Broadband Infraco

Connect. Growth, UNLOCKED.

Securing South Africa's Digital Future: Insights from Broadband Infraco's Senior IT Manager, Climate Bainze

October 2025

As technology continues to transform the way we live, work, and connect, the question of cybersecurity has never been more critical. Every day, organisations face new and increasingly sophisticated cyber threats, many capable of disrupting essential services, compromising sensitive data, and damaging reputations built over years.

CLIMATE BAINZE

Senior IT Manager: Broadband Infraco

In recognition of Cybersecurity Awareness Month, Broadband Infraco sat down with its Senior IT Manager and Cybersecurity Expert, Climate Bainze, to unpack the state of cybersecurity in South Africa, the trends shaping the threat landscape, and the steps organisations can take to build stronger digital resilience.

According to Bainze, South Africa's cybersecurity landscape is maturing as more industries, both public and private, recognise the importance of protecting their information assets. "Every industry has started paying attention to cybersecurity," he explains. "Based on emerging threats, many organisations, whether government or private, have gone through cyber incidents. Events and conferences have also played a huge role in spreading awareness about how organisations can safeguard their information."

While awareness has grown, cybercriminals have evolved just as rapidly. Over the past year, ransomware and phishing attacks have become alarmingly common, making weekly appearances in the news. Yet Bainze notes that today's adversaries are no longer relying on old tactics. "As technology advances, cybercriminals have also adapted," he says. "We're now seeing deepfakes being used for impersonation, combined with social engineering to deceive employees and gain access to sensitive systems."

Industries such as banking, government, and fintech remain prime targets due to their financial and data sensitivity, but Bainze cautions that no organisation is immune. "Adversaries are motivated by both financial gain and reputational damage," he adds, stressing that complacency is no longer an option.

The shift to remote work and increased reliance on cloud services have also expanded cybersecurity risks significantly. "Remote employees often use personal devices and unsecured networks, making them more vulnerable to phishing, malware, and data breaches," Bainze explains. "While cloud environments offer flexibility and scalability, they can be misconfigured, leading to unauthorised access. Identity and access management have become absolutely critical."

One of the most common and costly mistakes Bainze sees is that many organisations only start investing in cybersecurity after a breach has occurred. "It's like wearing a seatbelt after the car has already crashed," he warns. "Reactive spending can't undo the damage already done. Preventive investment is always cheaper and more effective than crisis management."

For smaller organisations with limited resources, Bainze's advice is clear: start with the basics. "It all goes back to simple policies and employee awareness," he says. "You don't always need a huge budget to harden your systems. Focus on controls that strengthen security without significant financial implications, like password hygiene, data backups, and regular system updates."

But technology alone is not enough. A truly secure organisation is built on a strong cybersecurity culture, one where every employee understands their role in protecting information. "Cybersecurity isn't just IT's job," Bainze notes. "It's everyone's responsibility. A good security culture combines awareness, accountability, and best practices across all departments."

He emphasises that leadership plays a key role in driving this culture by leading through example, funding continuous training, and recognising secure behaviour. "Regular awareness programmes and open communication make it easier for employees to report suspicious activity without fear. When everyone takes ownership, the organisation becomes much harder to compromise."

Human error remains one of the most common causes of data breaches, reinforcing the importance of employee training. "Even the most advanced systems can be compromised by a careless click," Bainze says. "Continuous, scenario-based training helps employees recognise phishing attempts, manage sensitive data properly, and respond appropriately to incidents."

When a breach does occur, Bainze advises immediate and coordinated action. "Act swiftly to isolate affected systems and disable compromised accounts," he explains. "Activate your incident response plan, preserve all evidence, and assess the scope of the breach. Inform leadership, legal teams, and, where required, regulators and affected parties."

Compliance with South Africa's Protection of Personal Information Act (POPIA), he adds, is a critical component of modern cybersecurity strategy. "POPIA mandates adequate security measures to protect personal information. It pushes organisations to conduct risk assessments, implement encryption, and ensure responsible data handling. It's not just about compliance, it's about building trust."

For Bainze, cybersecurity is a shared responsibility that extends beyond organisational boundaries. He highlights the importance of collaboration between the public and private sectors to strengthen national cyber resilience. "Government agencies provide frameworks and regulation, while the private sector contributes technical expertise and real-time threat data," he explains. "Together, they enable shared intelligence, coordinated incident responses, and capacity building."

He adds that infrastructure providers like Broadband Infraco play a particularly crucial role in securing the national digital ecosystem. "As a national digital infrastructure provider, Broadband Infraco helps secure the ecosystem by detecting and mitigating threats, managing network traffic securely, and sharing intelligence to prevent large-scale attacks."

For Bainze, cybersecurity is not just a profession, it's a calling. "It's a niche environment that will always remain relevant," he says. "As technology evolves, data becomes more valuable, data is the new gold, and securing it should always be a priority."

To young professionals aspiring to enter the field, his advice is simple yet powerful: never stop learning. "This field evolves every day," he says. "Build strong technical foundations, stay ethically responsible, and keep adapting. The more you learn, the more capable you become of protecting others."

As South Africa observes Cybersecurity Awareness Month, Bainze hopes the message resonates widely: no one is immune to cyber threats. "Secure as much data as possible, and if you ever get compromised, make sure you can recover quickly and effectively," he advises. "Protecting your data protects your reputation, and your future."

Through the insights of experts like Climate Bainze, it becomes clear that cybersecurity is no longer an IT issue, it's a business imperative, a national responsibility, and a shared commitment to safeguarding South Africa's digital future.

Enquiries: Marketing@infraco.co.za