FORTRESSES OF THE FUTURE:

THE EVOLUTION OF DATA CENTRE SECURITY

AS AFRICA'S DIGITAL ECONOMY RAPIDLY EXPANDS, THE CONTINENT'S DATA CENTRES FACE A UNIQUE COCKTAIL OF CHALLENGES: FROM SOCIO-POLITICAL INSTABILITY AND CRIME TO CLIMATE EXTREMES AND POWER RELIABILITY. BUT AMID THESE RISKS LIES AN OPPORTUNITY — TO BUILD SECURITY FRAMEWORKS THAT ARE NOT ONLY ROBUST BUT FUTUREPROOFED. INDUSTRY EXPERTS WARREN TILBROOK OF ARUP, CHALON DILBER OF VCA TECHNOLOGY, AND NICO SMIT OF GALLAGHER SECURITY SHED LIGHT ON WHAT IT TAKES TO SECURE THE DIGITAL VAULTS OF AFRICA.

Chalon Dilber, VCA Technology

Nico Smit, Gallagher Security

Warren Tilbrook, Arup

A HIGH-RISK LANDSCAPE

Across the globe, physical data centre security must operate as a multilayered defence system, designed to address both conventional threats and region-specific risks such as theft, vandalism, and political instability.

"There may be a higher risk of physical intrusion and theft in some regions, higher crime rates or socio-economic instability which can translate to an increased risk of physical breaches, theft of equipment (such as copper, diesel for generators), or vandalism," notes Warren Tilbrook, Senior Engineer at Arup. "Political instability and civil unrest in some regions can also pose direct threats to data centre operations and personnel, requiring enhanced physical security measures."

As such, Tilbrook advocates for a Threat and Vulnerability Risk Assessment (TVRA) as a foundational step, which should be used to identify the specific threats to the facility and its associated data assets and set out the security measures required to mitigate the risks to the data centre.

The security perimeter forms the first critical barrier, typically enforced through high-security fencing topped with razor wire, vehicle crash barriers, and controlled pedestrian access points equipped with surveillance and intrusion detection systems. Adequate lighting and Perimeter Intrusion Detection Systems (PIDS) — including fibre-optic sensors and radar — enable early threat detection, while 24/7 surveillance with high-resolution, night-vision-enabled CCTV ensures continuous monitoring.

"A comprehensive network of high-resolution surveillance cameras with night vision capabilities should cover all critical areas, including entrances, exits, data halls, and perimeter fencing, ensuring 24/7 monitoring," says Tilbrook.

Chalon Dilber, EMEA Sales Manager, VCA Technology, adds that, "beyond basic perimeter monitoring, intelligent video analytics offer a more effective first line of defense. Intrusion detection features, utilising virtual tripwires and sophisticated object classification, can differentiate between genuine threats and environmental factors, drastically reducing false alarms. This allows security personnel to focus on real breaches, providing a more effective and efficient response."

Meanwhile, Nico Smit, Sales Manager for Africa, Gallagher Security, advises a thorough perimeter security system complete with barriers, 24/7 on-site guards, and vehicle access control.

"CCTV systems with high-resolution, night-vision-enabled cameras with 360° coverage; video analytics with AI-powered motion detection, facial recognition, and anomaly detection, and remote monitoring with centralised security operations centers (SOCs) for real-time oversight," are also recommended by Smit.

Internally, access control is enforced through biometric systems, mantraps, and role-based restrictions, all of which are logged for auditing and forensic investigation.

"Biometric authentication with fingerprint, iris, or facial recognition for staff entry; Multi-Factor Authentication (MFA) combining ID cards, PINs, and biometrics; and mantraps and airlocks to prevent tailgating and unauthorised piggybacking are also essential for through security," says Smit.

"Implementing strict control over who can enter the facility and specific areas using an enterprise level access control system is essential," agrees Tilbrook. "Using fingerprint scanners, iris scanners, or facial recognition can ensure highly secure access to critical areas like server rooms. Installing mantraps (interlocking doors or secure portals) at critical entry points ensures only one authorised person can enter at a time while implementing programmed access cards that restrict access can do so based on role, time, and area. All access attempts (successful or failed) should be logged."

This layered, proactive approach is essential to safeguard the facility against both opportunistic and orchestrated physical intrusions.

THE THREAT COMES FROM WITHIN

Physical barriers are not enough when the risks are internal. Insider threats, often overlooked, are exacerbated by socio-economic pressures and a diverse workforce.

"While insider threats are a global concern, socio-economic pressures in some African contexts could potentially heighten the risk of employees being coerced or tempted into malicious activities," says Tilbrook. "Managing physical access for a workforce that may include expatriates, local staff, and various contractors requires robust and consistently enforced access control protocols, mindful of diverse cultural backgrounds."

Key to this is multi-factor authentication: something you have (smart cards), something you know (passwords), and something you are (biometric scans).

Smit agrees and suggests that Zero-Trust architecture should be in place even for internal users: "least privilege access, which grant users only the access necessary for their roles, and behavioral analytics that monitor user behavior to detect anomalies (e.g., accessing systems at odd hours)," can all be used to tackle insider threats.

Strict role-based access is essential, alongside anti-tailgating mechanisms such as interlocking doors. Surveillance reinforces these measures: "access control in conjunction with surveillance at all high security transition points ensures that security teams can monitor activity, and forensic evidence is available," adds Tilbrook.

"Identifying and mitigating insider threats requires more than just access logs," asserts Dilber. "Behavioural analysis tools within video analytics can learn typical movement patterns and flag anomalies such as unusual access times or prolonged presence in sensitive areas by authorised personnel. Furthermore, integrating facial recognition analytics with access control systems provides an added layer of verification, ensuring the right person is accessing the right zone at the right time and deterring potential misuse."

KEEPING TENANTS IN THEIR LANE

Africa's growing cloud adoption is driving up demand for multi-tenant data centres (MTDCs), where co-location introduces the risk of cross-tenant breaches.

"In multi-tenant environments, maintaining strict segregation is crucial," outlines Dilber. "Video analytics can enhance access control by using tailgating detection analytics to ensure only authorised individuals enter secure areas."

"Managing access in multi-tenant data centres (MTDCs) is a challenging security environment that requires physical and technical solutions that ensure strict isolation and control for each

tenant to maintain segregation and ensure the security integrity of each tenant," warns Tilbrook.

In addition to the security layers for the facility as a whole, physical segregation and access control within co-location spaces is paramount. Dedicated, physically secured cages or private suites for each tenant within the data hall allow tenants to implement their own electronic security measures such as access control and video surveillance that are independent of the main facility security systems. Access to these areas must be restricted to authorised personnel of that specific tenant, says Tilbrook, enforced through individual locks, card readers, and potentially biometric scanners specific to the cage/suite.

Smit calls for local segmentation: "virtual LANs (VLANs) and Software-Defined Networking (SDN) to isolate tenant traffic, and microsegmentation to enforce granular security policies. For physical segmentation, dedicated racks or cages for each tenant and separate biometric access zones for different tenants are effective."

"For physical keys to racks, using smart key cabinets that log who takes a key, when, and for which rack, often requiring authentication can restrict rack access," Tilbrook. "This can also be controlled using specialist rack access control hardware; compartmentalised racks are also available giving further granular control over access to equipment."

Moreover, video analytics steps in again to address potential slip-ups. "By integrating video verification and/or facial recognition with access logs, data centres can create a robust audit trail of entries and exits, providing granular control and preventing unauthorised cross-tenant access to sensitive infrastructure." These tools offer instant video verification — making it clear who entered, when, and whether they were allowed to.

EARLY THREAT DETECTION

Security today isn't just about locking doors — it's about being everywhere, all the time.

"Integrating real-time system monitoring and early fault detection into security protocols is critical for rapid response and minimal disruption. Unified Monitoring Systems - a centralised platform for monitoring both physical and cybersecurity events - provide a holistic view of the data centre's security posture and allows rapid response to security events in real time," explains Tilbrook.

Video analytics is the ultimate enabler in this environment.

"Minimising downtime requires proactive security measures. Real-time event detection capabilities within video analytics can identify security-related events as they happen – from unauthorised entry attempts to suspicious object placement," agrees Dilber. "Immediate alerts allow security teams to respond swiftly, potentially preventing a minor breach from escalating into a system-wide failure and significantly minimising operational disruptions."

According to Tilbrook, deploying advanced DCIM solutions provides real-time visibility into power, cooling, environmental conditions (temperature, humidity), and asset status. Security Information and Event Management (SIEM) systems collect and correlate log data from various security devices (firewalls, IDS/IPS, access control systems) and IT infrastructure (servers, network devices). Real-time analysis can detect patterns indicative of a security breach in its early stages.

At the heart of it all is the Security Operations Centre (SOC) — a mission-control hub for physical and cyber defence.

"The data centre Security Operations Centre (SOC) is a centralised command unit responsible for the ongoing monitoring, detection, analysis, and response to cybersecurity threats and incidents targeting a data centre's infrastructure and the information it houses. It serves as the hub for all security-related activities, ensuring the confidentiality, integrity and forms an essential part of the security apparatus," asserts Tilbrook.

EFFICIENCY VS. SECURITY

Building a secure data centre without crippling operational efficiency is possible — if smart automation is in place.

"Achieving a balance between operational efficiency and robust security hinges on intelligent automation. A suite of video analytic tools, including loitering detection, object classification, and people counting, automates the monitoring process, freeing up security personnel to focus on higher-level tasks and incident response. This intelligent surveillance optimises resource allocation while simultaneously enhancing security posture, creating a more resilient and efficient operation against evolving threats," says Dilber.

Tilbrook agrees that efficiency and resilience go hand-in-hand with planning. "A risk-based approach to security is the foundation of implementing a robust and cost-effective set of security measures that protect the data assets of customers and ensure resilience and reliability."

According to Smit, best practices include:

- Security by design: integrate security into the architecture from the ground up.
- Regular audits and penetration testing: identify and fix vulnerabilities proactively.
- Staff training and awareness: educate employees on security protocols and social engineering threats.
- Redundancy and failover systems: ensure uptime even during attacks or failures.
- Compliance with standards: align with ISO/IEC 27001, Uptime Institute, and local regulations.

Finally, Tilbrook reminds us that human readiness is still paramount: "in addition to physical protection measures data centre operators must ensure that there is a highly effective operational security presence on site and an emergency response plan that works alongside local law enforcement and emergency first response agencies. Having a 24hr security presence on site with well trained and well-paid security personnel with the well-designed security measures are the best protection against these risks."

AFRICA'S DIGITAL BACKBONE

As Africa's data economy continues to thrive, so too does the need for vigilant, adaptive security strategies. From robust fences and biometric locks to AI-powered surveillance and predictive analytics, the battle for data security is increasingly fought on multiple fronts.

Africa's data centres aren't just building for scale — they're building for resilience. And if experts like Tilbrook and Dilber are any indication, the future of data in Africa may well be one of the most secure on the planet. ●