BUSINESS ⋮ TECHNOLOGY ⋮ LEADERSHIP

VOL 53 | ISSUE 44 | MARCH 2025 EDITION

CIO MAGAZINE

CIO AFRICA MAGAZINE
SOUTH AFRICA
REGION
EDITION

THE CYBERSECURITY EDITION

AFRICA IS NOT READY FOR AI ATTACKS ON HER INFRASTRUCTURE

INSIDE

LABAN NYARERA'S SKILLFUL STRATEGIES FOR CYBER WARFARE

DXNOVA: WHY ONLY FIVE MINUTES ONLINE MAKES BABIES SMARTER

FOUNDER AND EXECUTIVE DIRECTOR

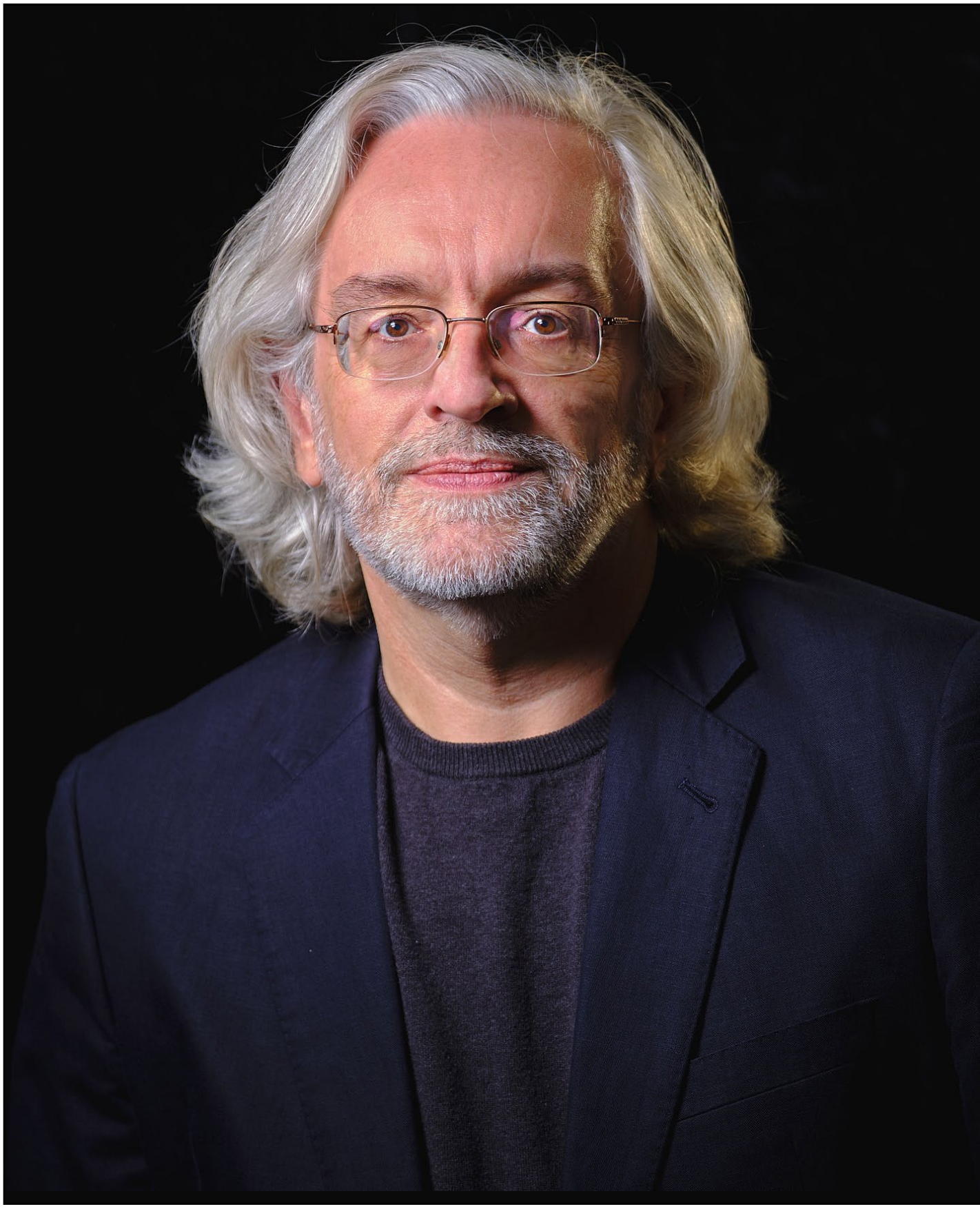
CUSTODIET ADVISORY SERVICES

STEVE JUMP

HE WHO GUARDS THE GUARDIANS OF THE DIGITAL GALAXY

www.cioafrica.co @cioafrica | @dx5ve

by dx5



ARTICLE BY KEVIN NAMUNWA

He Who Guards The Guardians

Steve Jump, the Founder and Executive Director of Custodiet Advisory Services, has built his career on solving complex problems and teaching others to ask the right questions before taking on any new technologies to their projects. It figures, seeing how he works in South Africa, who, just as the rest of the world, has been experiencing a fast-tracked digital transformation journey. Technology is moving so rapidly, regulators are almost always caught playing catch up with companies being forced pivot to stay competitive. Some companies and individuals turn strategic in the technologies they employ even as others are straggling. These are the kind of businesses that merely want to describe themselves as 'AI-enabled' or 'Supported by AI.' The problem with phoning it in is as technologies evolve, the attack surface area increases, putting systems at a higher cyber risk. A seasoned cybersecurity professional, Jump is best placed to unpack the cybersecurity situation in 2025.

From Engineer To Cyber Risk Guru

Jump's career began in the world of engineering. His early exposure to electronics, microchips, and large-scale systems instilled in him a unique, systems-oriented mindset. "My background taught me an approach to problem solving that goes beyond fixing symptoms." It allowed him to visualise the intricate interdependencies in complex systems, a skill that has been his secret weapon throughout his career.

As he transitioned from engineering to public speaking, teaching, and ultimately entrepreneurship, Jump discovered his true passion lay in demystifying complicated subjects. "I love helping people solve problems." And it is this passion that led him to hone a simple yet powerful method: rather than solving every problem himself, he asks the right questions, enabling others to find their own solutions. This method of questioning others not only scales his expertise, but also empowers his clients to become better problem solvers in their own right.

The foundation of Custodiet Advisory Services is steeped in both history and a personal calling. Derived from a Latin proverb—custodiat ipsos custodes, meaning 'who guards the guardians themselves,' this ancient adage encapsulates the very essence of his mission: ensuring that those entrusted with protection are themselves well-protected. Further, his journey to founding Custodiet was as much a personal evolution as it was a professional one. Having served as a Chief Information Security Officer (CISO) for many years, he became intimately familiar with the stresses and challenges that come with defending organisations against ever-evolving cyber threats. "I often describe myself as a recovering CISO," he remarks, emphasising the personal toll relentless cyber battles can take. The constant pressure of defending against digital adversaries, coupled with the internal strife of aligning IT and business objectives, inspired him to create a consultancy that goes beyond the technical. Custodiet Advisory Services was

ultimately born from a desire to bridge the divide between business and technology as well as reactive firefighting and proactive planning. Jump saw an opportunity in the chaos emerging during the COVID-19 pandemic when companies scrambled to adapt to remote work, exposing glaring vulnerabilities in cybersecurity strategies. Rather than simply managing crises, he envisioned a service that would equip businesses with the tools and mindset to build resilience from the ground up.

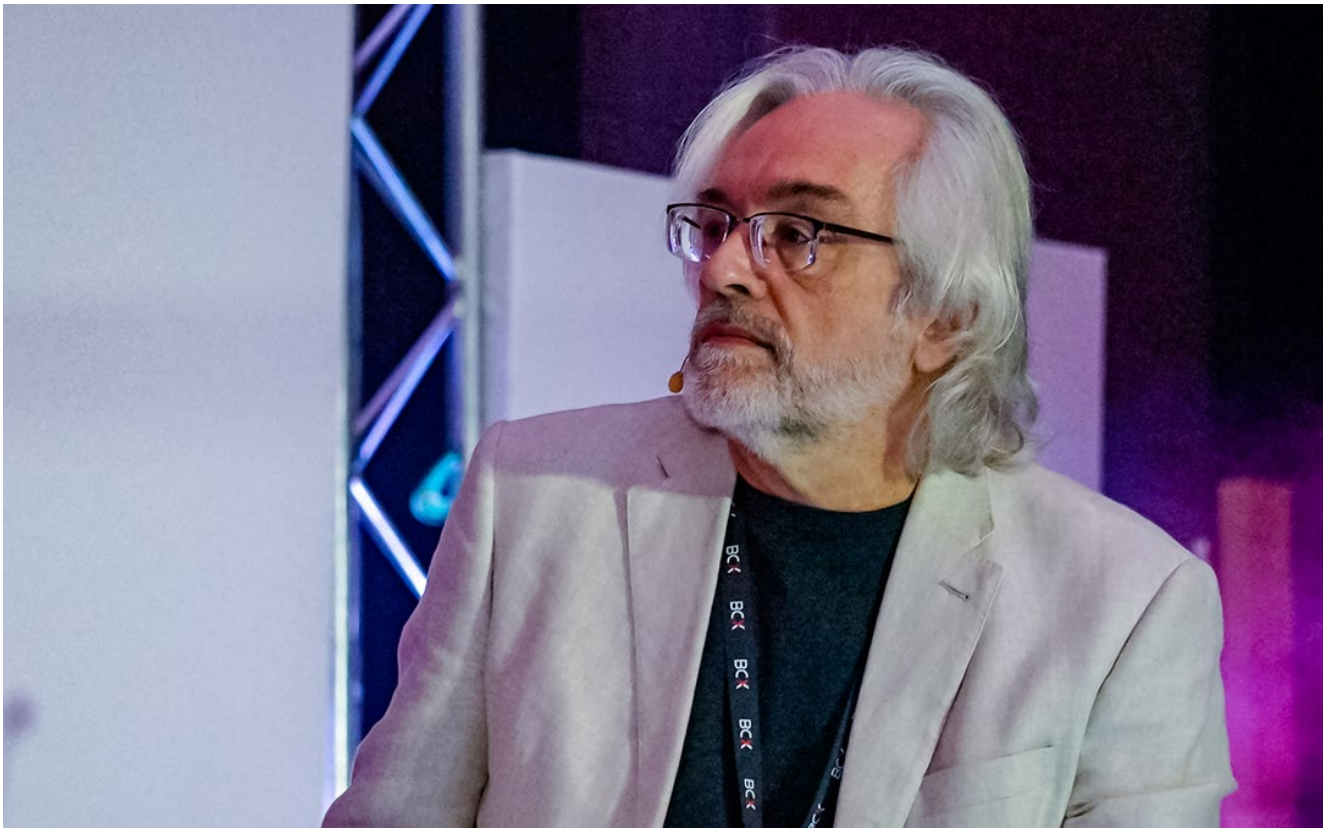
Cybersecurity As A Business Imperative

One of Jump's central tenets is cybersecurity is not just an IT problem—it is a critical business risk. "Cyber risk is far too important to leave up to IT alone," he explains. In many organisations, security is relegated to a technical function, treated as an afterthought that can be bolted on once systems are built. Jump argues that this mindset is not only outdated but dangerous. When security is viewed solely through a technological lens, the broader implications for business continuity and profitability are lost. Instead, he advocates for a holistic approach to cyber risk management, one that considers the entire business ecosystem. "What matters to a company is not just having secure systems but ensuring that business operations can continue even when under attack." Tis perspective leads directly into the concept of cyber resilience, a framework that accepts that breaches will occur and focuses on maintaining critical operations despite these incidents.

COVID-19 proved to be a turning point for cybersecurity globally. "Businesses had rehearsed and planned for work-from-home scenarios, but few had truly tested their resilience." The pandemic not only exposed technical vulnerabilities, but also highlighted the often-overlooked human element in cybersecurity. During the crisis, many companies outsourced their cybersecurity operations, assuming that the threat of cyber-attacks would somehow be mitigated by the measures in place. However, this outsourcing instead led to a disconnect between business objectives and IT capabilities. "IT assumes the business knows what it wants, and business assumes IT understands that need," a misalignment resulting in inefficient or even counterproductive strategies. Businesses invest in technology without a clear understanding of what they are trying to protect. Jump's experience during this period solidified his belief that cybersecurity must be a proactive, business-driven initiative. The stress experienced by CISOs during the pandemic – a stress so severe it would lead to burnout and post-traumatic stress – underscored the need for a new approach. By reframing cybersecurity as an integral part of overall business risk management, organisations became better prepared for and recover from cyber incidents.

Cyber Resilience: A Multi-Faceted Approach

Cyber resilience, the heart of Jump's philosophy, is built on three interrelated pillars: business resilience, IT resilience, and secure-by-design principles. It is



not about achieving an unattainable state of complete security; rather, it's about ensuring a business can continue to operate, even when under attack.

Business Resilience: The overarching goal. It's the idea that if a cyber incident occurs, the business should be able to sustain its core operations and continue to serve its customers. Jump emphasises that businesses must recognise that "cyber risk is an existential threat." Rather than viewing cybersecurity as a cost centre, companies should consider it an investment in their long-term viability. When a breach occurs, companies often find themselves spending vast sums on firefighting measures, money that could have been saved with a well-designed, resilient system from the outset.

IT Resilience: The focus shifts to the technology that underpins a business. It's not enough to simply have robust systems; these systems must be designed to endure and recover quickly from disruptions. Jump underscores that many companies still struggle with basic issues, such as managing identities, monitoring critical systems, or even knowing the full extent of their technological assets. "If your IT collapses today, your business is toast," he warns. The solution lies in continuous monitoring, regular updates, and ensuring that systems can be isolated and protected in the event of a breach.

Secure By Design: Perhaps one of the most critical points Jump makes is that security must be built into a system from its inception—it cannot be added as an afterthought. The notion of "secure by design" is a call to action for businesses to integrate security considerations into every phase of system development. "You cannot add security once your design is complete," Jump asserts. Too often, companies install firewalls and antivirus software on systems that were never designed with security in mind. This reactive approach rarely addresses the root causes of vulnerabilities and often leaves gaps that can be exploited by cybercriminals.

The Role Of AI In Cyber Resilience

The advent of artificial intelligence (AI) has brought a new dimension to the cybersecurity landscape. While many vendors tout AI as a silver bullet for all security problems, Jump offers a measured perspective. "AI is a data manipulation framework," he explains, noting while the technology is not new, its ability to process vast amounts of data quickly can be transformative if used correctly. To him, the promise of AI lies in its capacity to enhance human capabilities rather than replace them. In cybersecurity, AI can help sift through millions of data points to identify the few vulnerabilities that truly matter. "There might be a million vulnerabilities out there, but only a few hundred actually affect your business." By leveraging AI, companies can more efficiently focus their limited resources on protecting the systems that are critical to their operations. However, he cautions against relying solely on technology. "No security product can solve every problem specific to your business." AI, while powerful, is only as effective as the data and context it is given. The key is to integrate AI-driven insights with human expertise, a blend that can accelerate response times and improve the overall resilience of an organisation.

> "THERE MIGHT BE A MILLION VULNERABILITIES OUT THERE, BUT ONLY A FEW HUNDRED ACTUALLY AFFECT YOUR BUSINESS."

Bridging The Gap: Integrating IT And Business Perspectives

A recurring theme with Jump is the need to bridge the often-wide gap between IT professionals and business leaders. In many organisations, these two operate in silos, each with its own language and priorities. Business leaders are primarily focused on profitability and operational continuity, while IT professionals tend to concentrate on technical solutions. This disconnect can lead to misunderstandings and misaligned objectives. "When IT assumes the business knows what it wants and the business assumes IT understands that need, everyone ends up shouting at each other." His solution is simple: bring everyone to the table. By facilitating open dialogue between business leaders, IT staff, and security experts, companies can develop a shared understanding of what matters most.

His approach involves framing cybersecurity in terms that resonate with the entire organisation. Instead of bombarding stakeholders with technical jargon, he emphasises questions like, "What systems are critical to our business?" and "How can we ensure that our most valuable assets remain protected, even under attack?" This conversational approach not only demystifies cybersecurity but also fosters a culture where security is seen as a collective responsibility.

Looking To The Future

When asked about his predictions for the cybersecurity landscape in 2025, Jump's answer was refreshingly straightforward: the most significant threats are not new, but rather the same ones that have persisted over time. "The headline news is rarely about new threats, it's about us forgetting to do what we were supposed to do years ago." His perspective is a reminder that many vulnerabilities stem from basic oversights – failure to manage identities, monitor critical systems, or keep software updated. In a world where the stakes of cybersecurity are higher than ever, these seemingly simple issues can have catastrophic consequences. "Everything old is new again."