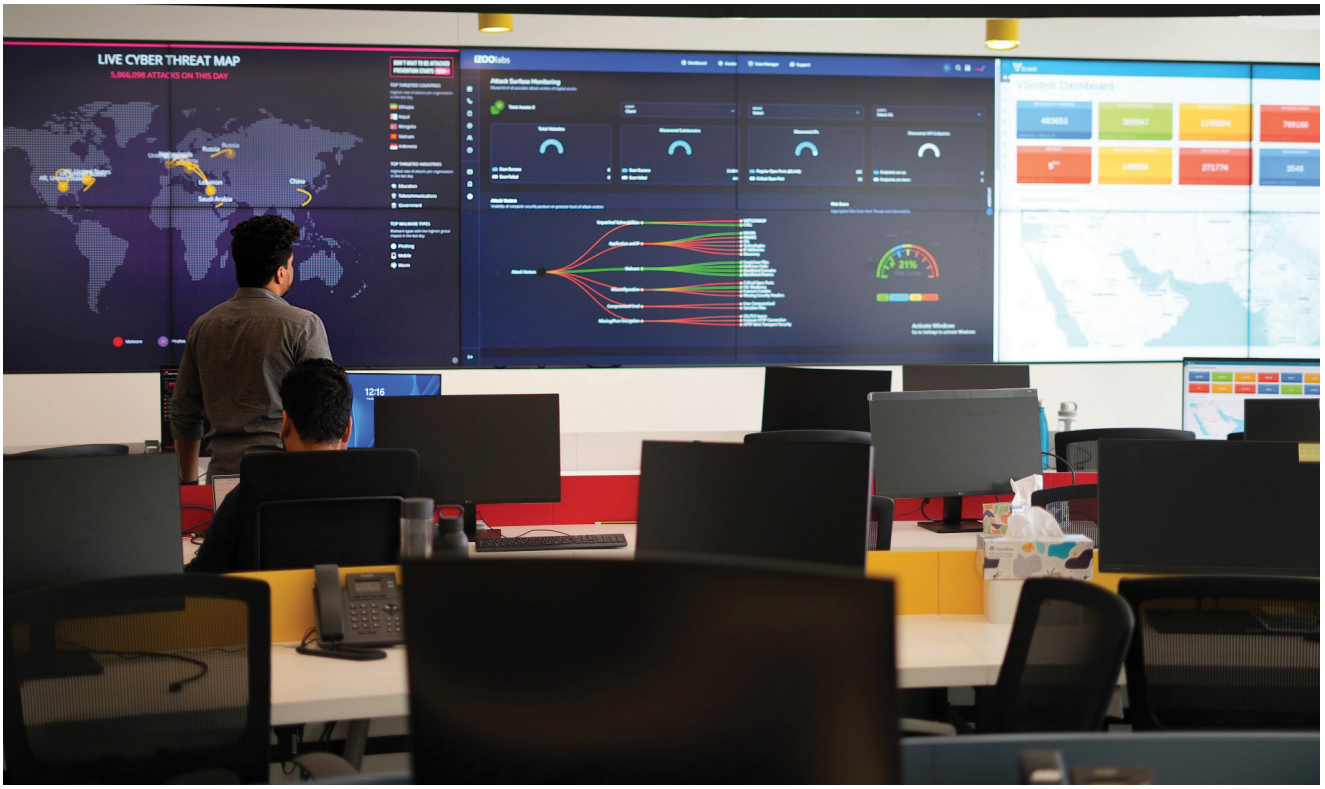

Pics: Supplied

Staying ahead of AI-driven cyber threats

PARAMOUNT COO **ASHOK CHANDRASEKHARAN** OUTLINES RISING AI-DRIVEN CYBER THREATS IN THE MIDDLE EAST AND HOW BUSINESSES CAN BUILD RESILIENCE

BY NEESHA SALIAN

Founded in 1992, Paramount has grown into one of the region's leading pure-play cybersecurity firms. Headquartered in the UAE, the company operates across seven countries and supports over 350 clients spanning government, banking, healthcare, telecom, retail, and energy. Its 550 cybersecurity professionals deliver services ranging from next-generation SOC operations and data governance to AI-enabled risk management, helping organisations build resilience in an era of fast-changing digital threats.

As cyberattacks grow more sophisticated and the Middle East accelerates its digital transformation, businesses are under pressure to protect critical data and infrastructure. Here, Ashok Chandrasekharan, chief operations officer of Paramount, explains the most pressing risks facing UAE and GCC businesses, how the company is adapting to artificial intelligence (AI)-powered threats, and the role the company plays in securing both government and private ecosystems.

Q Cybersecurity threats are evolving rapidly in the Middle East. What are the most pressing risks businesses in the UAE and wider GCC face today?

We live in a time when every business relies on advanced technology and hackers know it. In places like the UAE and the wider GCC, digital transformation has moved faster than security practices, making the region a prime target. Cyberattacks have evolved; it's no longer just about breaking into systems. Now, it's about exploiting trust, speed, and the complex web of interconnected networks we depend on.

With the emergence of AI, the game has changed completely. These aren't the slow, predictable threats of the past. AI-powered attacks can learn and adapt in real time, unleashing precise, high-speed intrusions that are unlike anything we have dealt with before.

Supply chain attacks are one of the biggest risks. Hackers go after trusted vendors, cloud services, or ERP systems to quietly slip in. We've seen a sharp rise in data exfiltration, ransomware, and credential sales on the dark web. Ransomware incidents alone are rising 32 per cent in the UAE and 58 per cent across the Gulf, with industries like healthcare, telecom, and oil being hit the hardest. The average cost of a breach in

> **AI WILL STRENGTHEN GOVERNANCE, WITH GOVERNMENTS SETTING STANDARDS FOR PRIVACY AND ETHICS. BUSINESSES MUST QUICKLY ADAPT, EMBEDDING COMPLIANCE INTO RISK STRATEGIES."**

this region is around $8.05m, almost double the global average.

Phishing and social engineering remain the most common entry points, accounting for 98 per cent of successful attacks. In 2024 alone, weak passwords and risky public Wi-Fi habits caused several incidents. Every day, we see about 500 alerts, 70–80 of which turn into real threats. Most are phishing or insider-related, especially in finance and government sectors. With the region facing about 10 per cent of all global cyberattacks, smarter AI-powered detection tools and employee training are no longer optional.

Paramount has been in the cybersecurity space for decades. How has your approach adapted to new technologies like AI-driven threats and cloud security?

For 30 years, Paramount has grown from tackling basic tech threats to securing complex business ecosystems where one breach can stop everything. Today, we support more than 350 clients across seven countries with a team of 550 experts.

The shift to cloud computing brings scalability and speed, but it also opens misconfigurations and access points that attackers exploit. Meanwhile, AI-driven attacks are getting faster and more sophisticated, slipping past traditional defenses. That's why at Paramount we use a layered defense strategy: conditional access policies, role-based controls, and EDR/XDR solutions for hybrid environments.

We also apply AI across SIEM, IDS/IPS, and DLP for behaviour monitoring and rapid automated responses. This reduces false positives and lets us respond to serious incidents in minutes. Our comprehensive approach is formalised in the Paramount AI Framework, built on four pillars: AI governance, Securing AI, AI-driven cybersecurity, and data/integration security.

The framework addresses emerging risks like model poisoning while ensuring compliance with global regulations. We recently presented it at the Gartner Security and Risk Management Summit, where it was recognised as a blueprint for resilience in an AI-driven future. Supported by a regional cybersecurity market projected to grow from $3.27bn in 2025 to $5.87bn by 2030, this approach has helped us sustain 30 per cent growth.

With Dubai pushing digital transformation across government and private sectors, what role do you see Paramount playing in securing this ecosystem?

Governments across the GCC are at the forefront of AI adoption, with the UAE standing out under its 'We the UAE 2031' vision. As national infrastructure and public services digitise, securing such a connected ecosystem demands advanced capabilities.

Paramount provides those capabilities with more than 100 SOC analysts working 24/7, proactive risk assessments, employee training, and digital risk protection. We align with DESC (Dubai Electronic Security Center) and CREST certifications, which validate SOC performance and incident response against international benchmarks.

Our impact is tangible. We helped a key government agency cut response times to 15–20 minutes and shielded a leading financial institution from phishing and DDoS attacks during a ransomware spike. By integrating UAE security entities into our operations, we ensure faster threat intelligence sharing across sectors.

There's growing awareness about data privacy and compliance in the region. How are you helping clients stay ahead of regulations while protecting their assets?

At Paramount, privacy isn't just compliance — it's a foundation of trust. We were the first in the region to offer end-to-end privacy solutions integrating legal consulting, advanced technologies, and automation. Our experts hold more than 30 globally recognised credentials, including CISSP, CISM, ISO 42001, and ISO 27701.

We provide a single-window GRC model, giving top management real-time visibility of risks. Beyond corporates, we also run awareness sessions at schools and universities to equip young people with knowledge

Ashok Chandrasekharan

of online threats, responsible digital behaviour, and privacy best practices. Building this culture early is key to long-term resilience.

Share some incidents that stood out for Paramount.

We handle hundreds of thousands of alerts every year, most contained within hours. Our average response time is under 15–20 minutes for critical cases.

One case involved a retail chain with 150 branches across 10 countries. A credential leak exposed sensitive customer data, traded on the dark web. We traced the breach to internal systems, not consumer negligence, helping the client understand and fix the real vulnerability.

In another instance linked to a state actor, we traced malware back to its source and neutralised it with minimal disruption to national critical infrastructure. For a banking client, we cut detection and response times from months to just days, protecting sensitive financial data.

Looking ahead, what emerging cybersecurity trends should UAE businesses prepare for in the next three–five years?

AI will be both the biggest enabler and the biggest threat. Expect AI-driven phishing, vulnerability exploitation at scale, and sprawl attacks across interconnected cloud systems.

On the other hand, AI will also strengthen governance, with governments setting standards for privacy and ethics. Businesses must quickly adapt, embedding compliance into risk strategies. AI-enabled security platforms will drive real-time insights and automation, helping detect and eliminate threats with greater accuracy.