2026: The year IoT became core infrastructure

By 2026, IoT is core infrastructure: only engineered, resilient, multi-network connectivity - not basic links - will scale and protect business operations.

CAPE TOWN, WESTERN CAPE, SOUTH AFRICA, February 4, 2026 /EINPresswire.com/ -- For much of the past decade, the Internet of Things (IoT) has been discussed in terms of devices: sensors, trackers, cameras, terminals. How many are deployed, how clever they are, how much data they generate. But, according to Ross Hickey, CEO and founder, Trinity, an IoT service provider, that conversation is over as IoT crosses a threshold and is no longer an innovation layer sitting on the periphery of the business: "IoT today is core operational infrastructure, on par with payments rails, fleet systems, and enterprise networks."

And, when it fails, Hickey says that operations stop, revenue is impacted, risk increases, and reputational damage follows quickly. "The organisations that understand this shift are pulling ahead. Those that don't are discovering, often painfully, that connectivity without strategy does not scale."

Ross Hickey, CEO and founder, Trinity

From "connected" to engineered

> IoT today is core operational infrastructure, on par with payments rails, fleet systems, and enterprise networks"
> *Ross Hickey, CEO and founder, Trinity*

The early phase of IoT was about getting things online. A SIM, a data plan, a dashboard. Hickey says that the model worked when deployments were small and non-critical but moving forward it no longer holds.

"Modern IoT environments demand ISP-grade thinking: private APNs instead of public internet exposure, deterministic routing instead of best-effort delivery, and redundancy built into the network layer rather than bolted on after the fact. This is especially true in sectors like telematics, fintech, logistics, and security,

where milliseconds, uptime, and data integrity directly affect business outcomes," says Hickey.

The question, he says, that leaders should be asking today is not "Is it connected?" but "Is it engineered to survive failure?"

Multi-MNO is now a business requirement

One of the most significant changes is the decline of single-network dependency. Relying on one mobile network operator might simplify procurement, but it introduces a structural risk that becomes unacceptable at scale.

By 2026, Hickey says that resilient IoT strategies are built on multi-MNO architectures. Not roaming as a fallback, but intelligent aggregation that actively selects the best available network, supports seamless failover, and removes single points of failure.

"This shift is being driven from the top down. Boards and executive teams increasingly recognise that network diversity is not a technical detail. It is a risk management decision," says Hickey.

Edge intelligence raises the bar for networks

As AI and automation move closer to the edge, IoT devices are no longer just reporting data. They are making decisions in real time.

That capability depends entirely on the network beneath it. Latency, jitter, packet loss, and congestion are no longer abstract technical metrics; they are business constraints. A network that is "usually good enough" is not good enough when decisions are happening in milliseconds.

Hickey says that edge intelligence demands deterministic, predictable connectivity: "This is where bespoke networking outperforms generic internet paths every time."

Why DIY IoT breaks at scale

Most organisations begin their IoT journey in-house. It feels agile. It feels cost-effective. And initially, it often is. But, according to Hickey, the problem emerges with growth. "As deployments expand, DIY IoT environments become fragmented. Visibility is split across platforms. Troubleshooting becomes reactive. Internal teams spend more time managing connectivity than delivering value, and support escalations turn into ticket queues rather than rapid resolutions."

At that point, many organisations realise they didn't just deploy IoT, they accidentally became a network operator. And that is rarely where their competitive advantage lies.

Support is becoming a differentiator

When IoT underpins operations, support models matter. Logging a ticket and waiting in a call centre queue is acceptable for non-critical services. It is not acceptable when fleets are idle, payments are failing, or security systems are degraded.

"In 2026, leading enterprises are demanding a different relationship: proactive monitoring, named engineering support, and direct access to people who understand their environment. In other words, speed dial rather than a ticket number," explains Hickey.

He says that this mirrors what is already seen in cloud and financial infrastructure. IoT is following the same maturity curve.

Turnkey beats tinkering

The most successful IoT programmes share one trait: they are deliberately boring at the network layer.

Connectivity, monitoring, redundancy, and MNO management are treated as utilities, delivered as a managed service with predictable costs and clear accountability. This frees internal teams to focus on what differentiates the business: products, data, customer experience.

"Turnkey does not mean inflexible. It means designed, supported, and scalable by default. IoT is no longer a side project. It is infrastructure. By 2026, the organisations that win will be those that treat it as such: engineered for resilience, designed for scale, and supported as a critical business system. The rest will continue to learn the hard way that connectivity alone is not a strategy," says Hickey.
Ends.

SJ Hogg-Brandjes
GinjaNinja PR (Pty) Ltd
+27 82 940 9730
email us here

This press release can be viewed online at: https://www.einpresswire.com/article/888962954