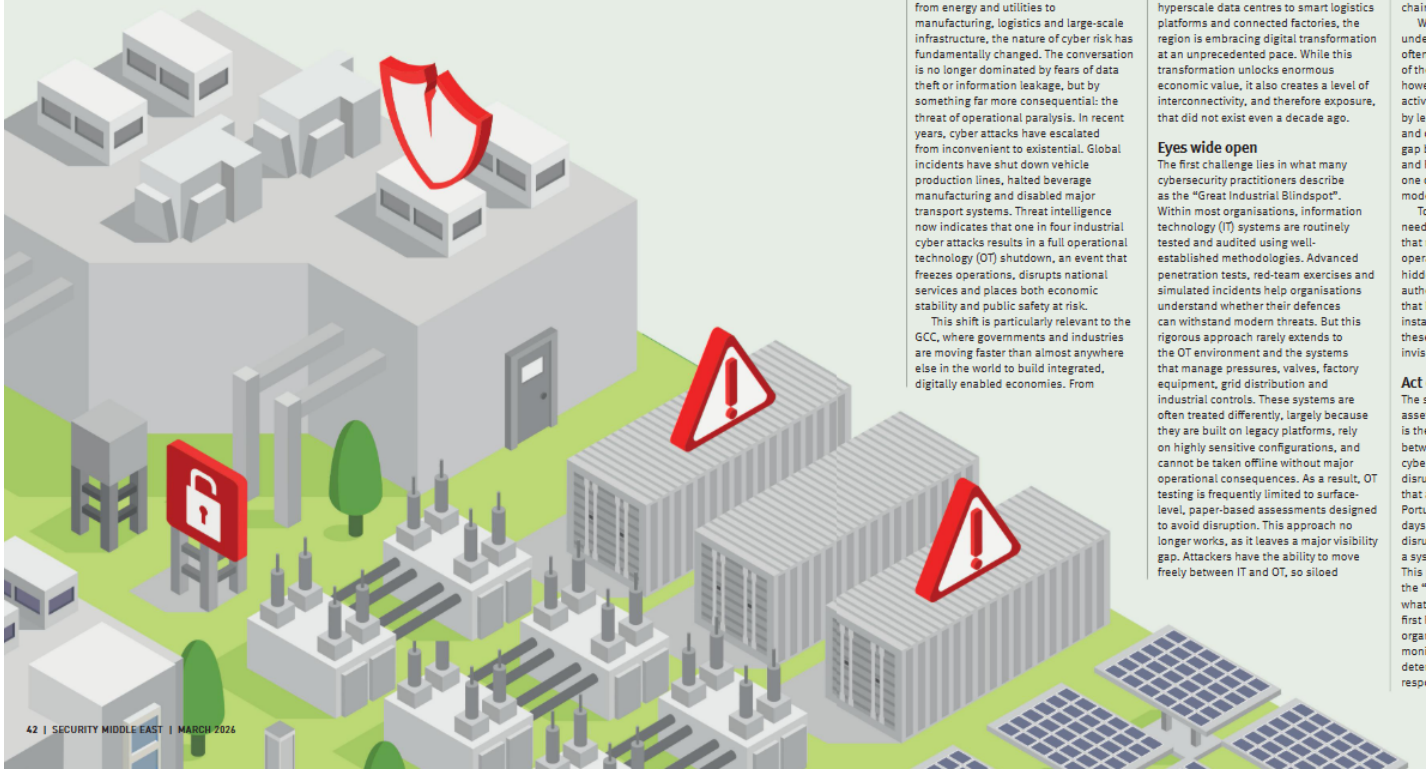
CYBERSECURITY | INDUSTRIAL ASSETS

The shift from data theft to operational paralysis

David Dunn, Head of Cybersecurity, EMEA and APAC; **Nebu Varghese**, Senior Director, Cybersecurity, both FTI Consulting; and **Vijay Velayutham**, Principal Information Security Officer, UAE Ministry of Energy & Infrastructure, look at the cyber risks facing industrial assets in the GCC



Across the GCC's industrial landscape, from energy and utilities to manufacturing, logistics and large-scale infrastructure, the nature of cyber risk has fundamentally changed. The conversation is no longer dominated by fears of data theft or information leakage, but by something far more consequential: the threat of operational paralysis. In recent years, cyber attacks have escalated from inconvenient to existential. Global incidents have shut down vehicle production lines, halted beverage manufacturing and disabled major transport systems. Threat intelligence now indicates that one in four industrial cyber attacks results in a full operational technology (OT) shutdown, an event that freezes operations, disrupts national services and places both economic stability and public safety at risk.

This shift is particularly relevant to the GCC, where governments and industries are moving faster than almost anywhere else in the world to build integrated, digitally enabled economies. From advanced renewable energy grids and hyperscale data centres to smart logistics platforms and connected factories, the region is embracing digital transformation at an unprecedented pace. While this transformation unlocks enormous economic value, it also creates a level of interconnectivity, and therefore exposure, that did not exist even a decade ago.

Eyes wide open

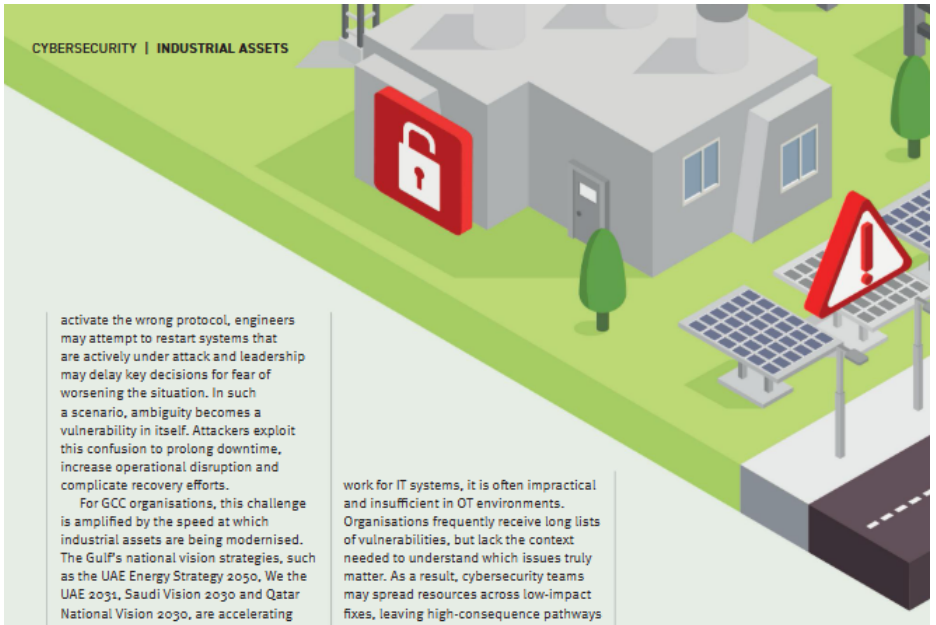
The first challenge lies in what many cybersecurity practitioners describe as the "Great Industrial Blindspot". Within most organisations, information technology (IT) systems are routinely tested and audited using well-established methodologies. Advanced penetration tests, red-team exercises and simulated incidents help organisations understand whether their defences can withstand modern threats. But this rigorous approach rarely extends to the OT environment and the systems that manage pressures, valves, factory equipment, grid distribution and industrial controls. These systems are often treated differently, largely because they are built on legacy platforms, rely on highly sensitive configurations, and cannot be taken offline without major operational consequences. As a result, OT testing is frequently limited to surface-level, paper-based assessments designed to avoid disruption. This approach no longer works, as it leaves a major visibility gap. Attackers have the ability to move freely between IT and OT, so siloed penetration tests fail to reveal real kill chains or critical interdependencies.

While IT teams gain a deep understanding of real threats, OT teams often receive only a lightly annotated list of theoretical vulnerabilities. Attackers, however, have no such hesitation. They actively hunt for the weak points created by legacy software, unpatched systems and outdated operational processes. The gap between how IT and OT are tested, and how threats actually unfold, is now one of the most significant weaknesses in modern industrial cybersecurity.

To address this gap, organisations need end-to-end attack simulations that mirror how adversaries actually operate. These exercises can expose hidden OT dependencies on IT, such as authentication or scheduling systems, that have potential to halt operations instantly. Without proactive stress testing, these vulnerabilities could remain invisible until a real incident occurs.

Act quickly

The second challenge facing industrial assets when it comes to cybersecurity is the inability to quickly distinguish between a technical fault and a cyber attack in the early moments of disruption. Last year's power outage that affected large parts of Spain and Portugal illustrates this problem. For days, organisations debated whether the disruption stemmed from a software fault, a systems glitch or a targeted attack. This period of uncertainty, described as the "Initial Ambiguity Crisis", is exactly what threat actors rely on. In the critical first hours of an industrial disruption, organisations without integrated monitoring across IT and OT struggle to determine what is happening, let alone respond effectively. Crisis teams may



activate the wrong protocol, engineers may attempt to restart systems that are actively under attack and leadership may delay key decisions for fear of worsening the situation. In such a scenario, ambiguity becomes a vulnerability in itself. Attackers exploit this confusion to prolong downtime, increase operational disruption and complicate recovery efforts.

For GCC organisations, this challenge is amplified by the speed at which industrial assets are being modernised. The Gulf's national vision strategies, such as the UAE Energy Strategy 2050, We the UAE 2031, Saudi Vision 2030 and Qatar National Vision 2030, are accelerating the deployment of interconnected OT, IT and Industrial Internet of Things (IIoT) systems across critical sectors. This includes renewable energy farms being linked to national grids, AI-powered data centres being built at hyperscale, factories connecting their machinery to the cloud to improve efficiency and competitiveness, and logistics and mobility systems becoming part of integrated smart city networks. While these advancements strengthen national capabilities, they also create a deeply interconnected attack surface unlike anything the region has managed before. Traditional industrial risks, which were once limited to oil and gas, utilities and core manufacturing, now extend to solar farms in the desert, remote hydrogen facilities, digital substations and highly automated production lines. The emergence of AI-driven hyperscale data centres adds further complexity, as these facilities rely on advanced cooling and specialised power systems managed with digital controls, often with third-party access. Every new connection strengthens operational capabilities, but simultaneously opens potential pathways for threat actors to exploit.

Identifying where to act

For many industrial companies, the current approach to cybersecurity remains overly focused on reducing the probability of an attack by attempting to fix every vulnerability. While this approach may work for IT systems, it is often impractical and insufficient in OT environments. Organisations frequently receive long lists of vulnerabilities, but lack the context needed to understand which issues truly matter. As a result, cybersecurity teams may spread resources across low-impact fixes, leaving high-consequence pathways that could lead to operational shutdown to go unaddressed. Instead of focusing on all theoretical vulnerabilities, we believe that organisations must focus on identifying and securing the small number of attack paths that could realistically lead to catastrophic operational failure. This requires threat intelligence-led assessments that prioritise vulnerabilities based on real-world attacker behaviour, not theoretical models. By understanding how adversaries are targeting similar organisations, what techniques are being used and how attackers move between interconnected systems, cybersecurity leaders can direct resources to the most significant vulnerabilities.

Match action to priorities

Real resilience is developed by stress-testing the entire ecosystem – IT, OT, cloud, supply chain and crisis response – against realistic attacker scenarios. Many organisations conduct tabletop exercises, but these are often too theoretical to expose the operational, procedural and technical gaps that emerge during real incidents. What is needed is the industrial equivalent of a dress rehearsal — an integrated war game. Unlike standard red teams, this full-spectrum stress test safely simulates a live attack across the entire interdependent ecosystem. It hits the IT network, probes sensitive OT controls, tests supplier connections, and – crucially – triggers a real-time crisis for the leadership team. These exercises force the business to confront the reality of an attack: how quickly are anomalies detected? Can engineers distinguish a cyber attack from a technical fault? Does the C-suite know how to make decisions when data is compromised? This is how organisations can build the 'muscle memory' required to act decisively. It shifts the posture from theoretically prepared to proven in practice and under pressure.

As the GCC continues its rapid industrial transformation, the region's cyber priorities must evolve just as quickly. The threats facing industrial assets today are more interconnected, sophisticated and operationally disruptive than anything the region has faced before. Protecting critical infrastructure is no longer just a technical challenge; it's a strategic imperative that demands leadership attention, cross-functional collaboration and sustained investment.

The organisations that recognise this shift and take action will be the ones best positioned to safeguard not only their own operations, but the broader economic ambitions of the GCC. Those that delay may find themselves navigating a threat landscape in which the cost of inaction grows exponentially with every new connection, asset and digital capability added to the industrial ecosystem. ■

fticonsulting.com