity skills can open doors to new opportunities. Some sought-after certifications in the industry are CCNA, CyberOps, CCNP, CISM, CISSP, CompTia Security+, CHFI, CISA, CISM, CRISC. Supplementing these with leadership trainings can be beneficial if you are looking at going down a leadership path in this industry.

confused
someone whose path
would like to follow and guides you
based on their learned experiences. A sponsor is someone who has influence, a seat at the table, knows your career vision, and can advocate for you. Among the women we spoke to, this has been a common theme along their journey. Here are some interesting stories of women in the industry sharing their experiences of mentors and sponsors.

3. Align yourself to a group supporting women in cybersecurity. There are many groups globally centred around women in cybersecurity. Being a part of groups and forums can give you opportunities around training, networking, exposure, and career progression. Here is a list of groups and forums that are out there.

4. Networking can give you exposure and access to opportunities. It is also something that you can leverage to make you successful at any part of your journey. Managing to build meaningful relationships can serve you well. Online many accessible videos can give you tips and best practices on networking, here is an interesting TEDx on meaningful networking. Networking is also about exposure, which forums and attending industry events can help with.

5. Thought leadership in cybersecurity can build your exposure and set the tone of being an industry expert. Contributing to knowledge articles and creating posts can foster this. Platforms like LinkedIn provide you with the tools and audience needed.



Being an Ally in Cybersecurity

1. Encourage women to pursue STEM as a further education degree. Research from isc2 has this as a leading indicator for growing representation in the industry. Volunteering to advocate at university career events, raising awareness on social platforms, or volunteering in different forums that promote STEM can help with this.

2. Providing sponsorship and mentorship opportunities develops representation. Signing up as a mentor on various forums, spotting, and grooming future talent, being a connector, and being accessible to people seeking sponsorship or mentorship help in being an ally in the industry.

3. Advocate eliminating the pay and promotion gap. According to isc2, there is still an inequity for compensation within the industry. Contributing towards training opportunities, development through mentorship, grooming candidates through a leadership track contribute to closing that gap.

4. Share your experiences to inspire women to pursue cybersecurity roles because the industry needs more role models. Be it a successful woman within cybersecurity or a man advocating for women in cybersecurity. Cybersecurity needs role models in both women and men to foster curiosity, awareness, and inspiration as we move forward and amplify as allies.

Cybersecurity is an industry filled with opportunities ripe for the taking. Growing women's representation in cybersecurity has advantages for all. There is a direct link for companies who have diverse teams which result in increased revenue. There is a direct link to creativity and innovation in companies that have diversity. Working jointly as allies and focusing on self-development will have representation continue to rise.

Transforming Cybersecurity Procurement Spend in the Public Sector

Ms. Nonku Dlamini: Founder and Managing Director of Mbokodo ICT Consulting Company

Small medium and micro enterprises (SMMEs) have a crucial role to play in building a sustainable and inclusive economy in South Africa. The National Development Plan 2030 (NDP 2030) is one of South Africa's strategic documents that has identified SMMEs as major sources of employment and drivers of growth in the economy to reduce inequality and redress the imbalances of the past. With the current unemployment rate sitting at 32,6% in the first quarter of 2021 as issued by Statistics South Africa, it is very imperative that as the Information and Communications Technology (ICT) sector we contribute to the economy by building an environment that will enable sustainable growth of SMMEs in the sector.

One of the challenges listed in the approved ICT SMME Development Strategy is the inability of most SMMEs in the sector to access markets for their goods and services. Access to markets is vital for SMMEs and plays a significant role in growing and sustaining their business. As we embark on the digital transformation journey it is therefore crucial that we prioritise initiatives aligned to the ICT technology roadmap that will accelerate the development and growth of SMMEs, unlock business opportunities and create an inclusive economy in the ICT sector.

At the **Department of Communications and Digital Technologies (DCDT) Budget Vote 2021/22,** Minister Stella Ndabeni-Abrahams informed the country that the Department and its entities always endeavour to support SMMEs through various procurement opportunities. The Minister also informed that the ICT Sector Council will publish its sector code to provide for 50% target procurement from majority Black Owned suppliers, an increase from 40% in the current code. The B-BBEE Act also enables organ of state and public entities to set B-BBEE criteria for procurement (Section 9) and develop and implement a preferential procurement policy (section 10). The B-BBEE Act is not an option but is mandatory for organs of state and public entities. Section 217(2) of the Constitution likewise allows the implementation of a preferential procurement system that will drive transformation.

It is of great concern that to date reports such as the B-BBEE ICT Sector Council, 4th Annual ICT B-BBEE Monitoring Report, 31st March 2020 results show that there is no real progress towards meeting the targets for Preferential Procurement within the measured entities that have submitted reports to the Council over the last 4 years. It is crucial that all government leaders responsible for the procurement budget fulfil the mandate and implement transformation initiatives that seek to increase SMMEs allocation of the government ICT procurement spend.

The **global cybersecurity market size is projected to grow.** As we transverse the COVID-19 pandemic while building a digital government ecosystem, the **need for a safe and secure cyberspace** has become more important than ever. The CIO survey by Gartner states that **Cybersecurity was the top priority for new spending,** with 61% of the more than 2,000 CIOs surveyed increasing investment in cyber/information security this year. As this is a global trend, it is critical that we ensure that South Africa's Cybersecurity Procurement Spend in the Public Sector grows within a transformed framework that includes SMMEs. We can't afford in the near future to be dealing with barriers to entry challenges due to long term contracts between public sector and Original Equipment Manufacturers (OEMs) that are not inclusive.

The President of South Africa signed the Cybercrimes Act into law on the 1st of June 2021. This provides the guidelines on the requirements for structures to deal with Cybersecurity (section 10) and Critical Information Infrastructure Protection (chapter 11). As the Justice, Crime Prevention and Security Cluster implement Cybersecurity systems and technologies to deliver on their mandate, it is of critical importance that working with the State Information Technology Agency (SITA), the Department ensures SMMEs are included in the procurement spend as a priority.

SITA as empowered by the SITA Act 88 of 1998, as amended by SITA Amendment Act 38 of 2002, must be the delivery vehicle for a transformed procurement spend framework. A framework that enables SMMEs access to the government ICT procurement spend. SITA must not only just deliver and efficient procurement system but ensure it has an effective procurement process structures/mechanism that will enforce legislation and policies that enables a transformed procurement spend.

In my view, all organs of state and public entities should not be signing any long-term contract with service providers that does not include SMMEs participation. When faced with a complex solution with critical Service Level Agreements (SLA's) that cannot be unbundled, SMMEs subcontracting should be compulsory to the prime bidder. Service providers including OEMs, through their enterprise and supplier development programs and channel partner programmes, must, at this point, have built sufficient SMMEs capacity to deliver aligned to their technology, road maps for continuous business to the market.

Collaboration and coordination are key in building a sustainable skills and development procurement readiness programmes to enable SMMEs to efficiently participate in the cyber security space. The Department is currently running a digital & future program driven by the department's National Digital and Future Skills Strategy. Cybersecurity is one of the three Strategic Implications for the success of the strategy implementation.

The Strategy Objectives include a roadmap for priority digital skills action points and a roadmap for stakeholder collaboration which can be used as base to confirm status of the cybersecurity skills already in the field and identified gaps for developing the required skills. In collaboration with its stakeholders, the Department led coordinating mechanism can also address the urgent needs of cybersecurity capacity by fostering knowledge, upskilling, and building competencies.

It's been my experience as a management consultant that the organisation culture and human resources are often the barriers to access inclusive procurement spend. Hence it is very important that there is an Executive Oversight on the organisation procurement spend objectives & deliverables. This is to ensure all deliverables are driven, monitored, evaluated and reported at top executive level. It is also of great importance that we provide reinforced processes with an organisation adoption and change strategy to ensure all the internal barriers are removed.
As we rebuild the economy, it is time that we take action and ensure we build a sustainable and transformed ecosystem that is more inclusive, more dynamic and where the fruits of growth are shared equitably.

South Africa's Cyberinfrastructure: the challenges, the opportunities

The National Integrated Cyber Infrastructure System (NICIS) was established by the Department of Science and Innovation in 2007 and is tasked with provision of world-class cyberinfrastucture for the country and to support its role-out in the Southern African Development Community (SADC) and in all the Square Kilometre Array (SKA) and African Very Long Baseline Interferometry Network (AVN) partners countries: Botswana, Ghana, Kenya, Madagascar, Mauritius, Mozambique, Namibia and Zambia.

NICIS – the three pillars

NICIS spreads its mandate through its three sub-divisions: Centre for High Performance Computing (CHPC) whose core is data processing through its petaflop supercomputer and support to its userbase by full-time high-performance computing (HPC) systems engineers and domain-specific research staff. The South African National Research Network (SANReN) and the Data Intensive Research Initiative of South Africa (DIRISA) are respectively responsible for the design, acquisition and roll-out of national and international capacity for the country's research network and the provision of a robust and reliable national data infrastructure for data intensive research with services such as a petascale eight petabyte research data repository and data sharing and archiving services through the deployment of a 40 petabyte long term storage facility.

One of the strategic objectives of NICIS is to sustain a world-class and relevant system for Science and Technology in South Africa and to support this in the region and to also be an international resource in global projects such as the SKA project, as well as a contributor to CERN.

NICIS project to upgrade SA-CERN Tier-2 Grid System

The CHPC's Tier-2 Grid System forms part of the world's Large Hadron Collider (LHC) which has a mission to provide global computing resources to store, distribute and analyse the 50-70 Petabytes of data expected every year of operations at CERN on the Franco-Swiss border. The Worldwide LHC Computing Grid (WLCG) project is a global collaboration of around 170 computing centres in more than 40 countries, linking up national and international grid infrastructures. The centre is working on upgrading the current Tier-2 storage capacity from 388 terabytes to the raw capacity of up to 4908 terabytes to increase the amount of data stored onsite. The sufficient data stored onsite will reduce data latency and allow scientists to effectively continue to work on the experiments due to the greater proximity of the data.

Ms. Noxolo Moyake
Communications Manager,
Centre for High Performance Computing

Skills Transfer

NICIS has many on-the-job skills transfer opportunities and the upgrading of the CERN Tier-2 Grid is one such. NICIS currently has interns and is training them in the field of HPC. During the project, the interns will learn how to configure the storage from the ground up, including racking and stacking servers, cabling and networking, software configuration to run the underlaying storage system.

Figure 1: Interns racking and stackngi servers, cabling and networking

Challenge: COVID-19 causes increased demand for computational resources

Figure 2: Rack layout

With the onset of COVID-19 came the increased demand for fast computing, NICIS found itself running out of compute and storage resources. The centre, through support from the universities of Cape Town and the North West, plus Dell EMC and Intel's Pandemic Response Technology Initiative, was able to expand its OpenStack Production Cloud.

The OpenStack Production Cloud expansion included the following:

- 15 new compute nodes using Dell PowerEdge R640 servers with dual Intel Xeon Gold 6230R processors for a total of 780 cores providing performance of 33.285TFlops
- 3 new storage nodes using Dell PowerEdge R740XD2 servers with dual Intel Xeon Gold 6226 processors
- 80 TB of hot data storage using Intel SSD DC drives
- 480 TB of HDD storage (3 x 160 TB copies)
- 1x Dell Networking N2048 1GbE
- 2x Dell Networking S4128T 10Gbe
- 10Gbe (40GB up links)

The expansion was completed in mid-2020 and went into production with a total capacity of 780 compute cores, 480 TB of cold storage, and 60 TB of hot storage (Intel SSDs). With more storage and compute capacity, users are experiencing a much more capable system. "Instead of being far overprovisioned with continuous 100 percent utilization," commented Dr Sithole, Centre Manager: CHPC, "workloads now consume from 60 to 100 percent of the compute capacity, depending on the activities."

Results

"OpenStack provides a different offering for users of the data centre," said Sithole. "This implementation is a step in the right direction to revolutionise our data centre as a converged environment. We see this as a continuum between compute intensive and data-intensive computing. It allows us to easily support both HPC research and general-purpose cloud computing in the same infrastructure", he added. With the original Supermicro cluster and the Dell EMC expansion, the expanded cloud can now support ongoing pandemic-related activities by the Department of Higher Education and Training, Department of Health, university research, and other public and private projects to address needs from the pandemic. Compute- and data-intensive projects include sequencing and virus research, remote education and online learning, bandwidth analysis of remote communities who need remote learning, television whitespace analytics, analytic epidemiology (including track and tracing), and others. The discovery of the South Africa variant of COVID-19 was accomplished using CHPC resources.

Figure 3: MeerKAT telescope

Support in the SADC Region and in African SKA/AVN partner countries

NICS has been very instrumental in supporting the SADC region towards the establishment of a regional cyberinfracture facility that would focus on research geared towards areas of mutual concern among member states, such concerns as: climate change, communicable diseases, economic development; etc. The SADC Cyberinfrastructure was signed by the ministers of Science and Technology/Innovation/Higher Education in the region and working committees are busy with implementation.

Challenge: training on the requirements and workings of supercomputing clusters

Many researchers in the region have never been exposed to HPC and some of these countries are SKA/AVN partner countries that will be hosting large telescopes but are not yet ready to process the data that will emanate from them.

A step in the right direction

NICIS through its establishing body the DSI and through the Department of International Relations and Corporations as well as through other well established computing centres in the world, has donated components of its own retired computers and some sourced from other centres internationally, to many South African universities and research councils, as well as to research institutions in the region and in the SKA/AVN partner countries. This was done for training as well for research purposes so that when the time comes, countries have acquired the skill to process their own data and the researchers are on gear to make use of these resources.

Ms. Anna Collard: Senior Vice President of Content Strategy & Evangelist for KnowBe4Africa

EDUCATE A GIRL CHILD ABOUT CYBER SECURITY

Anna Collard is the picture of a proper role model for teenage girls and women. Presently she's the Senior Vice President of Content Strategy & Evangelist at KnowBe4Africa. She clinched the Women in Tech Award for Central and Southern Africa in 2020.Collard was listed in the top 100 women in cyber security by the Cyber Defence Magazine last year.

As a woman with more than two decades experience in the digital sphere, she believes in the empowerment of the girl child and wants to see more young women enter the field in the coming years. She states that there are currently over four million vacancies in the cyber security world and that figure is expected to rise to around ten million in the coming years.

The Information Systems Audit and Control Association (ISACA) 2020 report indicates that 62% of companies' security teams are understaffed and 61% believe that fewer than half of all applicants are qualified for the job. The skills shortage is not only confined to Africa, but the continent has only ten thousand registered cyber security personnel and 9% of those are females. South Africa's economic growth hinges on the advancement of digital technology to move the country towards the Fourth Industrial Revolution(4IR).

The youth make up the majority in the country and they are demanding access to the Internet and are driving digitalization, especially on their mobile devices. Cyber criminals have shifted their focus to African countries owing to our growths in digitization, low levels of security awareness and a lack of or inadequate cyber security regulations. They attack both private and public infrastructure with ransom attacks and siphon off valuable data or finances.

Cybercriminals have shifted their attention toward the emerging economies, and Africa is a particularly attractive market for them for various reasons:

1. Africa's growth in digitization, leapfrogged by the pandemic and mobile adoption.
2. A relatively immature regulative environment.
3. Low levels of cybersecurity awareness on all levels from government to businesses, and consumers make our continent vulnerable to cybercrime.

Collard emphasizes that there is a need to see a cyber security culture instilled in all organisations across the board and cybersecurity must be taught in all schools from an early age. Recent reports by her company show that only 3.7% of higher learning institutions in Africa offer cyber training as a course or career path to students. These low numbers have made Collard believe that it is imperative that government must work hand in glove with academic institutions as well as the private sector to spread awareness and safeguard society.

"We need African solutions for African problems, and cyber security is a major opportunity, cybersecurity is no longer just a tech skill, it has become a life skill, "said Collard.

Collard believes more girls can be enticed to take up cyber security as a career once they are exposed to other successful female entrepreneurs or security trailblazers in the field. Therefore, this can be achieved through sharing stories of female role models as well as offering them bursaries and encouraging them to partake in competitions.

Ms Siphokazi Novukuza
Director: Cybersecurity Hub

Defending Against Ransomware

You could call it the global wave of cybercrime: Transnet and other South African government departments have joined tens of thousands of victims of ransomware, in which cyber criminals break into computer systems and encrypt and/or steal files in order to demand a ransom payment.

This document will discuss the recommended technical defenses and preparation (including people, processes, technical defenses) organizations should implement to mitigate the threat of ransomware. Ransomware is listed as the top worry by cybersecurity professionals throughout the world, with good reason.

Emsisoft states, in 2020 alone, $18 billion was paid globally in ransom and total costs were in the hundreds of billions of dollars.

A recent study by ITWeb and KnowBe4 across 378 South African organizations showed that:
1. Thirty-four (34%) of respondents fell victim to ransomware. Of those, 48% experienced a significant or very significant impact on their business operations
2. Social engineering (27%), unpatched software (16%), misconfiguration (11%) and password issues (8%) were the top reasons for initial foothold.

According to Sophos, the average cost to rectify a ransomware attack in South Africa is ZAR 6,7M ($0.45 Million) in 20202. Kaspersky saw a 24% increase in ransomware in Q2 2021 in South Africa.

Worse than the actual direct financial costs are long term reputational impacts such as the loss of investor confidence in South Africa.

South Africa has a fairly high digital dependency and as developed nations clamp down on cyber criminals, the same criminals will shift their attention towards the emerging economies, making South Africa a more attractive target.

Motivation or Who Is Behind It?

How It Works
There are over 100 different “ransomware families” operated by criminals ranging from quasi-corporate, collaborative networks to individual gangs and participants. Ransomware operators call themselves apolitical, they don’t particularly care about the impact they are causing to their victims or the citizens of the affected country. But no matter what their form, their objective is to criminally-enrich themselves. Ransomware as a Service (RaaS) allows so called affiliate networks to license the technology from operators and split their takings. This allows criminal elements without much technical skill to take advantage of this (underground) market opportunity and makes this such a growing threat on a global scale.

Top Initial Exploit Causes

What Is Social Engineering?
The top initial exploit causes that allow ransomware to compromise devices and environments are (in order of popularity):

1. Social Engineering/Phishing 2. Abuse of Microsoft Remote Desktop Protocol (RDP) 3. Unpatched Software 4. Password Attacks. Social engineering is consistently the number one root cause used by ransomware and other malware attacks to gain initial access.

Mr. Garsen Naidu
General Manager: CISCO
Sub-Sahara Africa

Cybersecurity on a small business budget

How to secure your business in minutes

Just because you're a small business doesn't mean you won't be a target for cyberattacks. In fact, small businesses can be particularly vulnerable because they lack the cybersecurity resources of larger businesses.

With the increasing shift to remote and roaming work in 2021, businesses of all sizes are more vulnerable to threats and attacks. Employees working off the network, from the cloud, and with technology and apps that aren't necessarily sanctioned (or protected) by IT staff. And these attacks do real damage with small businesses spending an average of R15M per attack to restore normal operations, according to Cisco's latest security outcomes report.

"54% of small businesses think they're too small for a cyberattack, but the reality is that 43% of all attacks target small businesses," says Garsen Naidu, general manager for Cisco sub-Saharan Africa.

"Even more worrying is that 47% of small businesses surveyed say they have no understanding of how to protect themselves against cyberattacks."

For the small business owner who is potentially overwhelmed with the idea of having to manage complex cybersecurity protection on top of running a business, while knowing it is time to upgrade his/her security technology to something stronger, Cisco's Umbrella can fill in the gaps for small business cybersecurity teams.

"A single unified security service, Cisco Umbrella reduces the complexity of monitoring and managing threats and alerts, so your team can do more with less," says Naidu. "Plus, Umbrella provides the extra support you need to make the most of your solution and fewer infections overall mean less remediation time, less downtime, and fewer of the costs associated with each."

Umbrella converges DNS Layer Security, Secure Web Gateway, CDFW, Cloud Access Security Broker (CASB) and Interactive Threat Intel, which is powered by Talos, the largest privately owned threat intelligence agency globally. All these services can be consumed via the cloud, promoting a SASE architecture that also seamlessly secures SDWAN deployments.

Small business owners are invited to down the Small Businesses Deserve Big Protection guide to learn how to get enterprise-grade security on a small business budget, with:

- The most effective threat protection in the industry
- Visibility and protection for all devices, on and off the network
- Simple management and flexible policies
- Rapid deployment and quick time to value
- Reliability and performance, you can depend on

Cisco has also invested in Africa in the form of two datacentres on the African continent, one in Johannesburg and another in Cape Town, which address on continent and in country redundancy to ensure data sovereignty and minimises latency for users of Cisco Umbrella across the region.

"For small businesses, threats are never going to stop coming. But with simple deployment and powerful protection, visibility, and performance, Cisco Umbrella can provide the big win they need," Naidu concludes.

Guard against hackers by creating stronger passwords for systems

Ms. Tendani Mulanga Chimboza
Information Systems Lecturer C3SA Communications Manager TRA Coordinator
Department of Information Systems

Our work in cybersecurity reveals that government organisations need to increase awareness of the significance of strong passwords. One may wonder why in 2021 we are still talking about strong passwords! The sad reality is that majority of the data breaches are attributed to weak passwords. As cybercriminals continue to perfect their craft, the problem of weak passwords will remain with us for a long time. The recent attack on the City of Johannesburg, Transnet, The Department of Justice and multiple South African banks are a call to strengthen our cybersecurity efforts. Most of our cybersecurity problems come lack of strong passwords. Passwords are central to a healthy digital life!

Governments must create an information security culture that protects their digital assets. In one of our webinars, our panellists agreed that cybercriminals prey on African governments because of weak information security culture and policies. While we may not be at the same level as cybercriminals, there are strong password best practices that can secure our digital lives.

Globally, most crippling security breaches are attributed to weak passwords. Of these breaches, 60% come from people who recycle passwords across multiple sites. For example, using 123456 as a password, and using the same password for your PC, Chrome, work email Facebook and so on. Despite the increase in cybersecurity awareness, people from both the private and government sector are still bad password practices.

In the workplace, passwords protect the most valuable digital assets of your organisation. A data breach gives access to these assets and leaves your clients' information vulnerable. Choosing impenetrable passwords and keeping them secure may sometimes seem too stressful, but the consequences may be irrevocable. The strength of a password rests on our password culture, awareness of strong password best practices, and weakness in cybersecurity capacity.

The weak links in our password culture

One password for all sites

Users with this password culture are the most vulnerable users in cyberspace. They have the same password for the PC, work email, browsers, and work enterprise resource planning (ERP) systems and so on. They also have the same password for both personal and work purposes. Sadly, these users usually create a weak password-based on "memorability".

However, once hackers crack the password, they can easily access all their digital assets. The vulnerability of these users rests on attackers' easy access to social media accounts that are set up using personal email addresses.

Multiple passwords for categories of websites

These password users have various single passwords for varying categories of sites. For example, having the same password for all SAP systems at work, another password for Facebook, LinkedIn, Twitter, and Gmail, and another one for online banking and shopping activities. These users are most vulnerable to a Brute-force attack - an attack where hackers penetrate user's sites by submitting many passwords until they gain access.

Saving passwords in a browser

This is a culture of saving passwords on browsers. In this password culture, security rests on browsers' security features. It is the tendency to believe that the browser "can never work against us". While these password savers are encrypted, the problem may arise once the password is accessed externally. If we have weak passwords, we may have to refuse the temptation to save the password on browsers. This is because these password features cannot save us from the complex digital space, i.e., you use the saved password for Google Play where there are a host of applications that can expose your personal data, you risk the safety of your digital life. For example, it was reported that 60 million user data from wearable technologies such as Fitbit and Google health info was leaked because of a lack of or weak passwords.

Internal shared passwords

It is common for a department to have one shared password to access a certain system. Organisations do this practice to allow multiple users to work on the system in case others are out of the office. While it may guarantee continuity of work, it is not the safest practice. Organisations employ this strategy even though they are aware that employees remain the primary security risk. The challenge with this password culture rests on the difficulty to control people when it to sharing it with people outside the organisation. Moreover, because of the chaotic business life, organisations are often reluctant to change passwords once an employee resigns. Consequently, organisations can fall prey to insider threats.

Strong passwords best practices

Globally, organisations are developing strong password policies to safeguard their digital assets and the digital lives of their employees. However, there are various ways of discovering passwords – some have not been documented. The best practices outlined here are based on common cybersecurity threats faced by organisations.

Establishing password policy

The absents of a robust password policy can expose the organisation can lead to multiple and costly problems. Organisations must think through their passwords policy strategies that take its context into consideration. For example, an organisation with a larger percentage of Baby Boomers and Gen Xers must have password policies that are consistent with these generations' conception of information security. Password policies should be viewed as internal controls that safeguard organisations from costly cyberattacks.

Conduct internal strong passwords awareness campaigns
A list of guidelines for strong password must be accompanies by awareness campaigns. Organisations must not only 'police' strong password behaviours but must embed them in organisational culture through campaigns.

Enforcing multi-factor authentication (MFA).

Multi-factor Authentication adds another layer of protection in addition to your password and username. The additional factor is a mobile phone app or a One-Time Pin (OTP) that you will use to confirm that you are the one trying to log in. This practice adds an extra layer of security that makes it difficult for hackers to launch attacks.

Promoting long passwords.

This practice allows users to create complex passwords that are difficult to guess; for example, "#Try2@ttackngim3! MyWyF1*RSA" This is done by using illogical passphrases or a combination of characters, i.e., capital letters, special characters, numbers and small letters. It is a good practice to change passwords Essentially, the length of the password increases complexity, and makes it harder to decrypt.

Conducting periodical password resets

While it may be perceived as a tedious process, conducting periodical and mandatory password resets increase data safety. Organisations must take the responsibility of sending emails to teams to reset their passwords at an agreed period.

Introducing biometric authentication

Biometric authentication is a practice of using user's biological characteristics (e.g., eye movement, fingerprints, or facial and voice recognition) as a password. By far, biometric authentication is considered the most effective practice of securing data. It is particularly effective in organisation with highly sensitive information that can be accessed my multiple users.

Weakness in cybersecurity capacity in South Africa

At a macro level, weak passwords are a consequence of an uneven cybersecurity capacity at government level. We are now at a point where issues of cybersecurity should be placed as a matter of national importance so to protect the citizenry.

In the study about "Unpacking Cyber-Capacity Building in Shaping Cyberspace Governance" in the SADC region, C3SA's Director Dr Enrico Caladra concluded that there was a lack of capacity to respond to the cybersecurity threats and risks. The move to work from home due to COVID-19 increased cybersecurity vulnerabilities in the Sub-Saharan Africa. Meanwhile, there is an explicit difference between cybercriminals' skills and South Africa's current cybersecurity competencies. The time has come for governments to invest in cybersecurity training to increase the number of cybersecurity competencies.

Stay safe by safeguarding your information on the net

Mr. Ignus De Villiers – Liquid Intelligence Technologies: Group Head Cyber Security

Since the era of computers began, we have manifested an entire new universe with enormous benefits and cutting-edge technology that has made our lives a million times easier in comparison to that of our ancestors. It even seems fair to go as far and call computers our "super-power" but with every great power comes an even greater responsibility.

Computers may just be the cheat-code for our civilization to progress and advance at a lightning speed, but it is also tremendously vital to protect this asset like we protect our health, our house and our savings.

Our responsibility lies in protecting our sensitive data and information that is stored electronically. With technology advancing by the day, the level of threat from cyber-attacks has also increased with time.

The digital world is a lot like the physical world where you are more at risk of getting attacked if you are not really on top of your survival game. That's where Cyber Security steps in, it is an absolute crucial priority for businesses to protect information, save data and control privacy. Cyber-attacks have the potential to make an organization's information inaccessible, impacting businesses reputation leading to financial consequences.

Companies, corporations and businesses are especially vulnerable as most of the sensitive and confidential company information is stored online but individuals can succumb to such attacks too.

That is what makes cyber security so indispensable because anyone can be exposed anywhere in this digital economy.

Sitting on a Virtual Land Mine

A PwC study last year revealed that about 62% of global CEOs worry that cyber threats will affect their company's growth prospects. With the post pandemic era shifting gears to a totalitarian digital world, it is becoming apparent why organisations are rushing towards securing their Cloud and private assets.

Even before the onset of the pandemic that transformed the global landscape of working, accelerating digital adoption, Cyber Security risks and dangers were considered one of the biggest safety issues for an organisation.

However, the post-pandemic era hints towards Cyber Security being the single most important focus to secure a company's future.

A business is fundamentally at risk 24x7 if it does not have Cyber Security appropriate security controls/ safeguards in place. Organizations are at a higher risk of exposing their critical information, impacting them adversely should it get leaked. With a plethora of newer cyber-attack tactics mushrooming daily, it is vital that businesses irrespective of size or geography treat Cyber Security as a high priority.

Human Error – Number One Cause of Cyber Security Breaches

According to a study done by IBM, human error is the main cause of 95% of Cyber Security breaches.

In other words, if human error was somehow eliminated entirely, 19 out of 20 cyber breaches may not have taken place at all. Another research predicted that 94% of malware is delivered by email (CSO Online).

To make matters worse, many organizations don't have sufficient resources to educate staff on the best way to manage their data.

With this lack of awareness and resources, human error continues to be the driving force behind an overwhelming majority of Cyber Security compromises.

Poor password hygiene is also a significant contributor towards compromises, with not enough individuals and corporations applying best practice and taking advantage of built-in mechanisms such as group policy enforcement, strong encryption and multi-factor authentication that could save the day from such threats.

Defense in-depth

Partner with a service provider with proper expertise and experience, helping the business construct a well-tailored Cyber Security strategy specific to business needs.

With the number of complexities involved in protecting information, it is key to have a defense in depth multi-layered approach.

Perpetrators are coming up with newer and newer techniques to gather information through attacks causing punitive damages to the economy thereby sparking an urgent need for Cyber Security.

The only real way to ensure that you are protected against cyber threats, frauds and attacks is to have a resilient cyber security framework in place.

Entity News

The National Electronic Media Institute of SA (NEMISA) Partners with the .ZA Domain Name Authority (ZADNA) to bridge the digital skills gap in rural areas and townships across SA.

NEMISA and ZADNA have joined hands to execute a grassroots digital skills training partnership. The two entities, under the Department of Communications and Digital Technologies, have signed a 3-year-long partnership agreement which will see the two parties harness their expertise to address the digital skills shortages within the country and with a particular focus on schools.

NEMISA's mandate is to be a sustainable skills training provider in the digital technologies and creative media spaces. NEMISA targets in-school and out of school youth, women, people with disabilities, SMME's and communities in general. ZA Domain Name Authority. ZADNA is a State-Owned Entity established in terms of section 59 of the Electronic Communications and Transactions Act, 2002 (Act 25 of 2002). It is accountable to its members and the Department of Communications and Digital Technology (DCDT).

.ZADNA is mandated to manage and administer the .za domain namespace, which is South Africa's internet country code top-level domain (ccTLD). https://www.zadna.org.za

Among other initiatives, the two entities have agreed to
i. Enhance their drive to deliver training to schools, districts, and local municipalities to benefit from the NEMISA training programmes.
ii. Assist beneficiaries to take advantage of online presence by increasing .za domains for schools and SMMEs.
iii. Offer ZADNA advocacy support through its platforms.
iv. Avail NEMISA Learning Management System to deliver online learning.
v. Co-fund joint projects as may be identified from time to time.

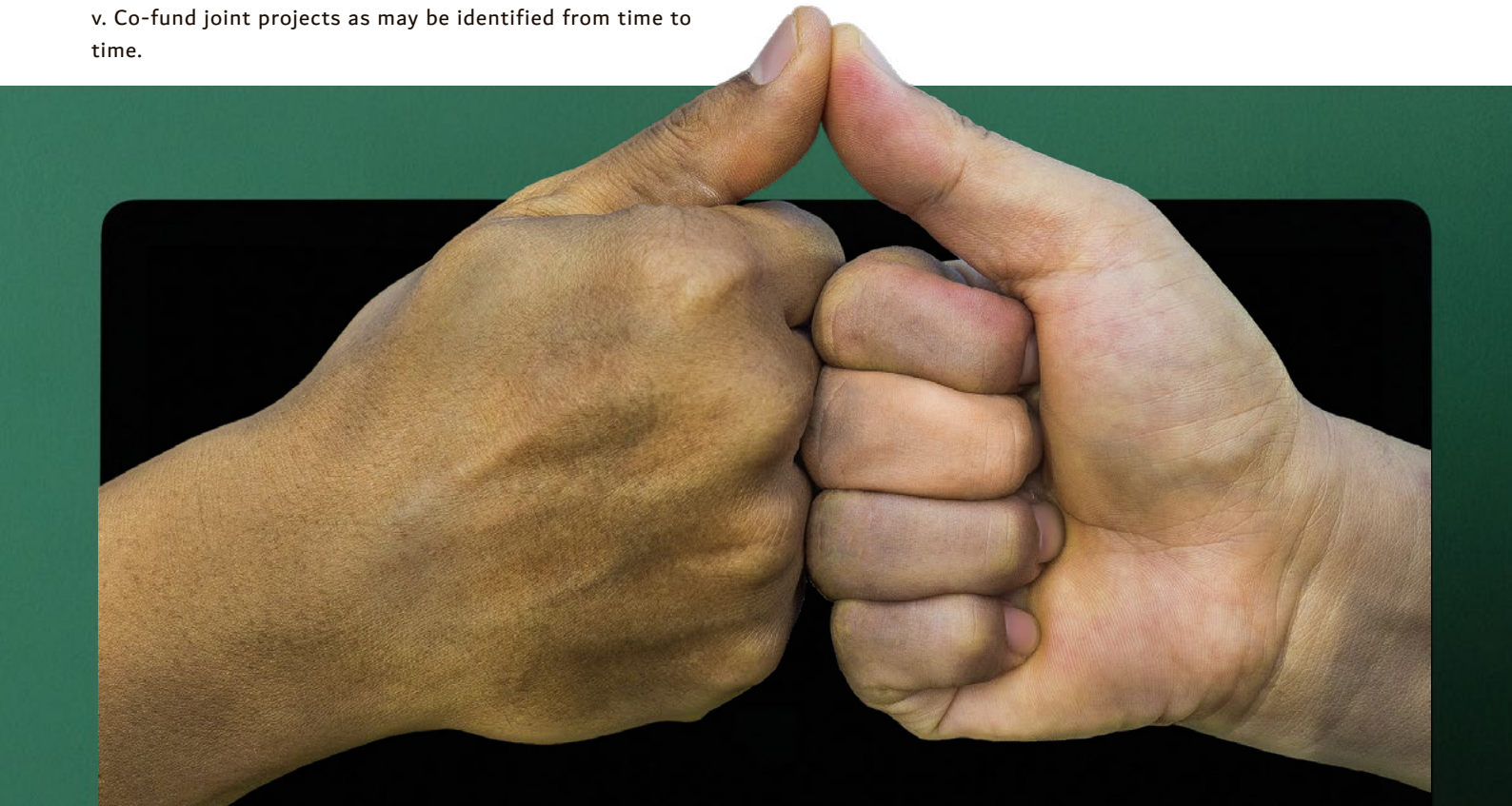
NEMISA CEO Trevor Rammitlwa said: "Introducing rural and township schools to the online world in a more aggressive way will make a big dent in fighting the digital divide in South Africa. The partnership between NEMISA and .ZADNA is the needed catalyst for this cause."

As part of this exciting partnership between the two institutions, ZADNA has identified a need to digitise South African public schools by providing the ".za domain" name under the school .za second-level domain (SLD). During the first 12 months of piloting the project, 200 school domain names will be registered and connected.

This will be followed by a further 734 public schools per year for the next two years and 734 public schools in the last year. A total of 2 400 schools during the life of the project will therefore have benefited. According to Mr Molehe Wesi, CEO of ZADNA, the .za schools digitisation project aims to digitise South African public schools by providing .za domain names to transform education through a viable alternative mode of teaching and learning.

"Through this initiative, as the Authority, we intend to ensure the Learners build and mature their digital presence. The beneficiary schools will leverage these domain names as a platform for teaching and learning.

In addition, NEMISA coordinators will go to the schools to conduct digital literacy training to the educators and students.



Film and Publication Board helps to convict Child Pornography offender

A recent conviction in the Oudtshoorn Regional Court upped the number of successful prosecutions for possession of child pornography that the Film and Publication Board (FPB) has contributed to in the past few years. The FPB worked closely with law enforcement on this case, conducting an analyses of the images found in the possession of the perpetrator, resulting in a 7-year sentence, of which 2 years is suspended.

The FPB Child Protection Officer involved in the analysis of the suspected images of child porn also provided expert testimony of the findings in November 2020. The charge was brought against the perpetrator according to the Films and Publications Act 56 of 1996, as amended, which makes the creation, possession, and distribution of child pornography as well as the exploitation of children for this purpose, a criminal offense. 200 images found in his possession were confirmed to be Child Sexual Abuse Material (CSAM).

“This sentencing, after many hours of diligent work by our Child Protection Officers in close relationship with our colleagues in law enforcement, is warmly welcomed,” says Interim Chief Executive Officer of the FPB, Ms. Nomvuyiso Batyi. “In our pursuit of eradicating the scourge of Child Sexual Abuse Material (CSAM) we employ internationally certified content analysts who are trained to ascertain whether people depicted in the suspected material are children (per South African law, anyone under the age of 18).”

The FPB are also currently working with police on a case of a woman in Bonteheuwel, Cape Town, who allegedly sold images of her naked child. “We are committed to supporting law enforcement in securing successful convictions when such cases are lodged. We will be providing technical assistance and monitor the case closely as it unfolds,” Ms Batyi adds.

The anonymity of the digital space has escalated the incidents of Child Sexual Abuse Material

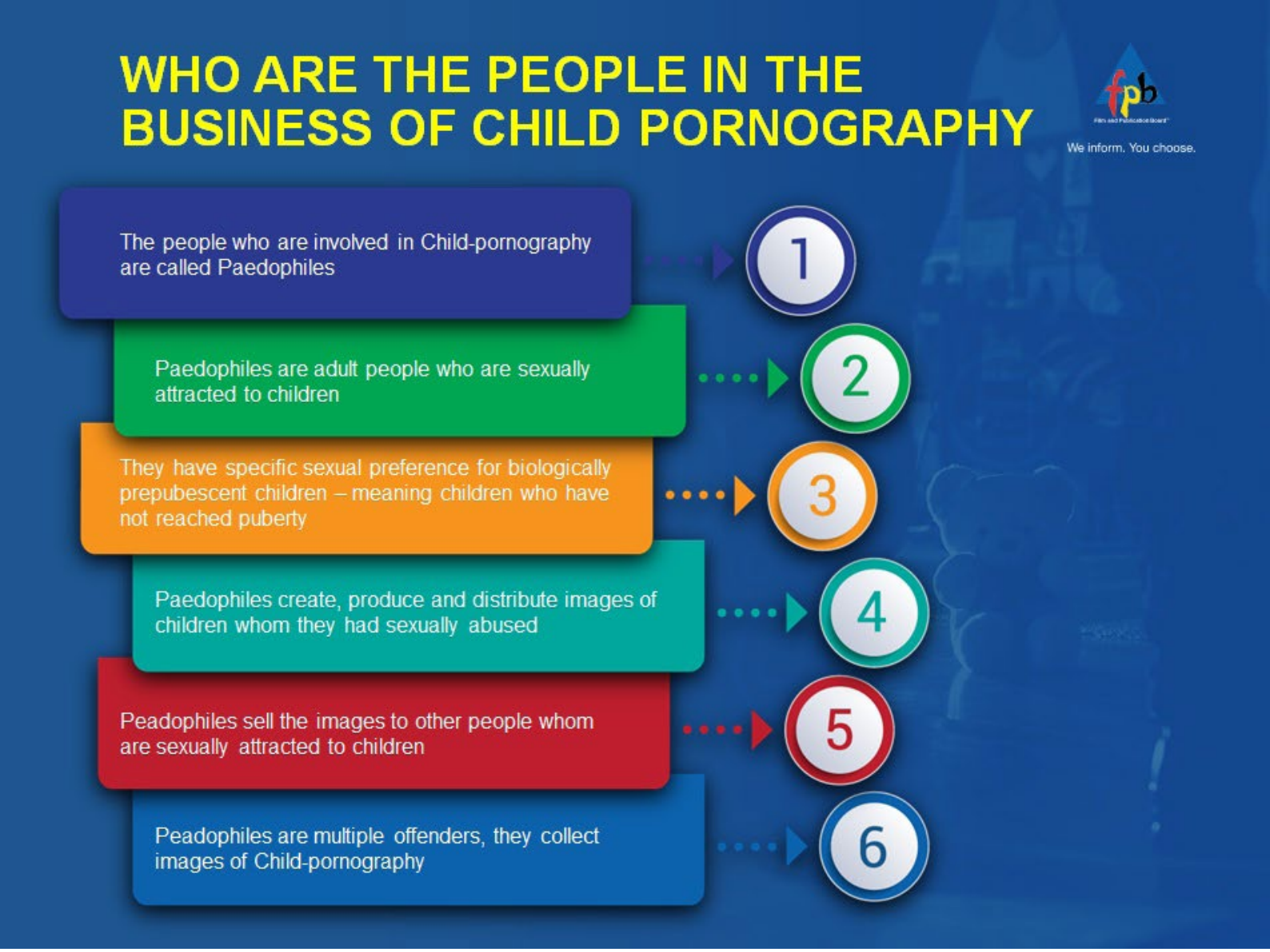
The rise of the digital space has made the work of the FPB and law enforcement in fighting CSAM doubly challenging. Sexual predators find an anonymous home on the internet, where it is easy to build a persona that is very different from reality, that can be used to exploit others. ‘Stranger danger’ is a mantra that caregivers should be teaching their children in the real as well as virtual world.

The FPB works in partnership with like-minded organisations in South Africa and around the world to close in on the perpetrators of these heinous crimes against children. “Working through the International Association of Internet Hotlines (INHOPE) and their links to the International Criminal Police Organisation (Interpol), we are able to track CSAM that has been created or distributed through international syndicates and finds its way to South African perpetrators online,” Ms. Batyi says. Through these international networks, the creators or distributors of CSAM are brought to book according to the laws of the jurisdictions where they are based.

In 2020/21, the FPB received nine cases of suspected CSAM from members of the public through its hotline or by direct email. In addition, the FPB worked on 23 suspected CSAM cases referred by the Family and Child Protection Services (FCPS) division of the South African Police Services (SAPS). In total, 733, 810 images were examined of which 3.7% (27,174) were found to constitute CSAM. Only three cases did not contain any child sexual abuse material.

Once case received from the Western Cape contained 417 DVDs with video footage of suspected child pornography and 21 of those DVDs were confirmed to contain video footage of CSAM.

“We treat cases of suspected exploitation of children with the utmost seriousness,” says Ms. Batyi. “A great deal of time is spent in the analysis of cases, with the gruesomeness of these images sometimes taking a toll on the officers employed to analyse them. While we do ensure that the officers are fully debriefed and able to access professional psychological care, the effort put into the analyses would be more greatly rewarded if more cases resulted in a sentence or if the sentences handed down would be more severe. However, we do understand that building a solid and water-tight case is a constitutional priority.”



A whole-of-society approach needed to eradicate Child Sexual Abuse Materials

The problem of child sexual abuse and CSAM is insidious and requires the vigilance of everyone in society to curb it. The long-term psychological damage to a child abused in this way is multiplied when the images of the abuse can be circulated and accessed online for all time.

The FPB conducts regular community outreaches to warn children, their parents, and caregivers about the dangers of online or in-person grooming. Often children are targeted and befriended by perpetrators and groomed for extended periods to gain their trust. They are then coerced into posing for nude photos or participating in sexual activities that are filmed.

A very alarming trend that has been noticed in recent months is user-generated nudes, where especially teenagers are paid to capture and send compromising photos of themselves or perform via online streaming. Sometimes the images are sourced through extortion, where children are threatened with the release of their sensitive information to the public.

Covid-19 restrictions have made it harder for perpetrators to target children physically, and the online space has become a new hunting ground for these criminals.

Understanding what to report

If you see a child whom you think might be at risk of sexual exploitation, then you should report it to local law enforcement or a hotline/help line. Members of the South African public are urged to report any suspected exploitation or grooming of children or instances of suspected CSAM in circulation to: hotline@fpb.org.za.

The more concrete the information you can provide with your report, the greater the chance that law enforcement will be able to act to save the child from continued abuse. Girls and boys are equally at risk of this form of exploitation, and both men and women can be perpetrators.

EDITORS

Mr. Siphiwo Nzawumbi
Mr. Frans Mthombeni

CONTRIBUTORS

Mr. Steve Jump
Ms. Siphokazi Novukuza
Ms. Nonku Dlamini
Dr Jabu Mtsweni
Ms. Anna Collard
Ms. Sindisiwe Chuma
Ms. Noxolo Moyake
Ms. Mamela Luthuli
Mr. Thomas Mangwiro
Mr. Garsen Naidu
Ms. Keitumetsi Tsotetsi
Ms. Tendani Mulanga Chimboza
Mr. Ignus De Villiers
Ms. Ranisha Reddy
Mr. Lerato Sepotokele
Mr. Lubabalo Sigonyela
NEMISA
.ZADNA
FPB

DESIGNER

Mr. Mvelo Mathe

For content submissions email:
snzawumbi@dtps.gov.za | lsepotokele@dtps.gov.za

PLEASE FOLLOW US BY CLICKING THE ICON BELOW

FOR MORE NEWS YOU CAN SIMPLY CLICK THE ICON BELOW
& PLEASE DO SUBSCRIBE ON OUR BYTES.ZA PODCAST
DON'T MISS OUT

STAY HOME
SAVE SOUTH AFRICA

2030 NDP

All Rights Reserved 2021DTPS| Used Images from Unsplash, Pixels & Pixabay