datacentrix

Second Edition **2023**

infocentrix

Sustainable Progress

infocentrix
Second Issue 2023

Contents

Infocentrix is an official newsletter for the Datacentrix Group, its partners and clients.

Datacentrix is a leading hybrid ICT systems integrator and managed services provider.

Our expert teams leverage the power of technology to connect, transform and future-proof business.

The company's value-driven approach and proven execution capability reinforce its position as one of the top ICT players in the market.

Datacentrix has a broad African footprint and presence in the Middle East.

Datacentrix marketing
Elzette du Preez
edupreez@datacentrix.co.za

Editing and design
SMart Strategic Marketing
santa@smart-sm.co.za
monique@smart-sm.co.za

We would like to thank our technology partners for their support and input into this issue:

HPE
Teraco
Veritas Technologies

Message from the CEO

While South Africa faces ongoing challenges and economic headwinds, the success achieved in the Rugby World Cup 2023 has brought with it hope, unity and national pride amongst its citizens. Through this win, our team demonstrated the power of collective strength, combined support and belief to overcome and triumph in the face of the strongest opposition. It also uncovered the success that can be achieved when we focus on harnessing the strength of our diversity, instead of placing emphasis on our differences. This is a learning that can play a key role in the unshackling of the downbeat mindset that can lead to a divisive society. We need to seek African solutions to our problems.

Our men in green and gold brought back the magic of possibility, underscoring what can be achieved when a unified approach is applied. It is within this context that Datacentrix is proud to be a part of our vibrant South African story. As such, we'll continue working hard towards achieving our national goal of a brighter future for all South Africans.

Datacentrix is a proudly South African company that is determined to contribute to building capacity in the business environment and in our communities to help mend what can be repaired and bring about social and economic success for all. For Datacentrix, this means that we'll keep contributing to our clients' future goals, be a responsible corporate citizen and have a positive social impact. In partnership with our clients, we support public and private enterprises in their steps towards unlocking the full potential of emerging technologies and business opportunities to drive growth.

We believe that the future of South Africa will be determined through education and sustainable transformation. The efforts around creating direct employment prospects, supporting the growth of smaller local businesses, enabling the training and mentoring of individuals, and building employment equity need to be consistent to fast track progress. Some of our endeavours include:

Empowerment: Datacentrix has maintained its level one broad-based black economic empowerment (B-BBEE) rating for the seventh consecutive year in 2023, achieving a total score of just over 127 out of a possible 130 points on its most recent scorecard – one of the highest for the local industry.

> “
>
> It is within this context that Datacentrix is proud to be a part of our vibrant South African story. As such, we'll continue working hard towards achieving our national goal of a brighter future for all South Africans.

Enterprise development: Datacentrix has engaged with a national footprint of vetted SMMEs as part of its delivery strategy. Many of these partnerships span more than 20 years with most of these SMMEs having successfully navigated a path that has allowed them to grow in both revenue and staff complement. Several partners have transformed from exempted micro enterprises (EMEs) to qualifying small enterprises (QSEs), and some have exceeded revenue of R50 million per year, underlining the business growth achieved. This type of development is vital for stimulating South Africa's economy.

Skills development: Datacentrix has shown long-term commitment to supporting learners and graduates. The organisation established its learnership and internship programmes in 2008, welcoming hundreds of learners and graduate interns into the programmes with the aim of combining theoretical knowledge with on-the-job skills training. The company has spent over R8 million on training during the past financial year alone and continues to prioritise skills development in pursuit of its educational transformation goals.

Continues on page 3

Message from the CEO continued

Employment equity: While we recognise more work is required, Datacentrix has long recognised the importance of levelling the playing field and reducing inequality within the workplace. The company has achieved employment equity of 70 percent, showing significant progress in this area.

Youth development: In one of our youth development initiatives, Datacentrix has contributed ICT network infrastructure installation services and expertise in support of the Greater Alexandra Chamber of Commerce (GALXCOC) Digital Hub and Township Incubator, which launched in 2022. The project provides digital start-ups with the support needed to succeed. Datacentrix also supports the hub with linkage opportunities through its supplier development and learnership programmes.

> “We believe that real change is possible when we work together and are cognisant of the significant contribution that our customers, partners and teams make to our success. As we approach the end of the calendar year, we would like to take this opportunity to express our humble and sincere gratitude.

Sustainability: Datacentrix acknowledges that it plays an increasingly significant role in sustainable development by investing in practices that reduce environmental impact, such as secure e-waste disposal, environmentally-friendly IT production, and a preference for low-power devices. These initiatives, while benefitting the environment, also boost the company's corporate reputation, accountability and waste reduction.

From a business perspective, Datacentrix has continued investing in capability to adapt to a changing technology landscape. Datacentrix has expanded its investment and capability in our localised cloud infrastructure to assist customers in reducing cost and addressing data centre residency concerns. In addition, we provide our clients with technical support to manage the exponential growth in cloud costs. This strategy, where possible, seeks to stimulate local growth instead of offshoring capability.

Datacentrix has also made further investment in the digital space to assist our customers on their application journeys. We understand the need for our customers to futureproof their businesses and to ensure that digital transformation delivers real business value. These investments are directed at ensuring that we respond effectively to our customers' real business challenges.

We believe that real change is possible when we work together and are cognisant of the significant contribution that our customers, partners and teams make to our success. As we approach the end of the calendar year, we would like to take this opportunity to express our humble and sincere gratitude.

On behalf of the entire Datacentrix team, I wish you and your loved ones a safe and relaxing festive season and trust that our partnership will continue to deliver value and grow from strength to strength.

We look forward to continuing our partnership with you along South Africa's journey to a brighter tomorrow.

Serious about performance, passionate about South Africa, and continuing to add value. Happy Holidays!

Ahmed Mahomed
CEO

Datacentrix reinforces commitment to sustainability with HP Amplify Impact Partner recertification

Elizabeth Naidoo
Datacentrix
Chief Financial and Risk Officer

Datacentrix is pleased to have achieved recertification as an HP Amplify Impact Partner. A programme that is centred on climate action, human rights and digital equality, this partnership status underscores Datacentrix's unwavering dedication to sustainability, environmental responsibility, and its continued collaboration with HP.

“Our position as an HP Amplify Impact Partner reaffirms Datacentrix's commitment to sustainable business practices and aligns with our vision for a more environmentally responsible future,” explains Datacentrix Chief Financial and Risk Officer, Elizabeth Naidoo. “Through this type of partnership, HP aims to drive change within the technology sector, promoting eco-friendly solutions and responsible business practices. And, as an HP Amplify Impact Partner, Datacentrix continues to work closely with the organisation to integrate sustainable technologies and practices into its product and service offerings.”

Datacentrix's sustainability practice focuses on reducing any negative environmental impact resulting from its operations, with an emphasis on the impact of climate change and also social inequality, adds Naidoo. The organisation uses the United Nation's 17 Sustainable Development Goals (SDGs) as a guideline, in particular those around good health and well-being; gender equality; decent work and economic growth; industry, innovation and infrastructure; and responsible consumption and production.

“As such, Datacentrix has invested in practices that reduce environmental impact, such as secure e-waste disposal, environmentally-friendly IT production, and low-power device preference, but will also continue to focus on strategic initiatives and set goals,” she continues.

Importantly, in addition to reducing the environmental impact of its products and services, Datacentrix places a strong emphasis on community engagement, education and corporate social responsibility.

“We are not only committed to delivering business value to our clients through cutting-edge technology, but also do so in a manner that is environmentally responsible and has a positive impact on society," adds Naidoo. "By being recertified as an HP Amplify Impact Partner, we are taking significant steps toward a more sustainable future."

Artificial intelligence, blockchain and other technologies contributing to the future of local agriculture

Innovative technologies, including blockchain, artificial intelligence (AI), drones and more, will continue to pave the way for growth within the local agricultural sector, while playing a critical role in helping to alleviate global challenges such as food security and wastage.

This was the central theme at the fifth Agri Indaba, hosted by Datacentrix in Limpopo.

In his welcoming address, Ahmed Mahomed, Datacentrix CEO noted that the South African agricultural sector has shown a remarkable performance, despite inhibiting factors such as load shedding, rising inflation and the global economic slowdown, providing food to approximately 60.6 million citizens (and several million other residents) as well as to every country within Africa, with the exception of the Cape Verde Islands and Eritrea.

Dr Tebogo Sethibe Group Executive at the Agricultural Research Council

"South African agriculture exported $12.8 billion in agricultural products last year, roughly half of its annual produce, and we believe that this can be even better supported by smart, data-driven farms and their improved efficiencies. This type of environment could potentially encompass solutions such as data management, AI, machine learning (ML), internet-based solutions, mobile technologies, drone-based applications and automation."

AI to play a key role in ending world hunger

2023 has been another year of extreme jeopardy for those struggling to feed their families, said 'human-centred AI advocate' and thought leader, Johan Steyn, who explained during his Agri Indaba keynote address that, according to data from the World Food Programme, 783 million people worldwide are uncertain of where their next meal is coming from.

"The global community must not fail on its promise to help end world hunger and malnutrition by 2023," he stated, adding that technological agriculture could be a game changer for Africa, as well as for the rest of the developing world.

"It is interesting to note that some of the most prominent voices on AI and technology have not been technologists, but historians and philosophers. Israeli author and historian Yuval Noah Harari, for instance, has said that the world is facing

Ahmed Mahomed
Datacentrix CEO

> South African agriculture exported $12.8 billion in agricultural products last year, roughly half of its annual produce, and we believe that this can be even better supported by smart, data-driven farms and their improved efficiencies.

three existential problems: nuclear war, ecological disaster, and AI," added Steyn. "However, for the agriculture sector, AI could help to improve malnourishment and hunger in the world. This could range from precision farming, where data from drones, satellites and ground sensors can be used for better predictions, reduced waste and improved crop yields; earlier detection of pests or crop disease; the use of AI-equipped machinery for faster planting and harvesting; and the streamlining of the agricultural supply chain to speed up produce reaching the market, thereby limiting food wastage.

But AI doesn't come without its challenges

Steyn suggested that, for industry to retain control over AI, both the regulatory environment and AI skills challenges need to be overcome. There are no regulations that govern AI in Africa, or globally for that matter; and the lack of technical skills and expertise is fuelled by skills migration that is prominent in South Africa specifically.

Furthermore, in order to prevent costly mistakes, he advises local agri-businesses to leverage the power of AI through critical partnerships with companies like Datacentrix, where past learnings and experiences contribute to stronger IP, rather than attempting to go the AI journey alone.

"It's important that agri-businesses embark on their AI journeys by looking at business problems, and focusing on financial returns and business longevity. Here, the modern agri-business leader needs to find the balance between human and technology collaboration by establishing a human strategy that is supported by AI and other technological interventions.

Blockchain bolsters broken food chain

Dr Tebogo Sethibe, Group Executive at the Agricultural Research Council (ARC), added blockchain technology to the Agri Indaba discussion, saying that, from a food security point of view, this type of solution is already being successfully used to rectify broken food chain challenges such as contamination and consumer demand for greater transparency within the food industry.

"Blockchain has the ability to hold the history of food items through the entire supply chain; from farm to fork. Its end-to-end traceability means that all players in the chain have access to the same information at the same time, helping to save time, decrease cost, reduce risk and also increase trust."

In conclusion, Steyn commented that "technology can revolutionise business, but we must not lose sight of why we are doing this. It is to ensure a sustainable future for our children, with the promise of nourishment and prosperity, by using technology responsibly."

The Datacentrix Agri Indaba 2023 was supported by the participating technology partners, including Platinum Partner, Veritas, and Gold Partners eNetworks, Fortinet (Exclusive Networks), Hewlett Packard Enterprise (HPE), HPE Aruba, ManageEngine (ITR Technology), and VMware.

For more information on the Datacentrix Agri Indaba 2023, please visit www.datacentrix.co.za/agri_indaba_2023.html

Datacentrix appointed as first local Rubrik Elite Partner

Datacentrix has achieved Elite Partner status with Zero Trust Data Security company Rubrik – the first of a handful of local partners to reach this category in South Africa.

According to Shawn Marx, Business Unit Manager: Converged Solutions at Datacentrix, the company has seen impressive growth with Rubrik over the last financial year, signing on a number of new clients during this period.

"Since becoming a Rubrik Authorised Partner around 18 months ago, we've worked closely with the organisation to make a positive impact within the cybersecurity, ransomware recovery and data protection space for local businesses," he clarifies. "In addition, Datacentrix has been named as a local services partner for Rubrik during this time, meaning that we are also able to implement these solutions for our clients."

Bassam Almasri, Rubrik's Director of Channel and Alliances for EMEA Emerging Markets, explains that the Elite Partner status is the second level of Rubrik's Transform Partner Programme.

"Following Authorised Partner status, partners must accumulate a certain number of points to become an Elite Partner," he outlines. "This is based not only on revenue, but also on training and accreditations, joint sales and marketing activities, and lead generation.

"I would like to congratulate Datacentrix on becoming an Elite Rubrik partner. We have established a brilliant working relationship, not only winning new business together, but also building a healthy lead pipeline.

"South Africa is a highly strategic region for Rubrik, and our success here has been underscored with the growth of our local team, which has expanded from one sales account manager two years ago, to a full team on the ground. And there is great potential for us moving into the future, in particular with Datacentrix."

Almasri adds that Rubrik also recently identified Datacentrix as a Rubrik strategic business partner in South Africa, building investment in the partnership to develop business penetration. "Rubrik is selective when it comes to appointing Business Partners. We have worked closely with Datacentrix through joint roadshows, client meetings and the identification of shared opportunities."

"Rubrik has placed serious focus on building its business in South Africa, and the fortification of local resources, as well as the appointment of a second local reseller, are indicative of this investment. We look forward to continuing to develop this partnership into the future," Marx concludes.

Bassam Almasri Director of Channel and Alliances for EMEA Emerging Markets at Rubrik

"

Rubrik also recently identified Datacentrix as a Rubrik strategic business partner in South Africa, building investment in the partnership to develop business penetration.

Datacentrix retains level one B-BBEE rating for seventh year, celebrates continued transformation

Kenny Nkosi, Datacentrix's Divisional Managing Director: Public Sector and Commercial Sales and Chairperson of the Employment Equity Committee

Datacentrix is pleased to announce that it has maintained its level one broad-based black economic empowerment (B-BBEE) rating for the seventh consecutive year, achieving a total score of just over 127 out of a possible 130 points on its most recent scorecard – one of the highest for the local industry.

According to Datacentrix Chief Financial and Risk Officer, Elizabeth Naidoo, the organisation's consistent approach to transformation has been a critical factor in this achievement. "For Datacentrix, the topic of transformation – and sustained transformation most importantly – is very close to our hearts."

Kenny Nkosi, Datacentrix's Divisional Managing Director: Public Sector and Commercial Sales and Chairperson of the Employment Equity Committee says: "Based on our current economic climate, the only way that we will be able to build South Africa into the powerhouse it has the potential to be, is to ensure that this type of positive change is ongoing. And this is through sustained efforts around creating direct employment opportunities, supporting the growth of smaller local businesses, enabling the training and mentoring of individuals, building employment equity, and more."

Nkosi notes with pride that the engagement of SMME partners is an important accomplishment for Datacentrix. "Datacentrix has engaged with many SMMEs over time, with some partnerships spanning more than 20 years. We have seen several partners transform from exempted micro enterprises (EMEs) to qualifying small enterprises (QSEs) – or even generic entities with revenue exceeding R50 million per year in some cases – which is a significant achievement in terms of business growth.

"Most of these companies have successfully navigated a path that has allowed them to grow in both revenue and staff complement. As an excellent example, one of our SMME partners that has engaged with Datacentrix since 2008 has grown their revenue by approximately 295 percent over the past 15 years. This type of development is vital to stimulating South Africa's economy and ensuring that it grows and thrives."

When it comes to skills development, Datacentrix has shown long-term commitment to supporting learners and graduates. The organisation established its learnership and internship programmes in 2008, welcoming hundreds of learners and graduate interns into the programmes with the aim of combining theoretical knowledge with on-the-job skills training. Most recently, the company instituted a bursary scheme with Wits University, and has already seen two of its graduates join the workforce to start their formal workplace training.

Datacentrix spent over R8 million on training during the past financial year, a praiseworthy achievement in upskilling initiatives, adds Naidoo. Datacentrix continues to prioritise skills development in pursuit of its educational transformation goals.

Nkosi further points out that: "Employment equity is another area on which Datacentrix has been assiduously focused over time, and our positive work here is apparent. Our most recent B-BBEE verification certificate shows employment equity of 70 percent, indicating significant progress in this area since our 59 percent score in 2020."

"Datacentrix has long recognised the importance of levelling the playing field and reducing inequality within the workplace, and so has placed long-term commitment to its development initiatives," Naidoo concludes.

Datacentrix bags two Lenovo Intelligent Devices Group (IDG) awards, named IDG Platinum Partner of the Year

Datacentrix has received two prestigious awards at the Lenovo Channel Awards for 2022, namely the Intelligent Devices Group (IDG) Relationship Partner of the Year and the IDG Platinum Partner of the Year, demonstrating the organisation's continued commitment to its strategic partnership with Lenovo.

Datacentrix is a Tier 1 Platinum Partner for Lenovo's Infrastructure Solutions Group (ISG), as well as for the IDG side of the business.

According to Anle Els, End User Computing (EUC) Product Manager at Datacentrix, it was Datacentrix's long-standing relationships with local customers that helped clinch the IDG Relationship Partner of the Year award.

“Several years post-pandemic, many South African businesses have had to refocus on their computing requirements once again, as end user devices have reached the end of their three-year cycle. Likewise, organisations upgrading from Windows 10 to Windows 11 need to ensure that their hardware meets the new system requirements.

“Datacentrix's mature technology and service offering has allowed it to extend its ongoing partnerships with clients to help them meet these changing needs.”

These strong, successful client relationships also played a role in Datacentrix's acknowledgement as Lenovo's IDG Platinum Partner of the Year.

“As one of only a handful of Lenovo Platinum Partners locally, Datacentrix demonstrated its continued commitment to its local customer base as well as a strong focus on its relationship with Lenovo,” Els continues. “And by achieving the highest revenue figures of all local Platinum Partners for the 2022 period, it's clear that this is a winning formula,” she adds. “Lenovo is a highly strategic brand for Datacentrix, and this will certainly remain the case moving forward.”

Werner Schoeman, Relationship Sales Lead, Lenovo Southern Africa says: "We congratulate Datacentrix on their well-deserved recognition as the IDG Relationship Partner of the Year and IDG Platinum Partner of the Year at the Lenovo Channel Awards for 2022. Their commitment to excellence and long-standing relationships with local customers truly set them apart. Datacentrix's expertise in navigating the evolving landscape of end user computing is commendable. We are proud to have them as one of our esteemed Platinum Partners, and we look forward to continued success together in the future."

Werner Schoeman, Relationship Sales Lead, Lenovo South Africa, Yugen Naidoo, Lenovo Country Manager, Anle Els, End User Computing Product Manager at Datacentrix and Dean Wolson, ISG Country Manager, Lenovo

Teraco releases second annual Sustainability Report

With the publication of its second annual Sustainability Report, Teraco reveals sustained progress towards its environmental goals.

The 2023 Sustainability Report demonstrates notable progress towards the company's Environmental, Social and Governance (ESG) goals across its seven operational facilities in South Africa.

Teraco has committed to powering its data centre colocation facilities with 50% renewable energy by 2027 and 100% by 2035. It will also maximise its combined rooftop solar footprint across its facilities to 6MW by the end of 2023, which equates to 83 000MWh in energy savings.

Furthermore, Teraco aims to mitigate more than 8 500 tonnes of CO_2 by the end of 2023 and has committed to diverting zero waste to landfill by 2028.

Alongside the impact made through sustainable building and renewable energy sourcing initiatives, Teraco raised a R1.5 billion green loan in 2022 to be applied towards its 200MW utility scale solar programme.

"The climate crisis, sustainability, diversity, inclusion, and positive impacts on our community are some of the most critical issues facing society today," says Jan Hnizdo, CEO at Teraco. "How we respond to these challenges as a business is something we take extremely seriously.

"Solving them requires ambitious thinking and progressive action from governments, businesses, and consumers. For example, harnessing the power of data can help us innovate and scale the technologies required to deliver a sustainable environment for future generations. As data centres have become pivotal to the global digital economy, we have a responsibility to act. We are proud of the work we're doing in this area and know we need to do more, and accelerate our efforts across the sustainability agenda.

"As we expand our reach, we remain committed to leading the industry in sustainable environmental performance and being a responsible partner to our clients," he adds.

50%
renewable energy by 2027

100%
renewable energy by 2035

6MW
roof solar deployed by the end of 2023

8500
tonnes of CO_2 mitigated by the end of 2023

To read more about Teraco's sustainability goals, please visit www.teraco.co.za/about/sustainability/

TERACO®
A DIGITAL REALTY COMPANY

Email security remains critical for organisations' cyber security practices as threat actors embrace AI

E-mail compromise still accounts for around 90 percent of breaches that occur within business on a daily basis, something that, in most instances, can be blamed on user error.

"New and evolving threats are landing in users' mailboxes daily, particularly within the hybrid workforce context, often using phishing campaigns that rely on clever techniques and panic to get users to click on links and share credentials or sensitive information, such as banking details," explains Gideon Viljoen, Pre-Sales Specialist: ICT Security at Datacentrix.

"US wireless network operator Verizon confirms in its Data Breach Investigations Report 2023 that 74 percent of data breaches (three out of four) involve a human element, with people being involved either via error, privilege misuse, use of stolen credentials or social engineering."

Social engineering is a lucrative tactic for cyber criminals, the report says, especially given the rise of those techniques being used to impersonate enterprise employees for financial gain, an attack known as business e-mail compromise (BEC).

The median amount stolen in BECs, it reveals, has increased over the last few years to $50,000 USD, based on Internet Crime Complaint Center (IC3) data, which might have contributed to pretexting incidents – a specific type of social engineering attack – nearly doubling this past year. With the growth of BEC, enterprises with distributed workforces face a challenge that takes on greater importance: creating and strictly enforcing human-centric security best practices.

Fighting fire with fire: User training and next-gen technology essential

"With a rapidly evolving landscape, changing attack strategies and new compromise techniques being introduced daily, it is imperative that users are trained and kept up to date on the latest campaigns and techniques being used," says Viljoen.

"This is the most effective way of ensuring a more secure environment, with users acting as a 'human firewall' for organisations, and being able to spot, report and block compromise attempts. User awareness training is an excellent proactive option to assist e-mail gateway administrators and engineers in staying on top of campaigns and potential breaches.

"And further to this, a collaborative workforce between machines and humans is key to successfully stem the attack on organisations, with the use of AI (artificial intelligence) additionally providing a smarter, faster approach to protecting against e-mail phishing and breaches.

"AI is being used increasingly to run phishing campaigns and information collection, doing the heavy lifting on behalf of threat actors. A good example of this is how AI-powered chatbot, ChatGPT, has been used to help less-skilled cyber criminals to write malware and launch cyber attacks.

"So, having a technology in place to combat this is a necessity, and businesses cannot rely on a human alone to be able to administer and catch these threats."

IBM's recently launched Cost of a Data Breach Report corroborates this statement, affirming that AI and automation have had the biggest impact on speed of breach identification and containment for studied organisations. The report says businesses making extensive use of both AI and automation experienced a data breach life cycle 108 days shorter than those companies that had not deployed these technologies (214 days versus 322 days).

According to the 2023 report, the incident costs shouldered by those organisations that were using AI and automation were significantly lower; on average, nearly $1.8 million lower data breach costs than organisations that didn't deploy these.

How to protect business e-mail

The best starting point for a business's e-mail security, according to Viljoen, is to invest in an e-mail gateway solution.

"In fact, Datacentrix's recommendation is that organisations implement an e-mail gateway solution as a first priority before looking at any other security product."

With several toolsets available on the market, finding the best fit for your organisation is key, Viljoen clarifies. "There are full enterprise solutions, as well as small-to-medium business e-mail offerings available to provide a secure e-mail environment. These solutions offer reactive, real-time and proactive response solutions to secure the gateway."

They also encompass a variety of functionalities that address the diverse aspects of an e-mail gateway, namely:

- Spam filtering and blocking;
- Stationery (e-mail signatures and campaigns);
- Anti-phishing (known bad threat actors);
- Sandboxing ('detonation' of suspicious e-mails found);
- Zero day protection (behavioural or unknown/untrusted e-mail domain);
- Data leak prevention (internal and external sharing of sensitive information);
- E-mail blocking (verification, blacklisting, whitelisting); and
- User awareness training and campaigns (helping users to keep up with phishing techniques and how to defend against those).

Ensuring the gateway is configured and maintained from the start is critical, with the requirement that a specialist, either an internal engineer or an expert managed services provider, enforces the policies and rules and maintains best practice standards.

> "This is the most effective way of ensuring a more secure environment, with users acting as a 'human firewall' for organisations, and being able to spot, report and block compromise attempts. User awareness training is an excellent proactive option to assist e-mail gateway administrators and engineers in staying on top of campaigns and potential breaches.

"Once you have the right technology in place and capabilities are procured and enabled within the organisation, the next step is to see that the policies and rule sets are updated, checked and verified in a cost-effective way to ensure losses are minimised. Running best practice assessments on policies and rules on a frequent basis is also vital to ensure a secure gateway.

"Finally, it is critical to utilise tools, such as pen testing and auditing, to ensure that the environment is hardened and stringently tested at frequent intervals."

Do we need another cloud?

By Jaap Scholten, Head: Group Hybrid ICT Strategy at Datacentrix, and Chief Operating Officer of eNetworks, a Datacentrix company

Amazon Web Services launched its cloud services in 2006, followed shortly by Microsoft's Azure offering in 2010. Three years later, the word 'hyperscaler' entered our lexicon – meaning large cloud service providers that can provide offerings such as computing and storage at enterprise scale – and #CloudFirst became the buzzword amongst everyone, from developer to chief information security officer (CISO).

Systems integrators were unsure how to measure the potential threat of cloud business, compared to traditional hardware and infrastructure sales. However, the groundswell of cloud adoption was not to be ignored, despite raising so many questions.

Business benefits and costs under the spotlight

One of the biggest shifts in executive think-tanks centred around ICT results versus business outcomes. Spurred on by the Covid-19 pandemic, cost-saving efforts were being applied at all levels of the business, and ICT – known for its ever-increasing price/performance indexes – was put under the spotlight as an easy target for cost saving.

The question being asked was how a cloud-first strategy would align to business outcomes: was this a pure-play in technological evolution, which would only benefit the new economy – the Ubers and Airbnbs of this world? And would the cost of modernising mainstream businesses into a cloud-first era outweigh the benefit?

Early results posed questions

After witnessing the mass-migration of numerous large customer workloads, the first rounds of feedback were not as euphoric as the technologists had hoped for. More questions were raised, and yet another word entered our vocabulary: 'bill-shock'.

“

One of the biggest shifts in executive think-tanks centred around ICT results versus business outcomes. Spurred on by the COVID-19 pandemic, cost-saving efforts were being applied at all levels of the business, and ICT – known for its ever-increasing price/performance indexes – was put under the spotlight as an easy target for cost saving.

Compliance officers also raised concerns over the sovereignty of company data. Patient records, student marks, financial information and intellectual property ... where exactly was all of this data being hosted? And why do organisations have to pay to retrieve their own records?

As the dust settled, customers began moving some workloads back, in an attempt to regain control, both financially and in terms of compliance. A serious re-think of the cloud-first strategy was required.

Dollar-based billing resulted in IT budgets experiencing unprecedented cost increases, without realising any associated operational benefit. The cost of extracting data, as well as the compliance issues around data sovereignty, rapidly led to a new approach. Given that almost all of an organisation's records – customer, supplier, product and financial records, applying to entities both large and small – now lived as data somewhere, it became paramount to place data at the centre of such a strategy.

And so, the #DataFirst concept was born.

New solutions, better results: 'Data First'

A healthy data-first approach results in a strategy that supports the fundamentals of where data is hosted, how it is transported, and how it is secured. These underlying principles must be supported by a 360-degree approach, encompassing assessment, implementation, support, modernisation and continued gap analysis to assess the strategy's execution progress. Ultimately, a data-first strategy is aligned to business outcomes and outperforms a pure ICT strategy.

Systems integrators started building smaller private/public clouds, hosted in sustainable data centres where power is guaranteed, with easily accessible sub-millisecond onramp paths and high levels of physical and cybersecurity, while addressing Rand-based billing and locally-based data sovereignty. These clouds offer organisations Infrastructure as a Service (IaaS) as well as Platform as a Service (PaaS) options, which often mean a happy home for many applications that are not hyperscaler native.

With multiple availability zones, users of these services address their disaster recovery needs and can start to realise large-scale, long-term savings compared to their pure hyperscaler or on-premises deployments. Systems integrators and cloud providers tend to concentrate top skills in these areas, thereby providing their customers with innovation, strategy, financial modelling and managed services all year long, while the customer can focus on their core business.

Multi-cloud adoption between different providers has proven to be both cost-effective and risk averse, now that multi-cloud management tools are readily available – even 'as a Service' – simplifying cost management, reporting engines, and optimisation efforts. Tools ensure that business outcomes are enhanced and realised.

As to the question “do we need another cloud”, the answer is therefore a resounding “yes!” – and there will be many more clouds to follow, almost moving into the boutique-genre of clouds designed for specific classes of workloads.

For more information on Datacentrix's Hybrid ICT approach, which encompasses a data-first strategy, please visit https://www.datacentrix.co.za/hybridit.html

Jaap Scholten, Head: Group Hybrid ICT Strategy at Datacentrix

“Multi-cloud adoption between different providers has proven to be both cost-effective and risk averse, now that multi-cloud management tools are readily available – even 'as a Service' – simplifying cost management, reporting engines, and optimisation efforts. Tools ensure that business outcomes are enhanced and realised.

Steps to build a more inclusive, skilled workforce

The local technology skills shortage has been well documented over time, with recent statistics underscoring not only a dearth of technical expertise in South Africa, but also a concerning youth unemployment rate.

New figures from Statista show a staggering number of unemployed youth (15 to 24 years), reaching 60.7 percent in the second quarter of 2023. Statista further noted higher unemployment rates for women than men since the start of 2016, measured at almost 36 percent in the second quarter of 2023, as opposed to 30 percent respectively.

From a technology point of view, a report released earlier this year by SAP Africa, called 'Africa's Tech Skills Scarcity Revealed', disclosed that three-quarters of the South African, Kenyan and Nigerian organisations surveyed reported negative effects from a lack of technical skills; including struggling to meet client needs (46 percent), reduced capacity for innovation (53 percent), and losing customers to competitors (60 percent).

According to the report, a top skills challenge for African organisations is attracting skilled new recruits, although in South Africa the retention of experienced employees was first on the list. It further noted the most in-demand skills as being cybersecurity and data analytics (63 percent); developer and industry skills (49 percent); and digital transformation skills (48 percent).

Skills development and mentoring play an essential role

"It's true that we're facing many challenges in the local technology sector, but there are measures that private industry can – and should – put in place that can contribute to the alleviation of both unemployment and the lack of technology skills," explains Charmaine Koffman, Head of Human Resources at Datacentrix.

"Datacentrix's stance on skills development is well entrenched and we have several initiatives to support this, including our graduate programme, which has been running for 18 years. This initiative places an emphasis on cross-functional training, encouraging the outcome of multi-skilled individuals with experience across more than one specialised area of technology, as well as more business-focused capabilities.

"This initiative places an emphasis on cross-functional training, encouraging the outcome of multi-skilled individuals with experience across more than one specialised area of technology, as well as more business-focused capabilities.

Charmaine Koffman, Head of Human Resources at Datacentrix

"Our graduate and learnership programmes have a strong focus on mentoring, as well as the development of personal skills such as work ethics, something that is a core value at Datacentrix. We're proud to have a high absorption rate of these learners and graduates at Datacentrix, as we want to be able to retain these talented young people.

"Mentoring plays a pivotal role in African skills development, regardless of industry, by providing the guidance, support and knowledge transfer needed to empower our workforce, as well as fostering innovation and bridging the gap between education and real-world industry requirements. Datacentrix actively encourages other local businesses to join us in mentoring local learners and graduates, further strengthening the foundation of skilled professionals across the continent," she adds.

"Across the industry, we're currently seeing the continuous movement of resources, especially at entry level, rather than within mid or senior management. It's a highly competitive market, but we're also seeing that a number of organisations are putting forward above-market-rate offers that are simply not sustainable over time."

Koffman cautions those individuals looking at new prospects to undergo their due diligence before accepting an offer that might well be too good to be true. "It's essential to remember that genuine career growth and job satisfaction often come from realistic and maintainable environments. Therefore, my advice would be for people to scrutinise job offers before accepting them – research the company thoroughly and seek guidance where necessary. Sometimes it's not just about finding a job; it's about building a meaningful and fulfilling career that aligns with your long-term goals and values."

Closing the gender gap

Datacentrix recently instituted a bursary scheme with Wits University and has already seen two of its graduates join the workforce to start their formal workplace training. This is one of the areas, says Koffman, that the company is using to support gender diversity within the ICT sector.

"There is a serious need for local businesses to implement targeted recruitment strategies to address the gender diversity challenge. Datacentrix is working hard towards an optimistic 50/50 gender split by the end of next year. In addition, it is critical to attract more young women to embark on STEM careers, like ICT and engineering, as we need to improve this diversity moving forward."

Koffman maintains that the key to inspiring more women to join the sector, as well as addressing the broader technology skills shortage in the longer term, is for organisations to nurture an interest in STEM careers at foundational level.

"We need to make an immense effort to turn around the pressing issue of the technology skills shortage, addressing this challenge at root level – earlier than grade 8 at school – to create a skilled workforce for the future. This will help to ensure that individuals from all backgrounds have access to educational and career opportunities in the technology sector, fostering a more inclusive skills pool.

"Datacentrix is committed to being part of this transformative journey, and we encourage other businesses to join us in this essential endeavour, building a brighter and more technologically advanced future for Africa," she concludes.

ADVERTORIAL

VERITAS

Artificial Intelligence: A great power that requires greater responsibility

By Johnny Karam, Managing Director & Vice President of International Emerging Region, Veritas Technologies

The rise of Artificial Intelligence (AI) powered chatbots has been evident in recent years, with organisations both public and private, implementing conversational AI software to serve a variety of purposes, including for customer experiences and support, as well as internal helpdesk and troubleshooting services. These AI solutions are effective in reducing the burden on customer services, filtering IT support needs and lowering call centre costs. Yet, many of the solutions are limited in their capabilities and can only address a narrow scope of use cases.

As a result, forward-thinking organisations are exploring the use of AI in a more advanced way by embracing the capabilities of general-purpose large language models (LLMs). The emergence of ChatGPT, an LLM trained by OpenAI, has given rise to a new-found realisation among organisations and individuals regarding a range of applications and use cases. Unlike traditional chatbots, ChatGPT can support a variety of purposes, such as writing code, drawing insights from research text, or creating marketing materials such as website copy and product brochures. These services can also be accessed through APIs, which allow organisations to integrate the capabilities of publicly available LLMs into their own apps, products and in-house services based on their particular needs. Adopting tools such as ChatGPT can help organisations change their processes, enhance their efficiencies, gain a competitive edge, and reduce manual requirements, thereby increasing their revenue. Used effectively, they can also help elevate employee capabilities by providing access to resources that were previously unavailable, enhancing an individual's skills set.

Johnny Karam, Managing Director & Vice President of International Emerging Region, Veritas Technologies

Balancing innovation and responsibility: Data management considerations around the use of AI for business

The pace of progress in the AI space is adding pressure on decision makers in terms of how these advancements fit into their existing data management strategy. As the implementation of AI in business processes becomes increasingly common, it brings a range of considerations over potential risks.

It is common to see organisations rush to implement emerging technologies like ChatGPT, only to realise the limitations after some time. When integrating AI into business processes, organisations will typically gather data not only from online sources but also from their own data – potentially including sensitive company information and IP – to train the AI. This creates significant security implications for organisations that become dependent on these AI-enabled processes without the proper frameworks in place to keep that information safe.

Any organisation interacting with these services must ensure that data used for AI purposes is subject to the same principles and safeguards around security, privacy, and governance as data used for other business purposes.

Many are already alerted to the potential dangers. Take for instance Amazon, who recently issued a warning to their employees about ChatGPT. Amazon employees were using ChatGPT to support engineering and research purposes. However, a corporate attorney at Amazon warned employees against it after seeing the AI mimic internal confidential Amazon data.

Organisations must also consider how to ensure the integrity of any data processes that leverage AI and how to secure the data in the event of a data centre outage or a ransomware attack. They must consider the data they feed into the AI engine and its status, as not all information produced by AI is accurate. Moreover, they must ask themselves how they will protect the data produced by AI, ensuring that it complies with local legislation and regulations, and is not at risk of falling into the wrong hands.

A broader consideration is what these developments in AI mean from a security perspective. The tools will be adopted not only for productive use cases but also by bad actors, who will seek to apply the technology to increase the scale and sophistication of the cyberattacks they conduct. It is imperative for organisations to recognise the potential harm that AI can cause to their operations and take the necessary steps to protect themselves from cyberattacks and data breaches.

Safeguarding your data infrastructure against cyber threats

While the true potential of AI is yet to be discovered, we know that its applications will be highly data-intensive, creating the need for enterprises to manage it efficiently and responsibly. An organisation's AI strategy will be a regular and seamless part of its overall data management strategy.

And when utilised in the right way, the opportunities are endless. For instance, it will use AI to conduct simulations that study the changes and impacts of new policies and legislation, predict results of different scenarios, evaluate the effectiveness of programmes, and support complex decision making.

Considered use of emerging technologies like AI has the power to change lives – it can transform consumer experiences, help governments make more informed decisions, accelerate scientific discovery, improve the delivery of more personalised healthcare services and so much more.

Ensuring the secure and compliant use of AI data, safeguarding against cost risks and cybersecurity threats can become overwhelming to those who don't have the right platform in place to help them safely harness new technologies. By working with a trusted provider to mitigate against the risks of AI, orgainsations can unlock the full potential of these emerging technologies to drive immense growth and innovation.

How to mitigate (and recover from) rising African cyber incidents

By Brian Smith, Business Unit Manager: Managed Services at Datacentrix

There's no question that African businesses are being increasingly targeted by cyberattacks, with ransomware, spyware and backdoor incidents, as well as data leaks, becoming ever more prevalent.

One such recent example is the Distributed Denial of Service (DDoS) attacks on Kenyan and Nigerian organisations by 'hacktivist' Anonymous Sudan during July and August this year.

According to a report by cybersecurity company Cloudflare, the original group emerged in Sudan, "in response to the country's ongoing political and economic challenges. They were also known for using digital activism, which includes hacking and DDoS attacks on governments and other high-profile websites, to draw attention to issues such as internet censorship".

Anonymous Sudan launched DDoS attacks against countries such as Sweden, Denmark and the US in early 2022 that continued into this year, with the group announcing that it would target the US and European financial sector in mid-June. From the end of July, Kenyan organisations were under siege, and a number of businesses within the country such as banks, media, hospitals, universities and other companies were all reportedly targeted in a days-long DDoS offensive.

The effects of these attacks are far-reaching, says the report, numbering challenges such as service unavailability, loss of revenue, decreased productivity, remediation costs and reputational damage.

How, then, do African businesses take steps to mediate this type of attack, or at least minimise the damage wreaked by cybercriminals? The answer is to ensure that the right strategic steps are in place.

Setting up an incident response plan

An excellent starting point is having an incident response plan in place; a formal, written document that is approved by senior management, providing a set of instructions for organisations to detect, respond to and recover from a cyber incident.

Should an attack take place, the business would then consult its incident response plan and take the recommended steps. For example, Datacentrix's incident response plan follows several stages:

1. The first, once the plan is invoked in the case of a cybersecurity incident, is to alert all responsible people within the business, including the governance and risk officer, senior management and executives.
2. The next step is to put together a team of security experts from the Datacentrix Security Operations Centre (SOC), which would encompass members from within different disciplines of cybersecurity.
3. Datacentrix would then open a 'war room', incorporating all its technical cybersecurity experts, who are tasked with investigating the attack, devising what needs to be done from a mitigation perspective, and carrying out the necessary measures.
4. All stakeholders would be kept up-to-date with progress during this process.

Ideally, an incident response plan should cater for all types of cyberattack, and whether it be ransomware or a malware attack, for example, the response should always remain the same – at least initially. This means that all members of the technical and operational teams are involved in the early stages, until it is decided how mitigation will be carried out. If different teams are assigned to manage different types of attack, the business runs the risk of losing sight of the bigger cybersecurity picture and could leave itself vulnerable to other types of incidents.

Proactivity is key

Datacentrix's advice is that organisations must not only have an incident response plan in place, but ensure that it is regularly put to the test. This could be carried out through attack simulations (penetration testing) to check for exploitable vulnerabilities, let's say, at least two to four times a year. These exercises will confirm that, as far as possible, all stakeholders and teams involved are ready for a real attack on the business.

In addition, companies must do frequent checks with their security engineering teams to confirm that they have the right security certifications in place.

Another essential exercise is making sure that the business offers ongoing cybersecurity training for end users. This is of paramount importance, considering that more than 80 percent of attacks are caused by human error.

You've been attacked, what next?

It's becoming less and less likely that African businesses will remain unscathed from cyberattacks, so it's important to look at how to recover in the event of an incident.

To begin with, the organisation must look at the type of incident experienced and see how it can then take more effective steps to secure its business systems from similar future attacks.

Again, the company should also look at more effective end user training, as well as raising awareness around its incident response plan with stakeholders, ascertaining what the plan means to the business and how it can be improved.

Businesses that do not have a dedicated internal security team should look for support from an established cybersecurity partner that offers SOC services.

An outsourced SOC delivers the benefits of immediate, 24x7 access to a team of cybersecurity experts as well as the latest advanced technologies, shared threat intelligence, scalability options, and also reduced operational costs.

> “An excellent starting point is having an incident response plan in place; a formal, written document that is approved by senior management, providing a set of instructions for organisations to detect, respond to and recover from a cyber incident.

In addition to the bouquet of powerful, proactive, multi-disciplined cybersecurity measures, an experienced cybersecurity partner will furthermore be able to assist with the establishment of a rock-solid incident response plan and regular simulations and testing scenarios.

For more information on Datacentrix's Security Services offering, visit https://www.datacentrix.co.za/security-services-672943.html

Brian Smith, Business Unit Manager: Managed Services at Datacentrix

Navigating cybersecurity challenges within the African transport and logistics space

The African transport and logistics sector is a rapid adopter of industrial automation, embracing technologies such as the Internet of Things (IoT) and Operational Technologies (OT) to enhance efficiency. However, cautions Ben de Klerk, Eastern Cape Branch Manager at Datacentrix, with these advancements comes a well-documented history of cybersecurity vulnerabilities that still demand attention.

The rapid development and deployment of new technologies are also often associated with limited protocols governing their use, which poses its own set of risks, he explains.

Ben de Klerk, Eastern Cape Branch Manager at Datacentrix

The complex landscape of cybersecurity risk

"The local transport and logistics industry relies heavily on the smooth flow of goods across a complex network of multiple entities; from suppliers and manufacturers to distributors and retailers," De Klerk explains. "This intricate supply chain structure is highly vulnerable to cyberthreats, as attackers can exploit any particular point in the supply chain.

"Moreover, the industry's reliance on IoT and OT devices – such as sensors, GPS trackers and automated control systems – introduces new potential vulnerabilities."

In fact, De Klerk maintains that this is a serious security challenge within the sector, as these sensors often lack robust built-in security features. This vulnerability opens the door to cyberattacks that can disrupt operations, compromise data, and lead to costly downtime, he says.

"Another area of great concern to OT security leaders within the transport and logistics sector is the risk of either unwitting, unaware, or malicious insider threats."

Addressing security challenges

In order to mitigate these risks and bolster cybersecurity, organisations within the transport and logistics sector should look at adopting a comprehensive approach that combines technical, personnel and policy-based measures, De Klerk advises.

Ideally, this should include:

- **Identifying and prioritising assets:** Start by identifying and categorising OT assets based on their importance to the business. This prioritisation helps focus security efforts on critical assets first.

> In order to mitigate these risks and bolster cybersecurity, organisations within the transport and logistics sector should look at adopting a comprehensive approach that combines technical, personnel and policy-based measures,

- **Safeguarding devices:** Secure all IoT and OT devices by implementing encryption, firewalls, access controls and regular patch management to prevent attacks and the associated costly downtime.
- **Securing supply chain and remote access:** Establish secure supply chain access protocols to ensure that only authorised personnel have access to critical systems. Implement robust authentication mechanisms for remote access.
- **Undertaking regular security assessments:** Conduct routine security assessments to identify vulnerabilities and take corrective action before they occur, assess the effectiveness of security measures, and proactively address potential weaknesses.
- **Establishing employee training:** Employees can be a significant source of vulnerability in any organisation, so it is essential that employees are educated on cybersecurity best practices to enhance their awareness of potential threats and empower them to respond effectively.
- **Putting in place robust cybersecurity policies:** Develop and implement strong OT cybersecurity policies and processes, with continuous monitoring and a disaster recovery plan to ensure business continuity.

"As the African transport and logistics sector continues its digital transformation, securing OT and industrial control systems (ICS) is of paramount importance. By adopting a multifaceted cybersecurity strategy, including risk assessment, device security, employee training, and policy development, organisations within this space can navigate these challenges and safeguard their operations in this dynamic industry," De Klerk concludes.

Local cybersecurity pressures on the rise

The cybersecurity sector in South Africa continues to grow at pace – with a compound annual growth rate (CAGR) of 12,97 percent between 2023 to 2028 predicted by Mordor Intelligence.

And this comes as no real surprise. Global attacks have increased, rising by 7 percent per week in Q1 2023 compared to the same quarter in 2022, according to Check Point Software Technologies, with each organisation facing an average of 1,248 attacks per week. African businesses are under even greater threat, the cybersecurity company said, at an average of 1,983 attacks on a weekly basis. In addition, over the same period, one in 15 African organisations were targeted in ransomware attacks.

"Looking at the continent, South Africa in particular has been under siege, rated at sixth worldwide for cybercrime density according to the local Council for Scientific and Industrial Research (CSIR), which estimates that the impact of cybercrime on the South African economy is at around R2.2 billion per annum," explains Brian Smith, Business Unit Manager at Datacentrix.

"Looking at the continent, South Africa in particular has been under siege, rated at sixth worldwide for cybercrime density according to the local Council for Scientific and Industrial Research (CSIR), which estimates that the impact of cybercrime on the South African economy is at around R2.2 billion per annum.

More attacks, fewer experts

He continues: "In South Africa we're dealing with what is essentially a double whammy: a swiftly multiplying number of cyberattacks and a dearth of local cybersecurity skills. Demand for cybersecurity skills is at an all-time high – and growing – but we're facing complex challenges in South African within this space."

As per Fortinet's 2023 Cybersecurity Skills Gap report, staffing up to strengthen security is a top board priority for organisations worldwide. Most boards recommend hiring IT and cybersecurity staff, states the report, with 83 percent of leaders indicating that their board recommended increasing IT and cybersecurity headcount in 2022, up from 76 percent in 2021, and 85 percent of boards that govern organisations with more than 5,000 employees recommended increasing IT security headcount.

"It's clear that the need for good cybersecurity skills is there. However, factors like emigration and 'semi-gration', where workers remain in South Africa but their skills are being

leveraged outside the country, have played a role in widening the current skills breach locally," says Smith.

Another issue is the vast array of cybersecurity products available on the market today, he adds. "While twenty years ago, there may have been around 5,000 solutions available, today we're looking at closer to 500,000. How do you choose which ones are the most important? And how does your cybersecurity team stay on top of the many required certifications and skills level requirements?"

Could Security as a Service be the answer?

According to Smith, a good rule of thumb would be to look at recent analyst firms' reports and identify what they're touting as the top five or six cybersecurity vendors.

Businesses could also look at how artificial intelligence (AI) can assist in automating and eliminating some of the more manual tasks, like data scanning, and the good news here is that we are seeing signs of AI-readiness within several cybersecurity products.

Another option – and one that would remove skills and certification worries from the business – would be to go the Security as a Service (SECaaS) route. Here, an organisation would opt for an outsourced, cloud-based cybersecurity offering that could include threat detection, data protection, e-mail, network and database security, intrusion management, identity and access management, data loss prevention, and more.

"The SECaaS approach is growing in popularity, as it offers organisations a number of benefits, including the ability to scale this service as it is required. This is an attractive option, as companies can then avoid potentially overspending on security services that may not benefit them.

"Aside from the cost saving aspect, SECaaS also provides access to the most recent tools and updates, as well as to skilled cybersecurity experts, thereby freeing up an internal ICT team instead of adding more pressure."

As a potential SECaaS partner, Datacentrix offers an end-to-end security service, including its state-of-the-art Security Operations Centre (SOC), manned by a team that is more than 50 strong.

Datacentrix has built a cybersecurity ecostructure that incorporates solutions from leading cybersecurity vendors such as BeyondTrust, Check Point, Forescout, Cloudflare, F5, GYTPOL, Fortinet, IBM, OKTA, Mimecast, Palo Alto Networks, Tenable, Trend Micro, ransomware protection backups with Rubrik and more. Not only do we maintain the highest levels of partnership status and certification levels with these partners, we've also ensured that they are integrated together within our SOC.

Says Smith: "The security landscape is changing on a daily basis, making it increasingly difficult for internal cybersecurity teams to effectively protect against threats. This also has a direct effect on the Chief Information Security Officer (CISO), as you can no longer plan a cybersecurity strategy for the next 24 to 36 months.

"With the right SECaaS partner behind them, businesses can review plans more regularly – at least every six months – creating shorter-term plans together and ensuring that the right skills and solutions are in place to achieve these goals."

For more information on Datacentrix's Security Services offering, please visit www.datacentrix.co.za/security-services.html

'Ghostbusters required': protecting organisations against huge potential fraud losses caused by ghost employees

By Rainer Jeske, Consultant at Datacentrix

A number of key South African organisations are potentially incurring significant losses due to 'ghosts' – that is, ghost employees, who exist on paper within business or government departments, but not in real life.

This issue is criminal rather than paranormal in nature, whereby ghost employees are one of the most prevalent types of occupational fraud, perpetuated through illicit payroll activities, and potentially resulting in substantial losses for the organisations concerned, whether at the level of a business or government entity.

And South Africa is not isolated in battling against this type of payroll theft: there have been many instances reported across Africa and even further afield, including the discovery of more than 80,000 ghost workers in the Nigerian police force; 30,000 on the Mozambican government payroll; and ghost employee scams also taking place within Zimbabwe and Kenya. Ghost workers are not exclusively a challenge for the public sector either; large organisations with diverse environments can be just as vulnerable.

To mitigate the risk and to protect organisations, leaders are needing to invest in technology that is capable of accurately defining positive identity, thereby ensuring transactional validity, assuring trust and data integrity, and enforcing accountability.

The Association of Certified Fraud Examiners (ACFE) is the world's largest anti-fraud organisation, with more than 90,000 members. In 2022, a global fraud study by the ACFE found that payroll fraud resulted in substantial financial losses overall, and that the presence of ghost employees was a key element of payroll fraud[1], accounting for nine percent[2] of reported cases globally.

> "Datacentrix's eDNA solution follows an authentication and trusted data management process to ensure that an organisation's individual identities and data are secured.

The ACFE report notes: "Try as they might, organisations cannot prevent all fraud; if an organisation is operational long enough, eventually an employee will commit fraud. Consequently, the ability to quickly detect fraud is crucial. Our research indicates that the median duration of fraud – that is, the typical time between when a fraud begins and when it is detected – is 12 months. Additionally, the longer a fraud remains undetected, the greater the financial loss.[3]"

How do ghost workers enter the system?

Ghost workers, who are fictitious employees loaded onto payroll and business systems with the simple goal of defrauding the organisation or committing a crime, can enter the system through a variety of methods. These include being loaded or left in the system by corrupt employees, or introduced by threat actors looking to do more than just defraud the payroll.

Many government institutions battle with the ongoing ghost employee challenge as they manage a vast network of databases, systems and computers that do not adhere to the highest level of data integrity. Tracking the ghosts is a

daunting task, and that's assuming that the business even knows that they are there.

For public sector organisations and large businesses around the world, it is imperative to create a comprehensive integrity management system, effectively managing and overcoming the challenges around counting employee heads accurately, and ensuring that there is comprehensive visibility into the complexities of ghost employees, duplicate records and potential insider threats.

So ... who are you going to call?

'I ain't afraid of no ghost' is the saying in Hollywood, when the legendary heroes of the 'Ghostbusters' movies are called in – but these won't work as well in the digital world.

Instead, Datacentrix encourages organisations to consider a unique transaction security solution, such as its own eDNA identity and access management (IDAM) solution that institutes people accountability across all critical enterprise applications. This solution is designed to eradicate ghost employees and any other forms of fraudulent transactions from public and private entities, validating employees through a fool-proof biometric identification process. This would include forensically examining and assessing specific transactions to ensure that the DNA of the payroll and other critical applications' activities are tied to a physical person, providing legally reputable evidence of every activity undertaken in the systems. This provides organisations with an exceptional additional layer of preventative security.

eDNA presents nine steps to trusted data

Datacentrix's eDNA solution follows an authentication and trusted data management process to ensure that an organisation's individual identities and data are secured in the following order:

1. Secure enrolment that is compliant with positive identity governance, POPIA and Electronic Communications and Transactions (ECT);
2. Three-factor digital authentication that uses biometrics, then a Public Key Infrastructure (PKI) certificate, and finally a smartcard;
3. A secure access gateway, where logon is only permitted via eDNA's three-factor digital authentication process;
4. Customer sensitive data transactions are performed that need to be secured;
5. Business rules are defined for tracking sensitive transaction data;
6. Transactions done with eDNA are signed and sealed at the data's source;
7. Using the basis of a business intelligence and alert system to build customer frameworks for business rule tracking and reporting;
8. The solution allows for the forensic production of legally accepted data evidence; and
9. A tamper-proof system that ensures all computing facilities adhere to an end-to-end highest security level data platform and ultimate data protection.

The prevalence of ghost employees reflects broader issues of corruption and unethical behaviour, which can produce negative effects within society at large.

As noted by Nigerian Professor of Accountancy, Emmanuel Ikechukwu Okoye: "Fraud has become one of the greatest threats to the world economy. It is a global problem, not only in terms of its impact on our major corporations and key financial institutions, but also its effect on smaller companies and the wider public who indirectly pay for the losses through increased costs of goods and services".

Rooting out ghost employees – and ensuring that systems are in place to make sure that they stay banished – is therefore an imperative undertaking for any organisation.

[1] https://legacy.acfe.com/report-to-the-nations/2022/
[2] page 12 of the report
[3] page 14 of the report

"This solution is designed to eradicate ghost employees and any other forms of fraudulent transactions from public and private entities, validating employees through a fool-proof biometric identification process.

Making the case for data-driven transport

By Jaap Scholten, Head: Group Hybrid ICT Strategy at Datacentrix and Chief Operating Officer at eNetworks

While the local transportation sector has been hit by major challenges over the past few years – the skyrocketing cost of fuel, fuel shortages and targeted criminal activity to name a few – there are signs of green shoots for the industry for 2023.

In his State of the Nation address (SONA) earlier this year, President Cyril Ramaphosa mentioned the local transport and logistics sector several times, with reference to reducing red tape, lessening the impact of the energy crisis, and building investment in a more efficient transport and road infrastructure system.

Technology too will play a critical role in futureproofing transportation beyond 2023 in Africa, with a data-driven approach helping to contribute to development within the sector. Artificial intelligence (AI) in combination with the Internet of Things (IoT), for example, can help improve efficiencies such as route, capacity and load planning, performance optimisation and demand prediction, as well as fleet management, maintenance and monitoring.

“

Technology too will play a critical role in futureproofing transportation beyond 2023 in Africa, with a data-driven approach helping to contribute to development within the sector.

However, there are three technology pillars that must be considered for this to become a reality, namely data hosting, data transportation, and data security.

Data hosting

There's no question that data needs to be hosted in the right place, but this in itself can become a complex process.

To use a transportation-related analogy: fossil fuel cars require a lot of maintenance requirements, from spark plugs to gearboxes, oil changes and timing belts, brake pads and filters. However, electric cars do not require the same level of upkeep, as even the brake pads are hardly used due to regenerative braking, and software updates are received via the internet.

One could say that hybrid cars seem to be the worst choice possible – all the maintenance of a fossil fuel car, plus only a small amount of the electric benefit. Yet, hybrid cars are an essential stepping stone to get to pure electrical vehicles, for reasons such as erratic electricity supplies on the one hand, and continuously improving battery technologies on the other.

When it comes to technology, hybrid ICT – or a combination of cloud and on-premises technology – provides the same stepping stone needed to get to a pure-cloud world (which, realistically, is still many years away).

Hybrid ICT offers the benefits of affordable mass storage, through hyperscaler clouds such as Amazon Web Services or Microsoft Azure, as well as a place for huge amounts of unstructured data – so-called data lakes – to be analysed using Machine Learning (ML) tools to find patterns or trends in your data.

Data transport: networking

Networks always seem to have simple beginnings, yet they generally become more complex than originally envisioned. Initially, networking was all about computer data, but rapidly expanded to voice and video, and now incorporates IoT devices as well. Each of these network services ultimately need to execute one goal: moving data between humans. There are numerous steps in between, from databases and web servers, to financial systems, operational systems, and of course cloud services.

An important note is that a network, in whichever form it is used, becomes the measure of one's data experience. A cloud experience is only as good as its network connection to that cloud, and users' experience is only as good as their Wi-Fi, 5G, or LTE signal to which they are connected.

Pervasive security

Gone are the days of a central firewall at the head office, or employing a network security specialist, who holds the keys to the front door. Data has moved out of the head-office and physical warehouse premises, to the far corners of people's homes, their notebooks and USB drives, to the cloud, and to wherever else users may be.

Data is on the move, and there is no stopping it. At the same time, many people want access to data, be it IoT data or financial data, and therefore no strategy is complete without addressing data security.

Security now lives on the network, as well as in the cloud. It has evolved to identity management, where all correctly identified users are granted access, based on their security profile and privileges.

The term used is SASE (Secure Access Service Edge), which means a network service indirectly reaches as far as people's homes, on the road or overseas in hotel rooms. This is the virtual edge of the network, and the only way that it can be secured, is by giving users access by means of their identity. Practically, this means that network access to services are based on Zero Trust – no access unless the users can correctly identify themselves, irrespective of the hardware they use or the location they find themselves at.

Making the case for hybrid ICT

By accessing and understanding data in real-time, the transportation sector will be able to improve user experience, increase revenue, decrease costs, and drive efficiencies. This is why a hybrid ICT approach, one that begins with a data-first strategy while providing an 'as a service' experience, is so vital.

The right hybrid ICT partner will be able to assist with a data-centric strategy that includes the fundamental pillars of the ideal data hosting environment, reliable data transport and connectivity, and far-reaching data security.

Building a framework for effective, agile endpoint security

The mitigation of endpoint security risks has come increasingly under the spotlight over the past few years, due chiefly to a growing distributed workforce. It therefore makes sense that local businesses are making the necessary changes to their cybersecurity strategies to accommodate the protection of rising numbers of remote workers and their endpoint devices.

So says Gideon Viljoen, Pre-sales Specialist: ICT Security at Datacentrix who explains that agile endpoint security measures – which are able to adapt quickly and easily to the changing attack landscape – are paramount for ensuring an effective first line of defence.

"With millions of Africans now working remotely, at least part-time, local businesses have had to amend their cybersecurity strategies to accommodate users who need remote access to mission critical data and applications. In fact, recent research from Microsoft and IDC shows that 65 percent of South African organisations have invested in endpoint protection solutions, and 61 percent in access management.

"For those companies that still need to ramp up endpoint security, we have some straightforward advice to offer."

The strategy behind endpoint security

It's important to start with the basics and ensure that all endpoints and servers, as well as critical assets and devices, are covered by an anti-virus (AV) or anti-malware security product, explains Viljoen. "And, sticking with the basics, the patching of these devices and endpoints is an excellent way to ensure known vulnerabilities are not open to exploitation."

With an ever-changing landscape and attackers using increasingly smarter techniques, machine learning (ML) and user behaviour analytics (UBA) have become absolute musts in the current landscape of cybersecurity, he continues. "In fact, for more mature cybersecurity portfolios, it is always better to have some form of ML and artificial intelligence (AI) in place, as these technologies can take the necessary action much faster than a human, leaving people to focus on critical risks.

"Furthermore, having an endpoint detection and response (EDR), or better yet, a cross detection and response (XDR) solution in place helps to identify, isolate and respond to suspicious behaviour on an endpoint or critical asset. These solutions also assist in reducing investigation and alert times, with far fewer false positives, which can tend to overwhelm engineers and analysts, and cause alert fatigue."

EDR and XDR solutions have helped to reduce response times considerably, providing effective protection against threat actors. However, their evolution is far from over, comments Viljoen, and with hybrid workforces not going anywhere soon, having agile solutions and technologies in place will continue to be beneficial to businesses.

Choosing the right endpoint technology (and partner)

The combination of a rapidly evolving landscape, changing attack strategies and new technologies being introduced on a daily basis means that organisations are under immense pressure to choose the 'right' endpoint security solution.

"Companies and their executives can be overwhelmingly bombarded with new technologies, and choosing the right solution for the organisation can be tough. With this in mind, it is essential that organisations wanting to outsource their cybersecurity requirements choose a provider that can provide technology solutions that are agile and quick to adapt and adopt; factors that far outweigh the cost element.

"Our recommendation is to look to independent, objective authorities like Gartner and Forrester for recommendations, which help provide guidance and greater confidence around which vendors and technologies are leading in which specific areas. Having a solution that is able to provide intelligence, visibility and response to the holistic network, while also being able to provide a single source of truth, is of utmost importance."

When looking at potential cybersecurity partners, reference cases and business case studies can provide some confidence in selecting the best option for a business, Viljoen adds.

"Visibility of these mobile and hybrid ICT workforces is critical: no business can protect against, or remediate, what cannot be seen. It has become essential to ensure the provision of a solution that can deliver visibility of all devices and assets, regardless of where they are, as well as users and user behaviours. This will allow for reduced response times and decreased risk," he concludes.

ADVERTORIAL

Enterprise next-generation compute engineered for a hybrid world

HPE ProLiant Gen11 servers deliver an intuitive cloud operating experience, trusted security by design and optimised performance for workloads.

Hewlett Packard Enterprise's next-generation compute portfolio delivers a cloud operating experience designed to power hybrid environments and digital transformation. The HPE ProLiant Gen11 servers provide organisations with intuitive, trusted and optimised compute resources, ideally suited for a range of modern workloads, including Artificial Intelligence (AI), analytics, cloud-native applications, graphic-intensive applications, machine learning, Virtual Desktop Infrastructure (VDI) and virtualisation.

"The foundation of any hybrid strategy is compute," said Neil MacDonald, Executive Vice President and General Manager, Compute, at HPE. "HPE Compute brings businesses closer to the edge, where data is created, where new cloud experiences are delivered, and where security is integral. The HPE ProLiant Gen11 servers are engineered for the hybrid world to deliver an intuitive cloud operating experience, trusted security by design, and optimised performance for workloads."

Intuitive cloud operating experience

On HPE ProLiant servers, an HPE GreenLake for Compute Ops Management subscription provides a cloud-native management console. This increases operational efficiency by securely automating the process to access, monitor, and manage servers, no matter where the compute environment lives.

The console provides simple, unified, and automated capabilities to allow customers to control their compute with global visibility and insight. Customers can also easily onboard thousands of distributed devices and benefit from faster server firmware updates to focus efforts on business operations, and not on managing complex IT infrastructure.

Trusted security by design

HPE continues to lead and deliver secure infrastructure, from edge to cloud, starting at the silicon level with the HPE Silicon Root of Trust, an industry-exclusive security capability that protects millions of lines of firmware code, from malware and ransomware, with a digital fingerprint that is unique to the server. Today, the HPE Silicon Root of Trust secures millions of HPE servers around the world. The next-generation HPE ProLiant servers build on this security innovation.

Optimised performance for any workload

As organisations run more demanding workloads, including AI, machine learning, and rendering projects, they require optimal compute and accelerated compute performance. The next-generation HPE ProLiant servers are optimised to deliver high performance on an organisation's most data-intensive workloads and support a diverse set of architectures. Service providers, and enterprises that are embracing cloud-native workloads, require dedicated, cloud-native compute to deliver agile and extensible capabilities to drive innovation.

Delivering a pay-as-you-go consumption model with HPE GreenLake

Organisations looking to transition from one generation to the next, can adopt HPE's next-generation compute through a traditional infrastructure purchase or through a pay-as-you-go model with HPE GreenLake. HPE GreenLake is an as-a-service platform that enables customers to accelerate data-first modernisation and provides over 70 cloud services that can run on-premises, at the edge, in a colocation facility, and in the public cloud.

Expanding the customer experience with new services

Through HPE Pointnext Services, an winning team of over 15,000 experts, customers adopting the HPE ProLiant Gen11 servers can leverage in-depth global expertise to deploy next-generation HPE ProLiant servers and create new experiences, gain real-time insights from their data, and modernise IT to unlock value.

Hewlett Packard Enterprise

GAUTENG

Corporate office
Corporate Park North
238 Roan Crescent
Old Pretoria Road
Midrand, 1685
Tel: +27 (0)87 741 5000

Logistics Centre
26 Landsmark Avenue
Kosmosdal
Extension 11
Samrand, Midrand
Tel: +27 (0)12 657 5000

COASTAL

Cape Town office
18 Oxbow Crescent
The Estuaries. Century City
Cape Town, 7441
Tel: +27 (0)21 529 0700

Durban office
Ground Floor, 6 The Terrace
Westway Office Park
Westville, Durban
Tel: +27 (0)31 389 0500

Gqeberha office
Southern Life Gardens
Ground Floor, Block B
70 2nd Avenue, Newton Park
Gqerberha
Tel: +27 (0)41 391 0200

East London office
Suite 2
11 Cavendish Road
Vincent
East London, 5217
Tel: +27 (0)43 705 8000

MIDDLE EAST

Dubai office
One Business Centre DMCC
Unit number One JLT-6-00
Plot number DMCC-EZ1-1AB
Jumeirah Lake Tower
Dubai, United Arab Emirates
Tel: +971 55 917 5028

Doha office
Eighteen Tower
19th Floor, Office 1972
Lusail
Doha, Qatar
Tel: +974 4007 1793

www.datacentrix.co.za