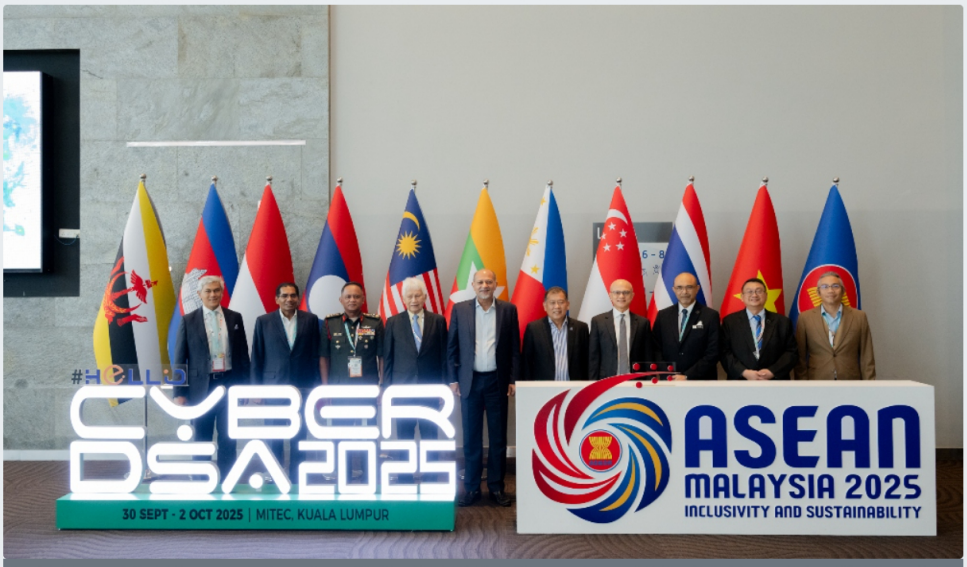
CyberDSA returns, converging cyber resilience, AI, and security across ASEAN

By Digital News Asia October 3, 2025

- ***Trust frameworks transform cybersecurity into a driver of economic progress***
- ***Borderless threats demand ASEAN-wide cooperation and shared cyber capabilities***



From left: Nadzeem Bin Abdul Rahman, executive director, Aerosea Exhibitions Sdn Bhd; Dr M. Gandhi, director of Aerosea Exhibitions Sdn Bhd; lt. general Azhan Hj Md Othman, chief of Staff; Asmat Kamaludin, chairman of Aerosea Exhibitions Sdn Bhd; Gobind Singh Deo, minister of Digital Malaysia; Wilson Ugak Kumbong, deputy minister of Digital; Al-Ishsal Ishak, chairman of the Board, CyberSecurity Malaysia; Shakib bin Ahmad Shakir, deputy secretary general (Management & Strategic), Ministry of Digital; Dr Haji Amirudin Abdul Wahab, CEO, Cybersecurity Malaysia; Fahri Azzat, director, Aerosea Exhibitions Sdn Bhd

"When the CrowdStrike outage left millions staring at blue screens, we didn't know whether it was a cyberattack or a system failure. There was no clarity," said Digital minister Gobind Singh Deo ***(pic below)***, addressing a hall packed with policymakers, security forces, industry leaders, and cybersecurity professionals as he opened CyberDSA 2025 at MITEC Kuala Lumpur.

"It could happen again, he warned. "The question is, are we ready if the next incident strikes at something as critical as national security?"

That question set the tone for the three-day event, held from September 30 to October 2 under the theme "Pioneering the Future: Building a Resilient and Trusted Digital Nation." But beyond the keynotes and ceremonial MoU signings, a harder truth emerged: Malaysia and the wider ASEAN region are racing against threats that are evolving faster than defences can keep up.

The shift from walls to resilience

CyberDSA 2025 confronts Asia's rapidly escalating cybersecurity landscape, translating Malaysia's national priorities into regional and global action. The event was jointly hosted by CyberSecurity Malaysia and the Armed Forces' Defence Cyber and Electromagnetic Division, reflecting Malaysia's dual commitment to building both digital trust and cyber defense.

The agenda examined the intersection of national security, corporate responsibility, and digital transformation, asking not only whether systems are secure but also whether societies, economies, and governments are resilient enough to withstand inevitable disruptions.

Cybersecurity as a national imperative

In his keynote, Gobind underscored that cybersecurity must be treated as a national imperative. Daily life, he said, is now inseparable from digital systems, and Malaysia's National Critical Information Infrastructure (NCII), from energy grids to financial markets to government services, faces the same vulnerabilities seen worldwide.

A successful cyberattack, he cautioned, could paralyse institutions and derail daily life for millions of citizens. "If we are to live in a world where we depend almost entirely on the digital gadgets of today and tomorrow, we must make sure the ecosystem gives us the tools we need for it to work," he stressed.

Gobind pointed to the swift creation of the Ministry of Digital and its immediate focus on governance as proof of urgency. "The first thing that we did was to table the Cybersecurity Act, within three months," he noted. The legislative framework, he explained, is critical to define and enforce baseline protections for the NCII, the backbone of national stability.

From static defence to active resilience

Al-Ishsal bin Ishak, chairman of the Board of CyberSecurity Malaysia (CSM), described how the agency is steering Malaysia away from traditional "castle wall" defences toward a strategy of resilience.

"Over the decades, cybersecurity's posture has been primarily defensive, to create walls and barriers that keep threats away," he said. "But with today's realities and advancements in technology, protection alone is insufficient. Resilience goes beyond defence. It is about adapting, recovering, and maintaining confidence in our systems, institutions, and society, even under attack."

This shift, he explained, is what CSM now defines as Digital Trust for the Rakyat—a trust that empowers every Malaysian to participate confidently in the digital economy.

Turning vision into reality, Ishal offered concrete examples of how CSM is operationalising this trust. Talent, he said, is the first pillar. "We have already trained 18,764 knowledge workers in domains from digital forensics to cryptography. But by 2026, Malaysia will need at least 28,000 skilled professionals. Bridging this gap is our immediate priority."

MOST READ IN TOPIC

Gamuda, the engineering and innovation leader with ambitions to elevate Malaysian software talent to the global stage
Digital Economy | Oct 8, 2025

Inside Malaysia's 6-way MOCN: How Maxis is implementing the world's first such network sharing agreement
Digital Economy | Mar 6, 2025

Malaysia Digital status companies delivering synergy and growth through AI
Digital Economy | Oct 11, 2024

IDECS 2024 concludes with initiatives to drive Sarawak's sustainable digital future
Digital Economy | Oct 18, 2024

Madani Government announces US$338 million to accelerate MSME digitalisation nationwide
Digital Economy | Mar 25, 2025

LATEST NEWS

Sabah SMEs accelerate digital adoption with CelcomDigi's MY5G Programme
Business | Oct 10, 2025

U Mobile launches U-Home 5G Borneo, making high-speed broadband more accessible in East Malaysia at just US$14 monthly
Business | Oct 10, 2025

Waste To Energy: Selangor's sustainable solution to its waste crisis
Sustainability Matters | Oct 9, 2025

Made by Malaysia: AI-powered IC design in the spotlight
Digital Economy | Oct 9, 2025

Selangor's premier Twin Accelerator 2025 crowns Deep-X & Retail-X winners at SDEC 2025
Digital Economy | Oct 9, 2025

MYCentre4IR and World Economic Forum position Asean as global voice in the intelligent age
Digital Economy | Oct 9, 2025

PACE Bootcamp 2025 embarks on nationwide hunt for innovative founders
Startups | Oct 8, 2025

DIGERATI50 2020-2021

Second is capability. Ishal highlighted CSM's recent launch of Malaysia's first Vehicle Forensics Laboratory, a facility capable of retrieving crash data, preserving dashcam evidence, and assessing the cybersecurity of increasingly software-heavy vehicles. "This is how we support law enforcement, protect society, and uphold privacy in an era where even cars are computers on wheels."

Finally, Ishal laid out CSM's threefold regional commitment. "We will continue to expand Malaysia's cyber talent pipeline, strengthen cross-border information sharing for faster and more coordinated response, and push the frontiers of research in emerging areas such as AI security and post-quantum cryptography."

The wake-up call

Telekom Malaysia's chief information security officer, Raja Azrina Raja Othman, delivered the ground truth of how threats are evolving in the field.

"The past year revealed that advanced persistent threat (APT) actors are refining their targets, becoming more geopolitically driven and highly sophisticated, with far-reaching impact," she said. "These campaigns of global espionage are infiltrating telcos, transport providers, and even military networks across more than 80 countries, putting national sovereignty itself on the line."

She cited the BPFdoor attack on South Korea's SK Telecom earlier this year, where hackers breached core systems to steal unencrypted USIM authentication keys, the cryptographic lifeblood of mobile networks. "The incident compromised data from over 23 million customers," she said, leaving them vulnerable to SIM-swapping fraud, device cloning, and a profound loss of trust in telecom operators.

"These attacks are serious, persistent, and a stark reminder that even the most advanced digital economies are not spared," Azrina said. "Cyber threats in Asia are escalating in complexity, making detection and attribution more difficult."

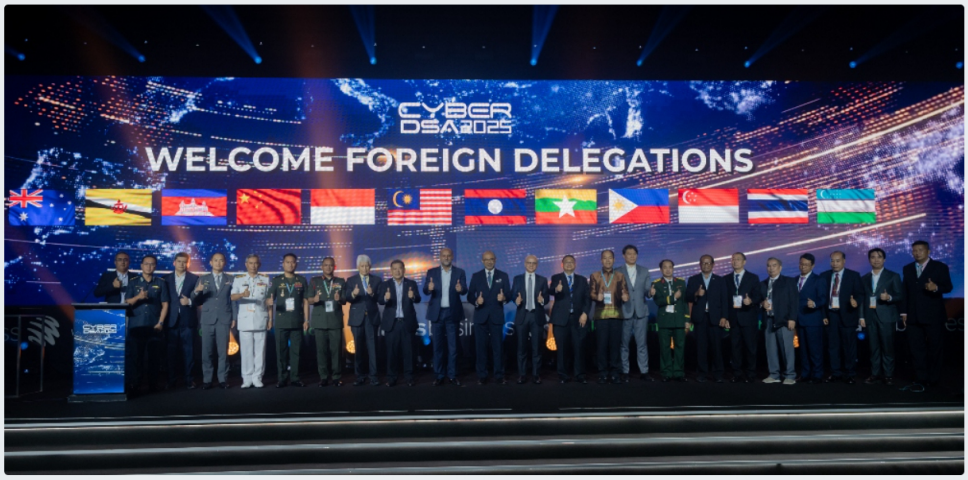
She also cited UNC3886, a state-linked espionage group recently escalating campaigns in Southeast Asia. In July, Singapore's Cyber Security Agency (CSA) confirmed the group had infiltrated critical infrastructure, from healthcare to energy. The risks extended well beyond data theft, encompassing long-term infiltration and the mapping of entire national networks.

Gobind later echoed these warnings, noting that the rise of AI, generative AI, and agentic AI represented both opportunity and threat. "It is only by understanding the technology at every layer that we can secure it," he said. "When we ask the hard questions and secure every single layer, only then can we ensure that technology is ready, sustainable, and future-proof."

From conversations to commitments

The opening ceremony of CyberDSA 2025 saw a series of memorandums of understanding (MoUs) signed to expand the reach of Malaysia's MyDigital ID platform. Partners included KTMB, CTOS Digital Berhad, HONOR, U Mobile, and XOX Mobile, covering applications from transport and financial services to SIM registration and device integration.

The agreements cemented MyDigital ID as a cornerstone of Malaysia's digital trust framework. Asmat Kamaludin, chairman of Aerosea Exhibitions Sdn. Bhd. said, "This blend of ideas and execution reflects the very spirit of the event. CyberDSA has been about creating a platform where governments, industries, defence authorities, and innovators could come together to chart the future of cybersecurity and digital resilience."



Building regional resilience together

The path forward lies in shared responsibility. "Government plays an important role in listening to the concerns of the industry and finding ways to build an ecosystem that delivers safety and trust. But we can't do this alone," Gobind said, calling for industry experts and academia to anticipate threats and strengthen national capabilities.

Yet, he warned, resilience cannot stop at national borders. "Even if we build a strong, secure, resilient ecosystem, threats will still come from outside our nation. This is why regional conversations are so important."

Al-Ishsal echoed this point, stressing that CyberSecurity Malaysia works closely with ASEAN counterparts in Singapore, Indonesia, Brunei, Thailand, Cambodia, Laos, and the Philippines. Malaysia also maintains an active presence in global forums such as FIRST, OIC-CERT, and APCERT. "CyberDSA," he emphasised, "is more than dialogue. It is a catalyst for collaboration and shared resilience."

Raja Azrina called for a mindset shift across ASEAN. "Security is no longer a shield or a cost centre," she said. "It enables the growth of the digital economy. When SMEs, which make up 97% of ASEAN businesses build resilience into their services, they can expand across borders with confidence."

As IT and operational technology converge, she urged resilience to be treated as a top-down national priority. "Digital trust is what allows innovation to scale, partnerships to flourish, and citizens to engage confidently in the digital economy," she said, adding that security and privacy by design, alongside regional collaboration, are vital to making resilience the standard.

Related Articles

Axiata and Cambodian Government forge cybersecurity alliance to empower digital future

Axiata has signed an MoU with

Asean affirms importance of closer coordination of cybersecurity efforts in region

Asian cybersecurity confidence levels take a dip

There has been a marked decline in

Axiata has signed an MOU with Cambodia's Ministry of Post and Telecommunications to strengthen cybersecurity and develop digital talent.

Business
Aug 13, 2025

Need to develop basic voluntary norms to guide responsible use of information and communications technologies.

Digital Economy
Sep 19, 2017

security teams' confidence in assessing cybersecurity risks across key IT infrastructure components compared to last year.

Insights
Apr 10, 2017

For more technology news and the latest updates, follow us on Facebook, Twitter or LinkedIn

Keyword(s) :

CyberDSA 2025 Gobind Singh Deo Raja Azrina Raja Othman Al-Ishsal Ishak Tan Sri Asmat Kamaludin Digital Trust Advanced Persistent Threats MyDigital ID

Author Name :

Digital News Asia