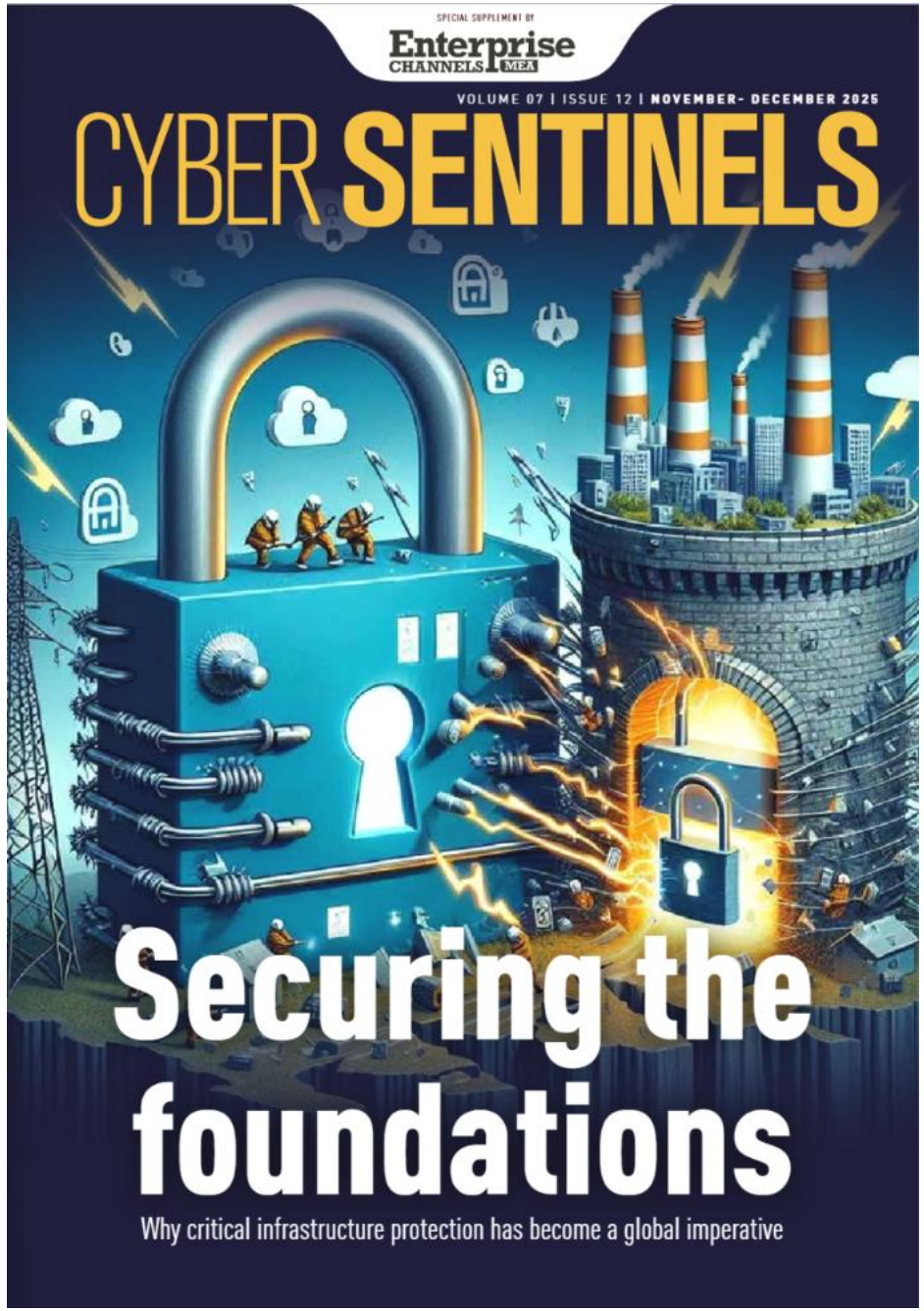
SPECIAL SUPPLEMENT BY
Enterprise CHANNELS MEA
VOLUME 07 | ISSUE 12 | NOVEMBER- DECEMBER 2025

CYBER SENTINELS



Securing the foundations

Why critical infrastructure protection has become a global imperative

Securing the foundations

Why critical infrastructure protection has become a global imperative

As digital transformation accelerates across essential sectors — from energy and water to telecommunications and transport — critical infrastructure security has moved to the forefront of national and organisational priorities. The rapid convergence of operational technology with modern IT ecosystems has created extraordinary opportunities but also alarming vulnerabilities. Industry experts across the region are sounding the alarm: the stakes have never been higher.

Harish Chib, Vice President Emerging Markets, Middle East & Africa, Sophos, says "Critical infrastructure security has become a top priority because attacks in sectors like energy, telecommunications, and transportation can have severe, wide-ranging impacts." He explains that ransomware and related threats have evolved, now targeting operational continuity rather than just stealing or encrypting data.

The consequences can be catastrophic. "An attack on the energy sector can cause blackouts affecting millions, a telecommunications breach can disrupt national communications, and transportation incidents can halt the movement of goods and people," he adds. As a result, "operational availability is just as critical as data protection," driving Sophos' focus on advanced technology, continuous monitoring, and proactive risk management.

Ahmad Ali, Principal OT & IoT Solution Architect, Solutions Architecture at Help AG, reinforces this urgency, noting that "critical infrastructure security is a top priority due to the increasing reliance on digital systems and interconnected technologies." As essential services become more digitized, their exposure increases. He warns that a successful attack "can cause widespread disruptions, economic damage, and even threats to national security," underscoring the need for proactive security to ensure continuity and resilience.

Ahmad Ali,
Principal OT & IoT Solution Architect, Solutions Architecture, Help AG

Harish Chib,
Vice President Emerging Markets, Middle East & Africa, Sophos

Kalle Bjorn, Senior Director, Systems Engineering Middle East, Fortinet, expands on the challenge: "Operational Technology (OT) systems are the backbone of critical infrastructure," and while digital transformation has delivered major benefits, it has also "increased the attack surface for cybercriminals." Attacks on OT environments can compromise industrial processes, critical equipment, and even public safety.

He notes that governments worldwide are tightening cybersecurity regulations for OT and ICS, emphasizing "stricter security directives, incident reporting requirements, and a focus on building resilience against cyber incidents."Effective protection, he stresses, requires "constant vigilance and resource allocation."

A new generation of threats

Threat actors targeting critical infrastructure are becoming more sophisticated, more persistent, and more diverse. Saif Alrefai, Solutions Engineering Manager, OPSWAT, says "the threat landscape is formidable due to the convergence of these dangers." Ransomware continues to cripple hospitals, utilities, and transport networks, where downtime can carry life-or-death implications. Nation-state APTs represent another escalating risk, targeting vital data, operational processes, and strategic intellectual property.

Saif highlights growing concern around supply chain infiltration, noting that attackers increasingly "weaponise trust" by breaching third-party vendors to gain indirect access. As IoT devices proliferate across smart grids and transport systems, this expanding perimeter becomes even harder to defend.

Harish adds that ransomware remains

Kalle Bjorn,
Senior Director, Systems Engineering Middle East, Fortinet

Saif Alrefai,
Solutions Engineering Manager, OPSWAT

especially concerning in critical sectors like energy and water. He cites findings from their report showing that "67% of organizations in these sectors were impacted by ransomware last year, with median recovery costs quadrupling to $3 million." Nearly half of these attacks leveraged known vulnerabilities — a clear sign that organisations must adopt stronger risk management practices. State-sponsored threat actors complicate matters further, with varied motivations ranging from destabilisation to espionage and financial theft.

Ahmad echoes these concerns, emphasizing that "nation-state actors and ransomware groups are the most concerned about threats today." While insiders may attract less attention, they still pose "a significant risk," capable of enabling or directly executing damaging attacks.

IT–OT convergence: A new attack surface

The blending of IT and OT systems has redefined the cybersecurity landscape for critical infrastructure. Kalle notes that many OT systems "are decades old and were originally designed to work in relative isolation." But as organisations digitally transform, the traditional air gap has eroded. OT environments now face threats historically confined to IT. "Many OT disruptions occur because of attacks on linked IT systems," he explains, stressing the need for integrated defences. Fortinet addresses this challenge through its Security Fabric, offering "unified visibility, threat intelligence, and automated response" across converged networks.

Saif from OPSWAT adds that the challenge is balancing connectivity with security. Industrial environments are increasingly connected to cloud services and AI-driven analytics, expanding both operational capabilities and the attack surface. Securing these ecosystems means protecting everything from USB ports to remote gateways, monitoring IT–OT data flows, and exercising stringent control over third-party access. Even temporary assets such as laptops entering a facility must be inspected. "Each connection can be a potential vulnerability," OPSWAT cautions, and the ultimate goal remains "seamless data flow without compromising security."

The critical role of incident response

As attacks grow more frequent and more sophisticated, incident response planning has become indispensable. Ahmad from Help AG says "Incident response planning is critical for minimizing the impact of cyberattacks on critical infrastructure." He emphasises the need for clear communication protocols, regular drills, segmentation to contain breaches, and a structured response plan that moves from rapid detection to full recovery. Lessons learned must feed continuous improvement.

Kalle reinforces this point: with escalating cyber threats, "an incident response plan plays an increasingly important role in a critical infrastructure operator's security defence." Preparation is paramount, as it "determines how well an organization will be able to respond in the event of an attack." He outlines key requirements: defined policies, a chosen response team, controlled access, tooling, training, and a comprehensive strategy covering identification, containment, eradication, recovery, and lessons learned. The plan must be regularly updated to reflect evolving risks and operational realities.

The role of frameworks and certifications

As threats accelerate, organisations are turning to global standards to strengthen their cyber foundations. Ahmad says "certifications and frameworks like NIST, IEC, and NERC provide standardized guidelines for securing critical infrastructure." He explains that these frameworks help organisations adopt best practices, improve risk management, and ensure regulatory compliance. By following structured standards, companies "can raise their security baseline, ensure continuous improvement, and demonstrate to stakeholders that they are proactively managing cybersecurity risks."