MAY 2021 ISSUE 3.0

CIAB MAGAZINE

AN INSIGHT INTO THE THOUGHT PROCESS OF BUSINESS LEADERS AND ENTREPRENEURS

CHANGEINAFRICA BUSINESS MAGAZINE

Tackling the Growing Concerns Over Cybersecurity in Africa

Kenyan startup Mazi Mobility launches

NEIL HARE-BROWN

CEO OF STORM GUIDANCE

Neil is a business leader with decades of experience in the Cyber Security sector. Known by his peers as the “Cyber Jedi”, Neil talks to us about cyber security issues in Africa and what needs to be done to address them

SPONSORED BY

BYP NETWORK

EDITOR'S NOTE

This Issue of CIAB Magazine features an interview with Neil Hare-Brown, the CEO of STORM Guidance, a Cybersecurity firm located in Africa and UK. Neil is a business leader with decades of experience in the Cybersecurity sector. Known by his peers as the “Cyber Jedi”, Neil talks to us about cyber security issues in Africa and what needs to be done to address them.

Rosie Hayes, the Head of Communications at STORM Guidance, also provides an insight into Cybersecurity issues in Africa, in her article titled "Tackling the Growing Concerns Over Cybersecurity in Africa".

We also feature an article about the launch of Kenyan startup, Mazi Mobility, which is backed by Satgana.

Lastly we would like to thank our Sponsors BYP Network who are doing great things in the black community and are bringing that value proposition to Africa

hubertn.

HUBERT NOMAMIUKOR
Editor-in-Chief

TABLE OF CONTENTS

4 INTERVIEW WITH NEIL HARE - NEIL HARE-BROWN

17 TACKLING THE GROWING CONCERNS OVER CYBERSECURITY IN AFRICA

26 INTRODUCING SATGANA'S FIRST PORTFOLIO STARTUP: MAZI MOBILITY - (SATGANA.COM)

CIAB
MAGAZINE
3.0

SPONSORED BY
BYP
NETWORK

9 772754 017009

INTERVIEW WITH NEIL HARE-BROWN CEO OF STORM GUIDANCE

WRITTEN BY HUBERT NOMAMIUKOR

Cybercrime is a big issue in Africa, and one that hasn't been addressed properly in the past. It is directly linked to the rate of unemployment and lack of job opportunities across Africa. Sci Dev Net estimates that Cybercrime has cost the world's economy roughly $500 billion. They also estimate it costs Africa's largest economy, Nigeria, $ 500 million per annum.

ChangeinAfrica Magazine caught up with Neil Hare - Brown, the CEO of STORM Guidance, a Cybersecurity firm based in Africa and UK. In the interview Neil talks about the Cyber Crime issues in Africa. He also talks about the proactive and reactive services his Cybersecurity firm offers clients.

> **"Sci Dev Net estimates that Cybercrime has cost the world's economy roughly $500 billion."**

Q: Hello Neil, we would like to know a little bit about your background, initial career aspirations and your journey to becoming a Cybersecurity expert?

Neil: I am an Electronics engineer by trade. I joined the UK Met Police in security systems before training as a programmer on IBM systems, and becoming an expert in iSeries security. In the early 90s, I worked in financial services for two banks in the City of London as a Computer Auditor and Information Security Manager whilst also working for the Met Police Computer Crime Unit. In the mid-90s I formed the UKs first Computer Forensics company, working mainly on criminal investigations whilst also consulting in InfoSec Governance, Risk Management and Compliance to blue chip organisations in Banking, Legal Services, Manufacturing, Marine and Aerospace. In 2014, I formed STORM Guidance as a boutique-style cyber investigations and cyber risk management advisory, setting up the first cyber insurance incident response team that has since responded to over 500 cyber incidents around the world.

> **"I formed STORM Guidance as a boutique-style cyber investigations and cyber risk management advisory, setting up the first cyber insurance incident response team that has since responded to over 500 cyber incidents around the world."**

Q: You run a Cybersecurity firm in Africa called STORM Guidance. Please outline its value proposition and target market within Africa.

Neil: We have three key service areas; Assess, Plan and Respond. Our risk assessments are specifically designed for clients, their brokers, and their insurers. It is comprehensive and illuminating, as well as the highest quality money can buy. Our planning services utilise many years of experience when dealing with cyber incidents first-hand . We help our clients build and test really effective cyber incident response processes. Our response service is a fully coordinated hotline and digital investigations service, incorporating technical, legal and crisis communications expertise for clients (insured or not) to investigate and recover from cyber incidents.

Q: What key challenges has “STORM Guidance” faced to date, and how have you navigated these?

Neil: Sourcing the absolute best talent and training them to be the cream in digital investigations. Growing our team to be suitably resourced to deal with the growing rate of cyber incidents.

Q: Why does STORM Guidance wish to expand into Africa?

Neil: We've had our digital forensics labs in Mauritius for 3 years. We want to expand out to assist African organisations with real on-the-ground assistance when they suffer a cyber incident. Our new Cyber Care service is specifically designed for African SMEs to give them the safety net they will need when they fall victim to cybercrime. Africa is home to the most exciting and growing nations in the world. They need our help to combat the effects of cybercrime, and we are proud to give it.

Q: Let’s talk about cyber criminals. Why do they target African SME's, it doesn't seem worth their time?

Neil: There is a very active market for personal and corporate data being used for fraud. The economic reality of an attacker in a developing nation makes it a valid living to breach organisations for data to sell. For the fraudsters pilfering this data and using it to defraud people and organisations, it is just another day in the office. It is important to appreciate that even if the victim's business may not seem like a worthwhile target, it is their connections (customers, partners etc.) who may represent a bigger opportunity. This may then cause reputational harm to the original victim.

Q: What is the profile of a cybercriminal?

Neil: Cybercrime is highly organised. The crime lords that deal in drugs and arms are now running global cybercriminal operations. In many cases, there is a blurring between nation state actors and cybercriminals. These criminals and their highly distributed teams work in offices just like legitimate businesses. They get up, turn on their computers or hit the phones just like us. There is organised crime originating from all over the world, especially in call centres that have been re-engineered for crime.

> **"These criminals and their highly distributed teams work in offices just like legitimate businesses"**

Q: Where do African businesses turn to for help when they suspect or know they have a cyber incident?

Neil: The first thing that many businesses do, is panic. The second thing they do is turn to either in-house or external IT support. Remember that one of the reasons why businesses suffer incidents is lack of resources, so turning to an under-resourced IT specialist, with little experience in digital investigations, is unlikely to be the best option. Furthermore, such IT specialists may cover up the real facts behind the attack. The next thing they may do is call the police. Whilst many police forces in Africa do have a cybercrime unit, they are usually also under-resourced, over-worked and valiantly fighting what are often complex technical crimes. It is unlikely therefore that they will be able to offer much on-the-ground assistance.

So, the availability of incident response services such as those provided by STORM, both separately and integrated into cyber insurance, is often the best and sometimes only option if you want a thorough investigation, rapid recovery and to be restored in a more secure state than before the incident.

Q: Are victims of cyber-attacks willing to report their losses or are they reluctant due to repercussions?

Neil: We find that one of the biggest, if not the biggest problem with encouraging organisations to take cyber insurance, is in helping them to clearly understand the cyber risks that apply to their business. Reputational harm tends to make organisations very averse to reporting the incidents they have suffered. Criminals know this and use this reputational threat as a lever to make their victims pay the ransoms. Very often organisations ask their brokers, "do we really need this cover, who else has it?". They're actually likely to be closely located to other businesses that have suffered a bad cyber incident, they simply don't know about it. Because of the reputational impact with cyber issues, they tend to want to keep that incident very confidential and so cyberattacks are seen as a 'black swan event'. That is absolutely not the case. There are huge numbers of businesses being destroyed by cybercrime right now. Quite simply, it is a crime pandemic!

Q: With the implementation of Data protection/Privacy Acts such as the GDPR and the POPI Act, beginning this year in South Africa, how would these legislations effect Cyber Risk Insurance? Would it help or possibly interfere and how so?

Neil: The GDPR and POPI both require organisations who suffer a data breach to notify regulators (with sufficient investigative detail) and to determine, again through investigation, any individual data subjects who may be at high risk because of the breach, and if so, then to notify them also. Both the first response, investigation, legal advice, and notification activities are expensive, and all are covered by most cyber insurance policies. So, cyber insurance should assist in the proper compliance with GDPR, POPI and data protection law in other African nations.

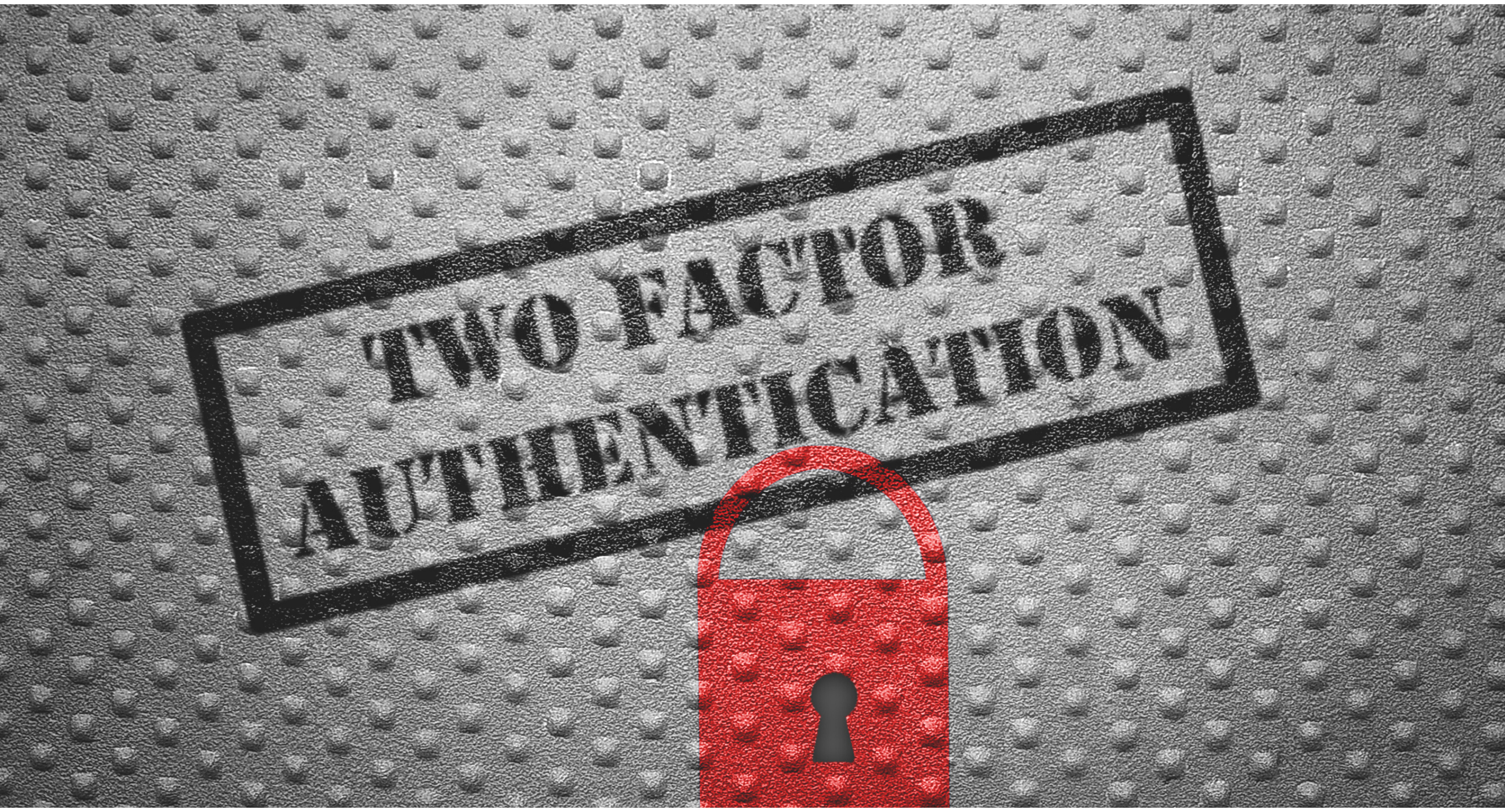
Q: We need legal legislations to regulate the management of cyber risk. How can we overcome such a challenge?

Neil: My view is that we need to look at it rather like Health & Safety. Even if not covered by regulation and contract, businesses should have a moral duty towards protecting the personal data and other business information entrusted to them. When it comes to understanding cyber risks, our Cyber3 assessment is the only one to include cyber underwriters' questions, as well as cybersecurity best-practice. Cyber3 gives clients a clear understanding of cyber risk in the context of their business.

Q: What will it take to improve the state of cyber risk management in Africa?

Neil: One word, “Investment”. According to the Global Cybersecurity Index, Africa has a low commitment to cybersecurity and a higher cyber risk exposure. Numerous organisations do not have the skills, resources, or funding to protect, detect and respond to cybersecurity threats, placing African organisations below the cybersecurity poverty line. In the African Cybersecurity Report 2020 (by Serianu), of the organisations asked, a disappointing 76% did not have cyber insurance. To address these issues will entail addressing the skills gap. We need to look at training IT professionals within organisations, vital cybersecurity skills, and to invest in their continuous training. Cyber risk is ever evolving and changing, and so cyber professionals must keep up with - and stay ahead of, potential threat. Using risk assessment services, African organisations must address this inept uptake in cyber insurance.

All lasting changes for the better must be supported with strategy. SMEs must not think of themselves as an island when it comes to cyber risk but to appreciate the relationships that they have with other organisations. It is this interconnectedness which cybercriminals seek to exploit, and so African businesses of all sizes need to consider whether they may be the weak link in the chain.



Q: What simple measures can my business implement to reduce our risk exposure?

Neil: First, consider that passwords alone are pretty much useless. They can now be easily cracked, learned via scams or available in breach data sets. Attackers know that if they have your password for one system it is likely this will be used in many others. Another layer of defence is now needed. This is called multifactor or two-factor authentication (username and password, AND a one-time code generated by an authenticator app, or received via SMS). Enable MFA on every account you have, everywhere to be reasonably safe.

Maintain regular offline backups and ensure your resilience to ransomware is addressed by segmenting the network and reducing the number of administrative accounts. Attackers are always looking for an admin account to log in.

Finally, obtain accurate Cyber insurance using a cyber risk assessment service such as Cyber3.

Q: What are the future plans of STORM Guidance, especially in Africa?

Neil: We are launching our new Cyber Care (www.cyber.care) service (think of it as a roadside assistance model) for organisations who are victims of cybercrime. Beginning in South Africa with the onboarding of membership/affiliation service provider client in Q2 . We aim to rapidly expand. In fact, we are already welcoming clients from all over Africa.

CIAB Magazine: We have come to the end of the interview, and would like to thank you for participating in this Q&A session.

Neil: Many thanks for inviting me to your interview

The Business Anecdote

A magazine for Business Leaders and Entrepreneurs

SUBSCRIBE

FREE

TACKLING THE GROWING CONCERNS OVER CYBERSECURITY IN AFRICA

WRITTEN BY
ROSIE HAYES
HEAD OF COMMUNICATIONS
STORM GUIDANCE

Looking at Africa's largest economy, Africa Centre for Strategic Studies article - Nigeria's Diverse Security Threats, explores Nigeria's growing state of emergency as a result of the continuously poor efforts in cybersecurity. Many have perceived Nigeria's main threat to peace and security to be centred on the terrorist organisation, Boko Haram, positioned in the north east. Through bombings, attacks and the spread of fear and violence over social media and cyberspace, the terrorists are fighting to overthrow the government and create an Islamic state. The group, together with the Islamic State in West Africa (ISWA), has caused mass disorder in Africa's most populous country, however, it is important not to be blindsided. The widespread nature of Nigeria's security challenges affects all the country's regions, and a deeper look into the state of cyber in Africa must be addressed.

An article in This Day - Addressing Emerging Security Threats of Cyberattacks, takes a closer look at cyberthreats such as cyber terrorism, cyber espionage, cyber theft and Distributed Denial of Service (DDOS) against individuals, businesses and critical national infrastructure. Examining the response from nations across the globe in addressing these vulnerabilities through both defensive and offensive actions, was a theme of the workshop held to address the issue at the Army Officers Mess, Outer Marina, Lagos. The field commanders of the army, Nigerian Navy (NN), Nigerian Air Force (NAF), Nigerian Police, Department of State Services, Nigerian Security and Civil Defence Corps (NSCDC), together with other Nigerian state departments, were brought together to address the increasing threat to Nigeria's security. Dubbed 'Exercise Crocodile Smile VI', it was the first-ever cyber warfare exercise to be conducted in the history of the African armed forces.

However, when the powers that are in place to protect and serve are actually part of the problem, where are the means for research, regulation and change? Nigeria's corrupt State Security Service (SSS), who are directly overseen by the president, together with the Presidential Guard Brigade, demonstrate a clear and often violent line between themselves and civilians. Corroding trust in the police and security forces accentuates the growing instability in Nigeria. Remedying this broken trust must be the top priority of any national security strategy. However, the terror inflicted by Boko Haram proved to be the perfect distraction, as cyber-terrorism to Nigerian infrastructure became the new and evolving weapon of destruction.

Operation Crocodile Smile VI, was set to look at armed robbery and other crime, however, cyberattacks were named as the most pressing issue - an emerging security threat in Nigeria. The workshop sought to identify Boko Haram terrorists and to reassure law abiding citizens who have been left fearful of their safety after the violent manifestation of the #ENDSARS protest and the political use of cyberspace. The Commander, 55 Signal Brigade, Brigadier General Henry Yanet, expressed concerns that the army and other government establishments may be vulnerable to cyberattacks from non-state actors such as the Boko Haram, ‘Anonymous’, and other hacktivists groups who exploit the dark web, as was seen during the #ENDSARS protests. The demonstrations led to a wave of attacks on governments, together with private and public web infrastructure. The fear is that the spotlight may now shift to Nigerian companies as they are perceived to be easier targets.

According to an article by Deloitte; Maritime, Telecommunications, Consumer Goods and Energy sectors risk falling victim to cyberattacks and data leaks. However, the Financial Services Industry (FSI), has made better progress with employee awareness, anti-phishing campaigns, email and web security solutions, next-generation antivirus solutions and overall technology hardening. With the inevitability of more sophisticated attacks, it is important the FSI does not become complacent.

Over the past two years, businesses in Nigeria have implemented the Nigerian Data Privacy Regulation (NDPR). However, attackers are not idly sitting in the shadows; they continually work to find new loopholes, vulnerabilities, and flaws to exploit.

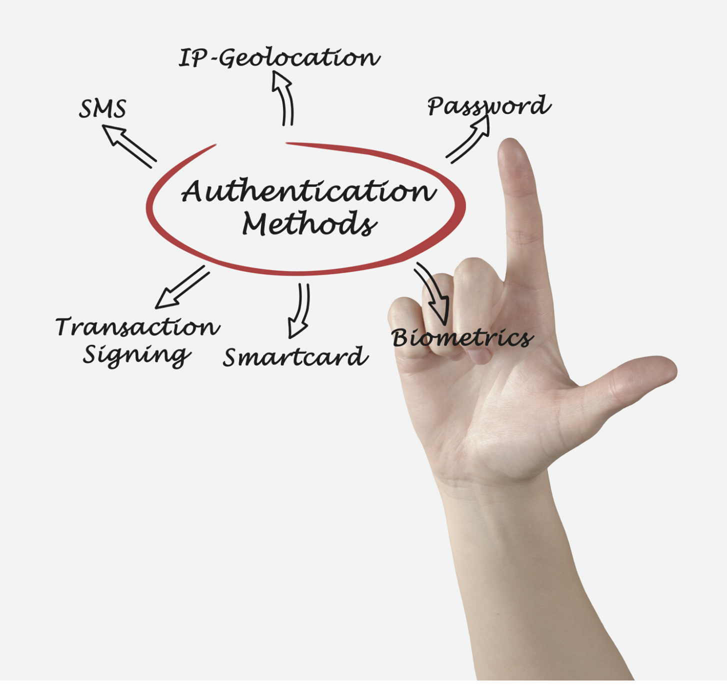
A January 2020, report by PWC - Cybersecurity & Privacy in Nigeria, outlined some simple measures that can be adopted for better preparation and protection:

- **Use Strong authentication** – Longer and stronger passwords, biometric authentication, and multi-factor.

- **Use email and social media with care** – If it looks too good to be true, it probably is. If an email or posts look suspicious, ignore/delete, or verify the authenticity through separate means of communication (a phone call for example). Do not open an email or its attachments if you do not recognise the sender. If you think you have been compromised, contact your IT team immediately: a few seconds can make a big difference when trying to contain a breach.

- **Install updates** – Updates often patch vulnerabilities giving users protection from attacks.

.



- **Stay cyber aware and informed –** Remember, an organisation is as strong as its weakest link.

- **Comply with applicable laws and regulations** – These are in place to protect against information being misused.

However, the 2019 National Information Technology Development Agency's (NITDA) introduction of the NDPR, failed to address one vital element in its regulation. It does not mandate that companies report data breaches. When a company is required by law to report the loss of data, it allows the person(s) whose data has been stolen to protect themselves, by changing passwords and alerting relevant people of the potential of fraudulent activity or impersonation.

Looking at Africa as a whole

The Global Cybersecurity Index (GCI) Framework, measures the commitment of countries to cybersecurity, looking at each country's level of development and engagement. In the interests of this article and its objective to shed light on the state of cyber risk management in Africa, this framework and its comparisons give a clear insight into just that. The UK was ranked as the most committed to cybersecurity, followed by the USA, then France. However, in Africa, Mauritius was the top ranked member state (globally 14th), followed by Egypt (23rd globally), then Kenya (44th globally), and Rwanda (49th globally). The final African member state ranking is Ghana, which is 89th in the world. In reflection, this demonstrates a low commitment to cybersecurity in Africa, and therefore a higher cyber risk exposure.

Serianu, is a Kenya based firm which gathers intelligence released by the Africa Cyber Immersion Centre (ACIC). Their 2019/2020 Africa Cybersecurity Report, highlights significant investigative research and trends in threat statistics. It highlighted the rise in regionally coordinated attacks in East Africa, the 50% rise in insecure remote connections in Kenya, and the rise of ATM malware attacks.

Key cyberattack vectors were indicated as:

- Malware (including Ransomware) - increased from 4,146,435 threats detected in 2016/17 to 40,893,141 in 2018/19.
- Web application attacks – rose from 2,656,675 threats detected in 2016/17 to 6,109,184 in 2018/19.
- Botnet/DDoS – grew from 952,327 in 2016/17 to 4,852,022 in 2018/19.

In fact, the total number of cyberthreats rose from 7,755,498 in 2016/17 to an eye watering 51,903,286 in 2018/19.

The previous 2018 report, demonstrated a clear cyber skills gap in African organisations, estimating that 90% of SMEs and large organisations will face a talent shortage of cybersecurity professionals in 2019. A disturbing figure which illustrates this concern is Botswana's meagre 200 certified security professionals. Two challenges faced by African organisations in patching the skills gap, are a lack of sufficient IT security budgets and keeping abreast of cyberthreats.

Returning to Serianu's 2017 report, Demystifying Africa's Cybersecurity Poverty Line, of the organisations asked, 90% had been impacted by cybercrime, yet only 28% reported these crimes to the authorities. In June of that year, Uganda ranked 7th highest risk country globally. In fact, 95% of African organisations in private and public sectors, were found to be operating on or below the Cybersecurity Poverty Line.

A focus on South Africa

Looking specifically at South Africa, the latest report by Accenture, illustrates that South Africa has the third highest number of cyberattacks in the world, losing R2.2 billion a year. It claims:

> "As an increasing proportion of the population begins connecting to the Internet for the first time, this inexperience paired with increased exposure is a potent combination that cyber criminals try to exploit."

To translate the scale of the problem, some of the major incidents in 2019 are outlined below:

- February 2019: A South African energy supplier suffered two security breaches in quick succession.
- July 2019: Ransomware infected a provider of pre-paid electric power, leaving customers without access to power.
- September 2019: One of South Africa's largest ISPs suffered a Distributed Denial of Service (DDoS) attack lasting two days.
- October 2019: Several South African banks, as well as financial institutions in Singapore and Scandinavia, suffered DDoS attacks resulting in a loss of service.

It is thought that cybercriminals perceive South Africa as an easy target, and as having lower defensive barriers than perhaps more developed economies. With South Africa's low investment in cybersecurity and cybercrime legislation, it may be that threat actors believe they are at a lower risk of being traced and of facing consequences.

South Africa are beginning to tackle the issue with the introduction of the Protection of Personal Information Act (POPI) which was enacted in July 2020. It requires that all South African institutions conduct themselves in a responsible manner when collecting, processing, storing, and sharing another entity's personal information. The act holds institutions accountable should they abuse or compromise personal information.

However, in terms of cybercrime accountability, while civil and criminal charges can be brought against people or organisations under Section 87 of the Electronic Communications and Transaction Act (ECTA), there is still a profound amount of work essential in bringing South African legislation in line with international principles and standards and South Africa has yet to introduce a specific Cybercrime Act.

Looking for a solution

Cyber insurance provides a positive step in the effective management of cyber risk in Africa, however, in the earlier cited 2020 Serianu report, a disappointing 76% of organisations surveyed, did not have cyber insurance. 25% said they did not have extensive cybersecurity controls and a mere 17% said they did have cyber insurance. African organisations must address this chasm of insecurity and ensure the proper economic quantification of their cyber exposure in order to address their cyber value at risk. They can achieve measurable outcomes with cyber risk management programs.

As part of a long-term strategy, African governments must work with their education ministers to develop curricula that will create future cyber experts, inspiring students to pursue the profession.

"The role of governments cannot be overemphasized in tackling cyberthreat. It should no longer be a backburner idea which should be handled only by the Ministry of Science and Technology, or the office of the National Security Adviser. It is a frontline issue that could result in cascading economic catastrophes."

(Deloitte - ‘Cyberharam’: can Nigeria prepare for the next generation of terrorists?)

THE

END

The Business Anecdote

A magazine for Business Leaders and Entrepreneurs

SUBSCRIBE

FREE

INTRODUCING SATGANA'S FIRST PORTFOLIO STARTUP: MAZI MOBILITY

ARTICLE WAS WRITTEN BY JASHNA PILLAY
AND FIRST PUBLISHED ON SATGANA.COM

Jashna Pillay is a Junior Researcher at Think Ecological Design and a Founding Member at Satgana. She graduated with a BSc degree in Environmental Science from the University of Kwazulu-Natal and thereafter obtained a BSc Honours degree in Environmental Management, with distinction, from the University of South Africa.
You can connect with her on Linkedin

INTRODUCING SATGANA'S FIRST PORTFOLIO STARTUP: MAZI MOBILITY

Since our launch in September last year, the Satgana team have been receiving and reviewing applications from impact-driven entrepreneurs all over the world. After months of work, we are elated to announce our first portfolio startup from Nairobi, Kenya, called Mazi Mobility.

In Africa, public transport is fragmented and highly inefficient. Mass mobility transportation systems largely contribute to CO2 emissions. Nairobi based startup, Mazi Mobility, plans to address issues faced by the public transport industry in the Global South by electrifying the motorcycle ('boda') industry.

Cities across Africa are undergoing a mobility revolution spurred by rapid urbanization, an increasing energy demand and economic growth. However, the results of inadequate infrastructure have led to high levels of congestion and poor air quality.

Mazi Mobility is launching electric bikes known locally as 'e-bodas'.

These challenges are presenting entrepreneurs with the opportunity to pursue an equitable and cleaner future through innovation, and Mazi plans to do just that.

Mazi is launching electric bikes to accelerate the transition to clean mobility. The startup is introducing battery swapping stations that provide on-demand energy, reducing transportation costs by 50%. Furthermore, they will use the Internet of Things (IoT) to mitigate range anxiety and optimize e-boda routes through Machine Learning (ML) to ensure a 99% service uptime for riders. Their key features include a choice between a single and dual battery, capable of up to 70km and 140km of range, respectively. Mazi is taking a multi-stakeholder approach to drive the e-mobility sector forward. They are working with boda operators, technical institutions and manufacturers to ensure the successful implementation of their service.

A CLOSER LOOK AT THE TEAM

Jesse Forrester, founder and CEO at Mazi, is a tenacious, young, impact-driven entrepreneur. The team strongly believes in the confluence of social impact and profit – a vision being brought to life through their latest venture.

The Mazi Mobility team. From left: (Pascal Aloo: Chief Engineer, Mark Maloba: Head of Machine Learning, Jesse Forrester: Chief Executive Officer, Troy Barrie: Chief Technical Officer)

"Mazi is not just an EV company, we are advocates for a sustainable mass mobility change ", says Jesse. He further adds that, at Mazi, "we believe that Africans should be able to move efficiently, and affordably across cities at less than the price of personal vehicle ownership while reducing CO2 emissions. What industry is better to see this change than the boda one? Mazi is taking a long approach to mobility, we don't want to just have the same status quo but with electric vehicles. At Mazi we move people, data and things. Twende Kazi na Mazi!"

The Satgana team has been closely involved with Mazi over the past 4 months. It's been an inspiring undertaking and we're excited to now publicly announce the launch of our first portfolio venture. This collaboration has resulted in hands-on venture-building in an effort to help achieve SDG 8 (Decent work and economic growth), SDG 11 (Sustainable cities and communities) and SDG 13 (Climate action) within the e-mobility sector.

"The urgent need to decarbonize our economies places transportation at the cusp of a fundamental shift towards electric solutions, and mobility in Africa is ripe for disruption. As such, Satgana is beyond excited to be involved in the launch of Mazi and truly believes in the founding team's ability to make it happen. Since day-1, we have been impressed by Jesse's vision and execution capability. As a Venture Builder, we are humbled to be able to support Mazi in its mission to make urban transportation sustainable while empowering low-income drivers.

ROMAIN DIAZ

Founder and CEO at Satgana

At Satgana, our aim is to build and invest into startups alongside purpose-driven entrepreneurs, wherever they are, by using innovation-led and market-based approaches to solve the greatest social and environmental challenges of our time. And with Mazi, we hope to write a new chapter in the history of e-mobility in Africa.

THE NEXT BIG MOVE FOR GLOBAL INVESTORS

The uptake of e-mobility is expected to increase globally, and with it comes a myriad of opportunities. In many East African cities like Nairobi, bodas form the backbone of public transportation. According to the Motorcycle Assembly Association of Kenya, the industry generates over $1.4 billion annually in Kenya. This number presents a massive opportunity to scale for startups in the sector, large returns for investors, and impact not just on environmental sustainability but also economic empowerment.

Transport is the fastest growing greenhouse-gas-emitting sector in the world, responsible for around 67% of Kenya’s energy-related CO2 emissions. To see results, adequate CO2 reduction requires changing the transport emissions trajectory through the development of an integrated e-mobility ecosystem. This is further envisioned in the Paris Agreement that seeks to electrify 20% of all road vehicles to curb carbon emissions by 2030.

With Kenya’s electricity grid predominantly powered by renewable energy, it is just one of the many African countries well equipped to lead the transition to e-mobility on the continent. The rise of greentech, the sharing economy, and electrification – many people associate these concepts with urban mobility. Analyses conducted by various market research companies show that 2030 will mark a turning point where environmentally friendly transport will be the norm in emerging markets like Nairobi.

Mazi Mobility launches on 11 May 2021, visit mazimobility.com for more information.

Also follow Mazi Mobility (@mazimobility) on LinkedIn, Twitter and Instagram for their latest updates.

THE END

The Business Anecdote

A magazine for Business Leaders and Entrepreneurs

SUBSCRIBE

FREE

CIAB

MAGAZINE

3.0

SPONSORED BY

BYP NETWORK

9 772754 017009