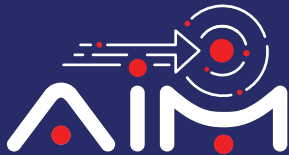


TECH TALK

Issue 170
August 2026

**Pioneering Tech
Leadership with a
Legacy of Excellence.**



Galaxy Office Automation Pvt. Ltd.



Galaxy & Lenovo recently hosted an exclusive technology session for our valued customers, showcasing how AI is transforming the modern workplace.

The session, themed "Scale Your AI Success with Smarter Partnership", explored AI-enabled devices, Windows 11 Pro for Business, intelligent computing, and secure digital transformation.

A big thank you to our customers, Lenovo experts, and partners for making the event a success. We look forward to continuing our journey of driving innovation and helping businesses unlock the power of AI.

Foreword

Dear Readers,

The World Cup is over, and it turned out the way I hoped it would when I wrote last month's column. Spain beat Argentina, and the winning goal came from a substitute, Ferran Torres, who was on the bench when the match started. Argentina had Messi. Spain had a system that worked whoever was on the pitch. That is the whole argument, settled on the field.

Enterprise AI is heading toward the same test. Last month I wrote about governance, cost discipline, and identity as the three things shaping how we deploy agents at Galaxy. The pattern we keep seeing is agents given access to systems well before anyone has decided who owns the controls around them. That is why we ensure the same discipline in every SOC and NOC engagement. Every agent gets an identity before it gets a task. Every agent gets a scoped, auditable permission set rather than a broad one that is easier to configure. And every agent we deploy sits inside a layer that is itself watched by other agents, trained to flag unusual behaviour and policy violations before they become incidents. It is the same zero trust principle we have applied to human users for years, extended to a workforce that does not sleep, does not take leave, and does not always ask before it acts.

Through our AI, Security, Data Centre, Network, and Cloud practices, we keep building toward the same outcome, autonomy that is governed and financially accountable from day one, not retrofitted once something has already gone wrong.

As for the World Cup, Spain's win made the point better than I could have. The team with the deepest bench and the clearest system beat the team with the biggest individual name. That is the bet worth making in the selection of your technology vendor too. Not on the ones with the flashiest demos, but on an organisation with the depth and the system to deliver on what you actually need. Do reach out to us for a conversation on how we can help you achieve your goals.

Happy reading!



Anoop Pai Dhungat
Chairman & Managing Director



A solar-powered aircraft, the Sceye HAPS, is shown in flight against a backdrop of a mountainous landscape. The aircraft has a long, slender fuselage and large, rectangular solar panels extending from its wings. The text "Future is now!" is overlaid in a large, bold, sans-serif font, with "Future" in red and "is now!" in white. A solid red vertical bar is positioned to the left of the text.

Future is now!

This flying solar-powered platform could deliver better internet from the air

Have you ever felt the frustration of losing internet access while camping, hiking or living in a remote area? Whether you're trying to connect with family, access important information or simply enjoy your favourite streaming service, losing internet access can be a real bummer. For many, this is a daily struggle. However, new technology from a company called Sceye could be the answer to these connectivity woes, offering a solution to the digital divide that leaves so many people in the dark.

Enter the Sceye HAPS: A blimp-like aircraft with a mission

The Sceye HAPS is not your average aircraft. This 213-foot-long uncrewed helium-filled behemoth is designed to soar to stratospheric heights, hovering between 60,000 and 65,000 feet above the Earth's surface. What makes it truly special is its ability to beam high-speed internet to areas that traditional infrastructure cannot reach.

Solar-powered stratospheric sentinel

One of the most impressive features of the Sceye HAPS is its power source. The aircraft is covered in a "solar cape" made of gallium selenide and gallium arsenide solar cells, allowing it to harness the sun's energy to stay aloft for months at a time. This sustainable power approach enables the HAPS to perform its critical tasks continuously, from providing internet access to monitoring environmental conditions.

Breaking records and bridging divides

The Sceye HAPS is already making waves in the real world. It set a long-range record by maintaining a data connection across a distance of over 87 miles, far exceeding the typical LTE range. This achievement has significant implications for bridging the digital divide, especially in areas like the Navajo Nation, where the HAPS is part of a project to provide universal

broadband access. By demonstrating its ability to connect over such vast distances, the Sceye HAPS is proving its potential to revolutionize internet access in remote and underserved communities.

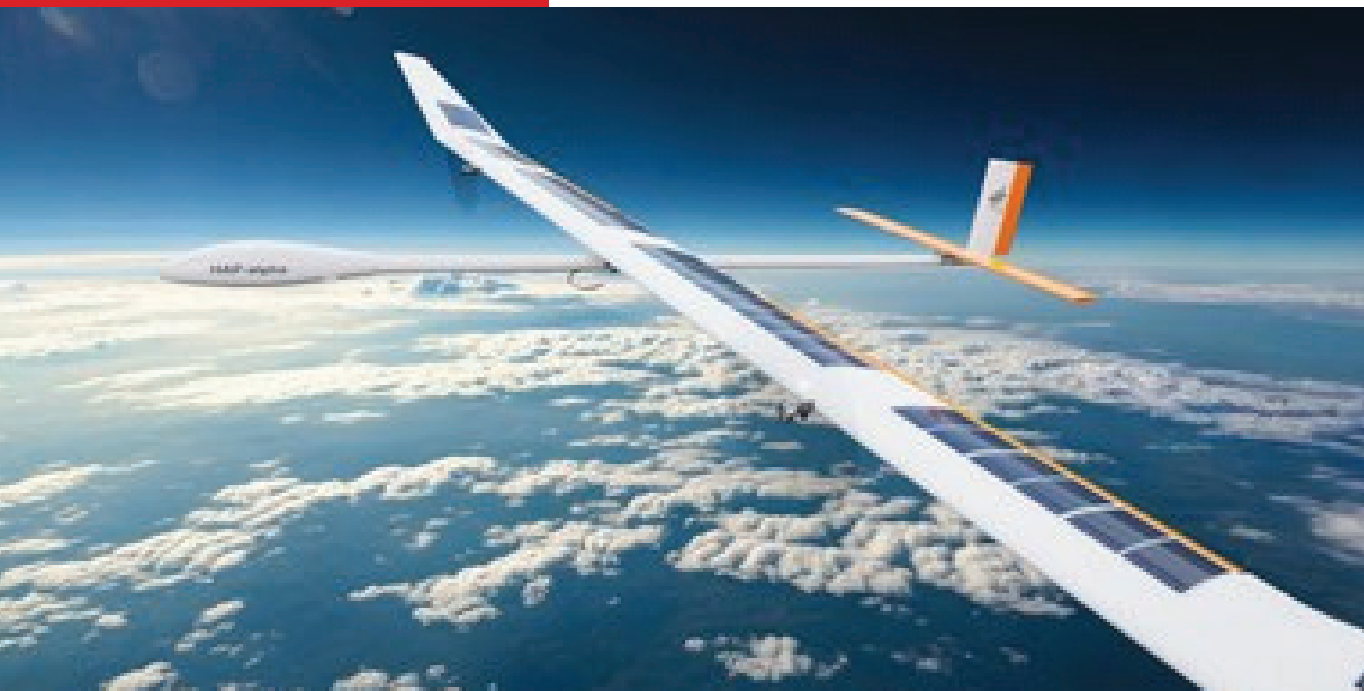
More than just internet

While providing internet access is a key function of the Sceye HAPS, its capabilities extend far beyond that. The aircraft is also being used for climate and environmental monitoring, disaster response, forest fire detection, and tracking and measuring methane emissions as part of an EPA study. The Sceye HAPS continues to impress with its technological advancements. In a recent flight, it demonstrated its ability to charge its batteries during the day and use that power to stay airborne overnight, a crucial step towards long-duration missions. With 20 test flights under its belt and commercial deployment planned for 2025, the future looks bright for this stratospheric innovation.

Kurt's key takeaways

The Sceye HAPS is shaking things up in the world of global connectivity. Think of it as a high-tech blimp that's on a mission to bring the internet to places that have been left in the digital dark ages. By floating way up in the stratosphere, this clever contraption is tackling problems that have stumped tech experts for years. This flying innovation could be a game-changer in making our world more connected and better prepared for whatever Mother Nature throws our way. Sure, there are still some kinks to work out. But the way things are going, it looks like the Sceye HAPS is proving that when it comes to solving big global problems, sometimes the best solution is to aim high, really high

Read more →



Cyber Resilience: Building Stronger Defences for a Safer Digital Future

Cyber resilience is an organization's ability to prevent, withstand and recover from cybersecurity incidents. Cyber resilience is a concept that brings business continuity, information systems security and organizational resilience together. It describes the ability to continue delivering intended outcomes despite experiencing challenging cyber events, such as cyberattacks, natural disasters or economic slumps. A measured level of information security proficiency and resilience affects how well an organization can continue business operations with little to no downtime.

Modern cyberthreats present new challenges, creating an environment where traditional security measures alone are insufficient. Organizations face sophisticated adversaries who use advanced technologies and techniques to cause disruptions. Threat actors and hackers increasingly exploit human vulnerabilities and system weaknesses rather than relying on traditional automated attack methods.

According to the 2025 Cost of a Data Breach Report from IBM and the Ponemon Institute, global breach costs decreased to USD 4.44 million on average. However, US organizations faced record-high costs at USD 10.22 million per incident. Despite these costs, 49% of breached organizations plan to increase security investments.

The importance of a cyber resilience strategy Enterprises must build effective cyber resilience through a risk-based strategy and coordinate initiatives to support it. A collaborative approach led by executives extends across the organizational ecosystem, reaching partners, supply chain participants and customers. It must proactively manage risks, threats, vulnerabilities and the effects on critical information and supporting assets, while also strengthening overall preparedness. Successful cyber resilience also involves governance, risk management, an understanding of data ownership and incident management. Assessing these characteristics also demands experience and judgment.

Furthermore, an organization must also balance cyber risks against attainable opportunities and competitive advantages. It must consider whether cost-effective prevention is viable and whether it can achieve rapid detection and correction with a strong short-term effect on cyber resilience.

To accomplish this goal, an enterprise must find the right balance between three types of controls: preventive, detective and corrective. These controls prevent, detect and correct incidents that threaten an organization's cyber resilience.

The benefits of cyber resilience

A cyber resilience strategy helps organizations achieve the following benefits:

- Mitigate financial loss
- Reduce operational damage
- Gain customer trust and business
- Increase competitive advantage
- Ensure business continuity

Mitigate financial loss

Financial loss from successful attacks might lead to a loss of confidence from company stakeholders, such as shareholders, investors, employees and customers.

The financial stakes are substantial. The IBM 2025 Cost of a Data Breach Report revealed

that organizations with extensive artificial intelligence (AI) use in security operations saved an average of USD 1.9 million in breach costs. These enterprises also reduced the breach lifecycle by 80 days compared to those organizations without these solutions. However, organizations experiencing AI-related incidents without proper access controls faced higher costs, highlighting the need for governed cyber resilience strategies.

Reduce reputational damage

Cyber incidents can severely impact an organization's reputation and customer confidence. A robust cyber resilience framework helps organizations respond quickly and transparently to incidents, minimizing long-term reputational harm and maintaining stakeholder trust.

Read more →

At Galaxy, we believe cyber resilience is more than just protecting against attacks—it's about ensuring business continuity, minimizing risk, and enabling organizations to recover quickly from evolving cyber threats. By combining proactive security, continuous monitoring, and resilient infrastructure, we help businesses stay secure, maintain customer trust, and confidently navigate today's digital landscape.

To talk to our experts, email us at marketing@goapl.com



Hardware Security Modules (HSMs): for Critical Infrastructure.

Hardware Security Modules (HSMs) are dedicated tamper-resistant devices designed to generate, store, and protect cryptographic keys while performing encryption, decryption, digital signing, and authentication operations. In sectors such as power, energy, banking, government,

and healthcare, HSMs provide a secure root of trust by ensuring that sensitive keys never leave the protected hardware. This enables organizations to safeguard critical applications, meet regulatory requirements, and defend against cyberattacks.

Key Features

AI Discovery & Visibility

- **Secure Key Management:** Generates, stores, rotates, and destroys cryptographic keys within certified tamper-resistant hardware.
- **Cryptographic Acceleration:** Performs high-speed encryption, decryption, digital signatures, and hashing without exposing private keys.
- **Tamper Resistance:** Detects physical tampering attempts and automatically erases sensitive keys to prevent compromise.
- **PKI & Certificate Management:** Supports certificate authorities, code signing, TLS/SSL certificates, and digital identities.
- **High Availability:** Supports clustering, backup, and failover for continuous cryptographic services.

Benefits

- Protects sensitive cryptographic keys from theft and misuse.
- Strengthens security for digital payments, PKI, databases, and applications.
- Ensures compliance with regulatory and industry standards.

- Improves application performance through hardware-based cryptographic acceleration.
- Minimizes business risk by providing secure key lifecycle management.
- Supports business continuity with HA and disaster recovery capabilities

Use Cases

- Public Key Infrastructure (PKI) and Certificate Authority protection.
- Database and file encryption key protection.
- Code signing for software integrity.
- TLS/SSL certificate key protection for web applications.

Why HSM over software-based key storage

HSMs provide significantly stronger protection than software-only key storage by ensuring private keys never leave tamper-resistant hardware. They offer certified security, faster cryptographic processing, centralized key lifecycle management, and regulatory compliance, making them the preferred solution for protecting mission-critical applications and sensitive data.

Galaxy Office Automation enables organizations to build a robust and secure cryptographic

infrastructure by delivering end-to-end Hardware Security Module (HSM) solutions. From solution design and deployment to integration and ongoing support, Galaxy helps customers protect their most sensitive digital assets and meet stringent security and compliance requirements. Protects encryption keys from theft or unauthorized access.

Best Practices

- Use dual control and role-based access for HSM administration.
- Perform regular key rotation and secure backups.

Integrate HSMs with IAM, PKI, databases, and cloud workloads.

- Monitor audit logs and validate compliance periodically

How Galaxy Enables Secure AI Adoption

Galaxy plays a critical role in helping organizations adopt AI securely. Services include AI readiness assessments, AI asset discovery, governance framework design, secure architecture, implementation of AI security controls, integration with existing security platforms, AI Red Teaming, continuous monitoring and managed services. Galaxy supports customers through a vendor-neutral approach, helping organizations deploy AI securely while aligning with business objectives and regulatory requirements.

Hardware Security Modules form the foundation of enterprise cryptographic security by protecting encryption keys, ensuring trusted cryptographic operations, and helping organizations achieve regulatory compliance. As cyber threats continue to evolve, deploying HSMs provides a resilient and scalable approach to securing critical infrastructure, digital identities, payment systems, and sensitive business applications.

To connect with our experts, write to us at marketing@goapl.com



Meta launches new app 'Seller' to provide sales tools for merchants.

Meta on Friday launched a new app called "Seller" to offer dedicated selling tools to merchants using the company's Facebook Marketplace platform for buying and selling items.

Increasing shopping activity on Facebook groups prompted the social media giant to launch Marketplace ten years ago, generating revenue from boosted listings.

Meta is looking to strengthen its Marketplace offering to better compete with e-commerce platforms like eBay, while enhancing the shopping experience on the platform, which sees 430 million items listed each month globally.

The "Seller" app is designed to sync with existing Marketplace accounts, carrying over current listings, messages and sales history. The app features AI-powered tools for c...

The company said "Seller" is now available on the App Store for U.S. users 18 and older, with a web version currently being tested for those who download the app.

[Read more →](#)



India data centre capacity to jump to 12 GW by 2030 as AI fuels demand: Wood Mackenzie.

India's operational data centre capacity is projected to increase more than five-fold to 12 GW by 2030 from 2.2 GW in 2025, driven by rapid adoption of artificial intelligence, hyperscale cloud investments and the country's expanding digital economy, according to a Wood Mackenzie report released on Monday.

AI-dedicated capacity is expected to rise multifold to 6,546 MW by 2030 from 275 MW in 2025...

The report said India's digital economy, valued at Rs 32 lakh crore in 2025 and accounting for about 12 per cent of GDP, together with more than 1.03 billion active internet users and around 22 billion monthly UPI transactions, is driving demand for data centre infrastructure. India's domestic AI market is projected to reach Rs 11.7 lakh crore by 2032.

Wood Mackenzie said Maharashtra and Tamil Nadu currently account for about 65 per cent of installed IT load,

but future investment is expected to expand into Andhra Pradesh, Telangana, Uttar Pradesh and Karnataka. These emerging markets are attracting significant commitments from global hyperscalers, including Amazon Web Services and Google, alongside domestic operators such as Adani Connex, which has announced a development pipeline of 2.6 GW.

The report said access to reliable, cost-competitive electricity has overtaken land and capital as the industry's primary constraint, with captive power generation and long-term renewable power purchase agreements emerging as preferred strategies.

[Read more →](#)





📍 Galaxy Office Automation Pvt. Ltd. B-602,
Lotus Corporate Park, Graham Firth
Compound, Off. Western Express Highway,
Goregaon (E), Mumbai - 400 063.

☎ +91 22 46108999

@ marketing@goapl.com

🖱 www.goapl.com