REGULATION, *skills*, SHOCKS *and* RESILIENCE

The Middle East's security ecosystem is undergoing a seismic transformation, write SSR Personnel's Peter French MBE and Andrew Hudson

The convergence of AI, workforce realignment and escalating climate threats presents both operational vulnerabilities and strategic opportunities. For security executives, policymakers and operators, understanding how these forces interact is no longer optional: It is essential to designing resilient urban and organisational frameworks for the future.

AI regulation

AI adoption across the Gulf Cooperation Council (GCC) and wider Middle East is advancing rapidly. Governments are investing heavily in AI-driven urban management, predictive policing, cybersecurity and critical infrastructure automation. Yet, regulatory regimes remain uneven.

Saudi Arabia's Saudi Data and Artificial Intelligence Authority (SDAIA) has issued AI Ethics Principles and Generative AI Guidelines, reflecting a proactive stance toward governance, transparency and human oversight. The UAE pursues a business-friendly AI regulatory environment through the National Strategy for Artificial Intelligence 2031, including sandbox frameworks, pilot licences and data governance requirements.

> **"For security executives, policymakers and operators, understanding how these forces interact is no longer optional."**

Bahrain and Qatar are codifying AI legislation, focusing on accountability, liability and ethical compliance in sensitive sectors. The Bahrain Labour Fund, Tamkeen, partnered with the SANS Institute to deliver specialised cybersecurity training. 25% of graduates from its first cohort secured local and international employment opportunities within weeks of graduating.

Despite frameworks, regulatory enforcement is inconsistent, leaving gaps in algorithmic accountability, model robustness verification and real-time audit capacity. The challenge is compounded by the speed of AI innovation: Untested generative AI deployments, automated decision-making in high-risk domains and insufficiently trained regulatory personnel are introducing systemic exposure.

When the UAE announced its AI strategy in 2017, it became the first country in the world to appoint a Minister of State for Artificial Intelligence, His Excellency Omar Bin Sultan Al Olama. This bold move signalled the UAE's intent to integrate AI across government operations, infrastructure and public services. Regional collaboration – through shared AI incident monitoring, with strategic MoU and public-private partnerships – is emerging as a critical enabler of harmonised oversight and risk mitigation.

Strategic reframing

The convergence of AI, workforce evolution and climate volatility is catalysing a fundamental paradigm shift: Security is no longer solely about protection – it is about resilience. Resilience encompasses anticipatory threat detection, adaptive operational continuity and rapid recovery. Operationalising resilience requires a multi-layered approach:

- **Predictive risk intelligence –** AI-driven models analyse flood patterns, infrastructure fragility, supply chain vulnerabilities and threat vectors to pre-empt operational disruption
- **Regulatory integration –** enforceable standards for AI deployment, infrastructure safety and business continuity embed resilience into governance frameworks
- **Workforce adaptability –** upskilling in AI ethics, model auditing, crisis response and multi-domain operational planning ensures human oversight complements automated systems.

Forecasting up to 2030

In the Middle East, cybersecurity incidents cost an average of $8.05m per breach, almost double the global average of $4.45m, according to the World Economic Forum. Against this backdrop, GCC countries are taking decisive steps to boost their digital defences. By 2030, the cyber-threat intelligence market in the Middle East is set to reach upwards of $3lb. AI deployment will be subject to enforceable standards covering liability, safety, auditing and transparency.

Security professionals will need competencies in crisis management, climate adaptation, cyber-physical integration and AI oversight. Flood defences, smart water systems, resilient transport and energy redundancy will become core priorities. Organisations that invest in reskilling and cross-disciplinary development will achieve operational superiority. ▸

AI in the UAE

The United Arab Emirates has positioned itself at the forefront of the global AI movement, transforming ambition into action through strategic policy, education and innovation. Since the launch of the UAE Strategy for Artificial Intelligence in October 2017, the nation has redefined what it means to prepare for a future driven by intelligent technologies.

The strategy marks what leaders have called the "post-mobile government phase," one that depends on automation, data and innovation rather than traditional digital transformation. According to government estimates, by 2030, AI will contribute $15.7t to the global economy – and the UAE aims to capture a significant share of that growth, potentially boosting national GDP by 35% while cutting government costs in half.

In April 2025, the UAE government, in partnership with Microsoft, launched an ambitious nationwide initiative titled "1 million AI Talents." The goal is to equip one million people, from public sector leaders to everyday citizens, with AI knowledge and practical skills. Beginning in the 2025/2026 academic year, AI became a mandatory subject in all UAE public schools, from kindergarten through Grade 12. This initiative supports the broader UAE National Strategy for Artificial Intelligence 2031, preparing students for a workforce increasingly shaped by automation and intelligent systems.

In May 2025, Abu Dhabi and the US announced a landmark deal to build an AI super campus, which will become the largest AI infrastructure outside the US, with a capacity of 5 gigawatts. The project includes Stargate UAE, a IGW data cluster developed by the state-backed tech company G42 in collaboration with OpenAI, Oracle, NVIDIA, Cisco and SoftBank. The agreement also includes ChatGPT Plus subscriptions for the entire UAE population.

Saudi Arabia's AI revolution

The next frontier in Saudi Arabia's AI journey is generative AI, which has the potential to reshape industries and boost economic output. According to research by Oliver Wyman, part of Marsh McLennan, generative AI could contribute between SAR 60b and SAR 90b to KSA GDP by 2030.

"Across the Middle East, a quiet but powerful shift is taking place in how businesses think about security."

While automation will inevitably transform some job roles, particularly those involving repetitive tasks, the overall shift is expected to increase demand for higher-level skills such as problem-solving, creativity and innovation. This transition reflects the Kingdom's broader aim: To build a resilient, future-ready workforce capable of thriving in an economy driven by data and intelligence.

Security to resilience

Across the Middle East, a quiet but powerful shift is taking place in how businesses think about security. The mindset of simply defending against threats is giving way to a more strategic focus on resilience, the ability to anticipate, withstand and bounce back from disruption. This evolution is being driven by rapid digital transformation, increasingly complex risks and the understanding that prevention alone is no longer enough to guarantee stability in an unpredictable world.

Rather than relying solely on reactive security measures, organisations are beginning to design systems that can adapt and recover when a crisis inevitably occurs. Whether those stem from cyber-attacks, geopolitical shocks or environmental disruptions. This marks a transition from a "protect and respond" mentality to a culture of "prepare, adapt and thrive."

A PwC survey highlights how seriously Middle Eastern organisations are taking resilience: 91% of business leaders in the region say that building resilience is now one of their top strategic priorities. What's more, four in ten organisations have already set up dedicated, cross-functional resilience teams that bring together experts from areas like business continuity, cybersecurity, crisis response and risk management – a higher adoption rate than the global average of 34%.

Executives now also recognise that cybersecurity and operational continuity are essential to safeguarding reputation, maintaining customer trust and ensuring long-term competitiveness. Real strength lies not in avoiding every threat, but in being able to recover quickly and continue delivering value no matter what comes next. ■