iSMG Studio

at GovWare 2025

GovWare Conference and Exhibition 2025:

Conquer the Unknown

GovWare Conference and Exhibition 2025, Singapore's premier cybersecurity trade event held as part of Singapore International Cyber Week, powered by the Cyber Security Agency of Singapore, brought together insights from cybersecurity researchers, law enforcement officials and policymakers from 80 countries.

Under the theme "Cyberspace: Of Starbursts, Black Holes and Last Frontiers," the conference highlighted the need for innovation, knowledge and digital trust that could transform Southeast Asia's cybersecurity landscape.

As the event's media partner, Information Security Media Group staffed a video studio at the conference, capturing insights from distinguished thought leaders and speakers including CEOs, CISOs, technologists, government leaders, threat researchers and legal experts. Experts discussed innovative approaches to govern, secure and sustain systems that are already thinking, adapting and sometimes acting beyond our immediate control.

Coverage of the GovWare conference is featured across ISMG media sites in Asia. You will also see insightful panel discussions featuring members of our CyberEdBoard community.

In these pages, you can find the thought-provoking discussions led by our seasoned editorial team, offering valuable takeaways for building trust and security in the digital era - and conquering the unknown.

Best,

Geetha Nandikotkur

Vice President, Conferences for Asia, the Middle East and Africa

Information Security Media Group

Visit us online for more ISMG at GovWare 2025 coverage:

ISMG.STUDIO

Video Interviews

“Some of the groups started to make coalitions because they understand that it's hard to work alone right now.”

Anastasia Tikhonova
Global Threat Research Lead, Group-IB

Ransomware Groups Evade Detection in Plain Sight

Group-IB's **Tikhonova** on Threat Actor Mimicry and Profit-Boosting Coalitions

Ransomware groups known for their unabashed and disruptive campaigns are using stealthier, more collaborative tactics to gain access to systems, said Anastasia Tikhonova, global threat research lead at Group-IB.

WATCH ONLINE

OT Security Is Gaining Strategic Focus Across Industries

Schneider Electric's **Andre Shori** on the Shift From Reactive to Holistic OT Defense

As OT environments face mounting cyberthreats, CISOs are transitioning from reactive defenses to comprehensive, risk-based strategies that integrate safety, visibility and resilience across IT and OT environments, says Andre Shori, APAC cybersecurity vice president and CISO at Schneider Electric.

WATCH ONLINE

Quantum Threats Demand Post-Quantum Cryptography Now

Benjamin Ang of RSIS Urges Organizations to Adopt Quantum-Safe Standards

Organizations must adopt post-quantum cryptography, and security teams need automation to handle real-time adaptive security without burning out, said Benjamin Ang, head of the center of excellence for national security, future issues in technology, digital impact at RSIS.

WATCH ONLINE

Singapore Military Chief Calls for Greater Cyber Resilience

Col. Clarence Cai Discusses Cyber Strategy, AI Defense and Partnerships

Singapore continues to take steps toward cyber preparedness by investing in the cyber-dedicated sector of its armed forces, the Digital and Intelligence Service, led by Col. Clarence Cai. Under his leadership, Singapore is injecting military-grade cyber tactics into the nation's cyber infrastructure.

WATCH ONLINE

Adam Meyers
Senior VP, Counter Adversary Operations, CrowdStrike

Ransomware, E-Crime 'Exploding' Across Asia-Pacific

Adam Meyers of CrowdStrike Says Group Stopped 320 Attacks Last Year

Ransomware and cybercrime schemes are exploding across the APAC region as threat actors use generative AI to develop malware fast, creating a dangerous asymmetry in the cybersecurity arms race, said Adam Meyers, senior vice president of counter adversary operations at CrowdStrike.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Meyers also discussed:

- China's global approach to cyber espionage compared to the regional focus of Iran and Russia;
- CrowdStrike's Threat AI solution using agentic AI for malware analysis and threat hunting;
- The need for public-private collaboration to disrupt cybercrime groups.

WATCH ONLINE

> "We've seen generative AI has played a role in this region. Particularly there's something called FunkLocker, which is a ransomware tool that was purportedly developed completely using gen AI."
>
> ***-Adam Meyers***

Government Modernization Creates New Cyber Challenges

SentinelOne's **Howell** on How AI Closes the Public-Private Security Gap

In today's heightened geopolitical climate, governments are racing to modernize their digital infrastructures. Through artificial intelligence-driven solutions and defense strategies, SentinelOne and other organizations are helping them secure against a growing attack surface.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Howell also discussed:

- Why real-time info sharing between public-private sectors is critical;
- SentinelOne's unified platform approach and recent acquisitions in generative AI;
- The emerging role of agentic AI through 2026.

WATCH ONLINE

> "As governments modernize, they change their attack surface and our job is to help them understand how their attack surface changes, anticipate attacks and protect from those attacks."
>
> ***-Andrew Howell***

How Defenders Can Keep Pace With AI-Supercharged Attacks

Reversec's **Daisy Radford** on Understanding Attacker Behavior to Secure Systems

Threat actors are harnessing artificial intelligence tools to supercharge their tactics, and that's putting cyber defenders on their back foot. It's time to rethink security tooling, strategies and the overall understanding of attackers, said Daisy Radford, regional managing director at Reversec.

WATCH ONLINE

Agentic AI Is Coming - Is Your SOC Ready?

Fortinet's **Derek Manky** on Rising Agentic AI Attacks and Autonomous Defenses

AI-enabled attackers are moving faster than ever, and so must cyber defenders. Derek Manky, chief security strategist at Fortinet, explains how modern SOCs are using AI to cut response times, expose vulnerabilities and defend against autonomous agents emerging on the darkweb.

WATCH ONLINE

Small Modular Reactors Bring 'Wild' New Cyber Risks

STUK's **Esa Joffel** on How Remote Operations, AI Create Oversight Challenges

Small modular reactors introduce technologies unprecedented in nuclear facilities, including remote operations, digital twins and AI-driven systems - requiring nuclear security teams to rethink traditional approaches, said Esa Joffel, inspector, cybersecurity, nuclear security - IT and OT, STUK.

WATCH ONLINE

AI and Cybersecurity: Beyond the Final Frontier

Industry Leaders **Monteiro** and **Lim** Call for Collective Resilience in Cyber Defense

AI dominance is transforming cybersecurity leadership and redefining resilience strategies as organizations confront evolving quantum and AI-powered threats, according to Cheri Lim, GovWare 2025 programme advisory board member, and Ian Monteiro, CEO, Image Engine.

WATCH ONLINE

“Everybody has a role to play. Those days of siloed approaches are gone. It's very much a holistic approach now.”

Andre Shori
APAC Cybersecurity VP & CISO, Schneider Electric

Zero Exposure: Simplifying OT Security With a New Mindset

Varriale of BSL Technologies Calls for Isolation-Based Architectures to Secure OT

Traditional IT defenses fail in operational technology environments. Antonio Varriale, CTO of BSL Technologies, explains why "zero exposure," not just zero trust, is essential for safeguarding industrial networks.

> "What you cannot reach, you cannot breach."
>
> ***-Antonio Varriale***

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Varriale also discussed:

- How zero exposure isolates systems, reducing the attack surface;
- How simplifying security layers improves resilience and reduces operational risk;
- Why human error is such a key weakness.

WATCH ONLINE

CISOs Must Secure Executive Buy-In to Prevent Burnout

Chuan Wei Hoo of StarHub Says Board Support Enables Realistic Security Road Maps

Security leaders need executive and board-level support to implement effective cybersecurity strategies and avoid burnout. Without this backing, business units resist security initiatives, making the CISO's role unsustainable, said Chuan Wei Hoo, CISO at StarHub.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Hoo also discussed:

- Why CISOs should prioritize people, process and technology in that specific order;
- The need to establish measurable technical guardrails for AI adoption;
- How quantum readiness should focus on network protocols including VPN, SSH and TLS.

WATCH ONLINE

> "If you're the CISO of a company, consider that the executive management and board will hold you accountable for anything that is cyber-related ... That's where you can either do it in your favor to turn ....This is the strategy. I need executive support. I need the financial support to get things moving."
>
> ***-Chuan Wei Hoo***

“In many cases, the humans just get fooled. It's difficult to be resilient in the face of an AI deepfake, then what kind of processes you can put in place in case people get fooled.”

Benjamin Ang
Head, Centre of Excellence for National Security, Future Issues in Technology, S. Rajaratnam School of International Studies

Why Cyber Hygiene Should Be a Top Priority for SMBs

MyRepublic's **Imran Nazi** on Reward-Based Models to Boost Cyber Hygiene Among SMBs

Small and medium-sized businesses often see cybersecurity as optional, focusing instead on daily survival. Imran Nazi, head of enterprise ICT at MyRepublic, says awareness and financial rewards could shift this mindset, helping SMBs view cybersecurity as essential to business continuity.

WATCH ONLINE

Preparing for Q-Day: Quantum Security Readiness

BlackBerry's **Jackson** Says Quantum Preparedness Is 20% Technology and 80% Planning

Quantum computing is no longer a distant threat. Jonathan Jackson, senior director of strategic technical solutions at BlackBerry, urges enterprises to shift focus from technology to readiness, reminding security leaders that quantum preparedness is "20% technology and 80% planning."

WATCH ONLINE

Speed vs. Security: The AI Arms Race

Mandiant's **Luke McNamara** on Threat Intelligence and AI-Driven Defense

Threat actors are experimenting with artificial intelligence to increase speed and efficiency, and defenders must use the same technology to detect intrusions faster and reduce alert fatigue, said Luke McNamara, deputy chief analyst for the Google Threat Intelligence Group at Mandiant.

WATCH ONLINE

AI Enables Faster, Smarter Threat Response

Sysdig's **Marc Brown** on How AI Transforms Threat Intelligence for Cloud Security

AI is helping cybersecurity teams counter rapid, cloud-based threats that unfold in minutes. Marc Brown, senior director for solutions engineering at Sysdig, says automation and intelligent analysis enable teams to respond faster and strengthen decision-making amid growing cloud complexity.

WATCH ONLINE

NIST Framework Drives Global DNS Security Standards

Infoblox's **Craig Sanderson** on Integrating DNS Protection Into Compliance Frameworks

NIST's updated DNS security guidance is pushing organizations to treat DNS as a measurable cybersecurity control. Craig Sanderson, principal cyber security strategist at Infoblox, says companies must align DNS with broader risk frameworks to strengthen cyber resiliency and business continuity.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Sanderson also discussed:

- Scaling challenges of protective DNS deployment and shared operational models;
- How DNS telemetry supports risk-based cyberthreat exposure management;
- The role of artificial intelligence in automating DNS hygiene and asset visibility.

WATCH ONLINE

> "There's also a requirement for organizations to start to think about how they incorporate DNS into that broader compliance frameworks. There are things that require a focus around building a road map from a risk mitigation point of view in those broader frameworks."
>
> ***-Craig Sanderson***

Craig Jones
Independent Strategic Advisor, Group-IB, and Former Director, Cybercrime, Interpol

Separating the Noise From Actionable Threat Intelligence

Former Interpol Cybercrime Director on Public-Private Gap

Closing the divide between public policy and private data remains one of the most pressing challenges in the fight again global cybercrime, said Craig Jones, independent strategic advisor at Group-IB. Jones says the public and private sectors need to share information.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Jones also discussed:

- How organizations can use AI to filter out noise and focus on actionable threat intelligence;
- The growing strain of compliance amid borderless cybercrime;
- Why AI-driven deception is eroding trust and reshaping digital security.

> "There's so much data and information. How do we turn that into an action? It's important that we understand the rules and processes for being able to share data. Once you have that correct and that trust is built, then you can start sharing."
>
> ***-Craig Jones***

WATCH ONLINE

Agentic AI Poses Next Wave of Security Challenges for CISOs

Darktrace's **Mike Beck** on Why Non-Human Identities Require New Defenses

While generative AI has weaponized phishing attacks over the past year, the emerging threat involves autonomous AI agents making business decisions and managing non-human identities with broad data access across organizations, said Mike Beck, global CISO at Darktrace.

WATCH ONLINE

Map Assets, Dependencies to Build Supply Chain Resilience

Miriam Howe of BAE Systems Says Visibility Is the Foundation for Risk Management

Threat actors target supply chains and trusted partners, forcing security leaders to extend protection beyond organizational boundaries, map infrastructure and understand critical dependencies, said Miriam Howe, head of international consulting at BAE Systems Digital Intelligence.

WATCH ONLINE

AI Models Need Human Oversight to Ensure Cyber Trust

Lenovo's **Nima Baiati** on the Need for Human Control in AI-Driven Enterprise Security

As artificial intelligence becomes central to enterprise defense, Nima Baiati, executive director and general manager of cybersecurity solutions at Lenovo, says that without human oversight, AI systems could reinforce vulnerabilities and erode digital trust.

WATCH ONLINE

Managing Cloud Security in Asia's Digital Transformation Boom

ViewQwest's **Peter Molloy** on Building Cyber Resilience and Agility

The move to cloud throughout the APAC region has been gradual, slowed by concerns over data sovereignty and a lack of local instances by major cloud providers. But now with those barriers largely gone, cloud adoption is accelerating, and new hybrid and multi-cloud models call for new security and network strategies, said Peter Molloy, chief growth officer, ViewQwest.

WATCH ONLINE

“Shadow AI, rogue agents and integration failures are all converging. The only way to stay ahead is to shift left - faster than the adversaries.”

Derek Manky
Chief Security Strategist & Global VP - Threat Intelligence, Fortinet

Strong Cyber Hygiene Is Healthcare's Best Defense

Arctic Security CEO **David Chartier** on Proactive Risk Management in Healthcare

Healthcare organizations should shift from reactive responses to proactive defense rooted in automation, monitoring and strong cyber hygiene practices, says Arctic Security CEO David Chartier.

> "Sometimes you get the basics right, and you're going to be way ahead."
>
> ***-David Chartier***

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Chartier also discussed:

- How automation enhances early detection and risk mitigation;
- Building resilient supplier relationships through shared visibility;
- The productivity benefits of AI for overburdened security teams.

WATCH ONLINE

The Great Cyber Divide: Smaller Enterprises Start at Disadvantage

StrongKeep's **Keerthi** on Meeting Compliance Despite Cyber Inequity

Gaurav Keerthi, CEO and founder of security start-up StrongKeep, said the threat landscape has created what the World Economic Forum calls "cyber inequity," in which large enterprises remain well protected, while smaller ones lag behind in cyber readiness.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Keerthi also discussed:

- Why governance and procurement controls can mitigate third-party risk;
- How resilience frameworks are expanding beyond tech;
- The importance of enterprise collaboration to strengthen cyber landscape.

> "Cybersecurity is unequally distributed. Big enterprises have a lot of it. Small enterprises have none of it, and they become the targets because the attackers are trying to get after your company through them."
>
> ***-Gaurav Keerthi***

WATCH ONLINE

“In SMRs, there is a lot of new IT-type features coming into the nuclear process... There's upcoming autonomous systems like digital twins, digital shadow. But AI and machine learning is one topic approaching the nuclear facilities.”

Esa Joffel
Inspector, Cybersecurity, Nuclear Security - IT & OT, STUK, the Radiation and Nuclear Safety Authority

AI, OT and the Rise of Shared Cyber Accountability

Fortinet's **Rashish Pandey** on Security Leadership, Regulation and IT-OT Convergence

Artificial intelligence is no longer just a business enabler. It's a cybersecurity challenge. Rashish Pandey, vice president of marketing at Fortinet, said organizations face rising threats fueled by AI, growing attack surfaces and regulatory uncertainty across geographies.

WATCH ONLINE

Building Trust and Security in the Age of AI

Google's **Royal Hansen** on Securing AI Systems, Preparing for Quantum Threats

Royal Hansen, vice president of engineering at Google, outlines how AI can strengthen cybersecurity when built securely, why agent accountability and crypto agility matter, and how trust remains central to technology adoption.

WATCH ONLINE

AI, Quantum Computing Are Raising Stakes in Cyberwarfare

Athenian Tech's **Relia** on the Growing Threat of Attack on OT Systems

Hackers are using AI to automate attacks and evade detection. To add to the risks, future advancements in quantum computing capable of breaking current encryption standards within minutes will add to the threats posed by hackers., said Sanjeev Relia, retired Army officer and chief strategy officer at Athenian Tech.

WATCH ONLINE

Building Security Into Business Innovation

Advanced Intelligence Group's **Singh** on AI, Resilient Digital Transformation

CISOs can manage API and third-party risks without stifling innovation by integrating governance and controls early in the process, said Shishir Kumar Singh, group head of information security at Advanced Intelligence Group.

WATCH ONLINE

Countering Cybercrime Networks With Human-Centric Strategies

CYBR's **Jasmin Ilic** on Disrupting Cybercrime's Supply and Demand Through Awareness

Transnational cybercrime networks continue to evolve, exploiting technology and human vulnerabilities. Jasmin Ilic, CEO and co-founder of CYBR, outlines how leaders can disrupt these systems by addressing both human and technical elements.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Ilic also discussed:

- Why disrupting supply chains and labor sources is as critical as technical defenses;
- Why threat modeling and organizational awareness are central to proactive security strategies;
- Building organizational capability through education and leadership.

> "We have to tackle both supply and demand if we want to progress."
>
> *-Jasmin Ilic*

WATCH ONLINE

AI in the Physical World Creates New Security Risks

CSA's **Stanley Tsang** on Building a Secure and Responsible AI Ecosystem

AI is evolving from productivity tools to autonomous vehicles and robotics, significantly expanding the attack surface and bringing cybersecurity and physical safety concerns together, said Stanley Tsang, distinguished engineer and senior director, Cyber Security Agency of Singapore.

WATCH ONLINE

Industry 5.0 Demands Human-Centric OT Security

OT-ISAC's **Steven Sim** on Evolving OT Resilience Through Collaboration and Governance

Industry 5.0 is transforming OT with collaborative robots and AI-driven systems. Steven Sim Kok Leong, chair of the advisory committee at OT-ISAC, shares why human-centric cybersecurity is critical for safety, resilience and innovation as machines and people work closer than ever.

WATCH ONLINE

Secure AI Tools: From Visibility to Post-Quantum Readiness

Thales' **Todd Moore** on Managing Data Risk, Securing Agentic AI and Emerging Tech

Adoption of artificial intelligence tools is accelerating innovation, but it's also increasing data risk at unprecedented levels. Todd Moore, global vice president of data security at Thales, said over 90% of newly generated data is unstructured, much of it created by artificial intelligence systems - creating major challenges for visibility, classification and control across hybrid environments.

WATCH ONLINE

Engineering Mindset Builds Stronger OT Cyber Resilience

Conny Tech's **Sim Siang Tze** on Designing Systems With Cyber-Informed Engineering

An engineering mindset creates more secure, resilient OT systems by embedding security at the design stage and aligning digital defenses with real-world physics, said Victor Sim Siang Tze, OT cybersecurity consultant, Conny Tech.

WATCH ONLINE

“It's no longer a matter of if you're attacked, it's a matter of when. Look at cyber resilience as a key strategy, meaning your ability to detect early, mitigate and recover fast.”

Cheri Lim
Member of the GovWare 2025 Programme Advisory Board

AI, Human Risk and the New Era of Agentic Workspaces

Proofpoint's **Cheng** on Cybersecurity, Collaboration and Evolving Human-AI Dynamic

Artificial intelligence tools are helping threat actors create more targeted business email compromise - and a growing number of attacck are aimed at Asian countries, said Jennifer Cheng, director of cybersecurity strategy at Proofpoint.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Cheng also discussed:

- Collaboration on cyberthreat intelligence and disruption efforts;
- Human factors driving APAC's data security priorities;
- AI's influence on phishing and social engineering.

> "Regardless of AI adoption, humans are still going to be a target."
>
> *-Jennifer Cheng*

WATCH ONLINE

"We can look into different sort of incentives. If an SMB has good cyber hygiene, has never had any formal intrusion for the past few years, these can be factored in the discounts when they are looking for insurance premiums on cybersecurity."

Imran Nazi
Head, Enterprise ICT, MyRepublic

Building Cyber Resilience in the OT Era

Global Resilience Federation's **John Lee** on Future-Proofing Critical Infrastructure

OT security has evolved from a compliance checkbox to a business imperative. John Lee, managing director for the Asia-Pacific region at the Global Resilience Federation, explains why resilience, governance and human accountability form the foundations of OT security in an interconnected world.

> "OT cybersecurity is part of the business risk."
>
> ***-John Lee***

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Lee also discussed:

- Balancing innovation and security in Industry 5.0 environments;
- The role of AI governance and agentic AI in OT cybersecurity;
- Strategies to bridge OT cybersecurity skills gaps across organizations.

WATCH ONLINE

"Threat intel, when done properly, should help scope down the problem for organizations."

Luke McNamara
Deputy Chief Analyst, Google Threat Intelligence Group, Mandiant

Jon Lau
Director of Cybersecurity, the Agency for Science, Technology and Research in Singapore - A*STAR

'Harvest Now, Decrypt Later' Attacks Drive Quantum Urgency

Jon Lau of A*STAR on Why IBM's 2033 Road Map Accelerates Q-Day Timeline

With IBM planning 1,000 logical qubits by 2033 and threat actors already stockpiling encrypted data, the quantum threat isn't a distant concern. Organizations must deploy NIST's post-quantum algorithms now, says Jon Lau, director of cybersecurity at Singapore's A*STAR.

> "A lot of the threat actors are now looking ahead. They are collecting all our data with the vision that once a quantum computer is available, they will be able to break them."
>
> *-Jon Lau*

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Lau also discussed:

- Why symmetric encryption like AES-256 remains more robust against quantum attacks than asymmetric encryption;
- How NIST's four standardized post-quantum algorithms provide replacement capabilities for vulnerable RSA encryption;
- The role of crypto agility in managing cryptographic assets as organizations transition to quantum-safe systems.

WATCH ONLINE

“We've gone down the pathway of ISO 42001, which is a governance and management framework, both on our product side and on how we consume AI in the business.”

Mike Beck
Global CISO, Darktrace

Driving Cyber Resilience Through Human-Centric Security

Seatrium's **Lim** on Redefining Cybersecurity Accountability for Industry 5.0

As Industry 5.0 transforms operations through human-robot collaboration, cybersecurity must shift from a technology-led model to human centricity, says Seatrium's Lim Shih Hsien. Clear accountability and simpler, human-centric frameworks help make security integral to daily operations.

> "At the boardroom level, we have to change our demeanor, the language we use when we present cybersecurity at the strategic level - it all starts from the top."
>
> ***-Lim Shih Hsien***

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Lim also discussed:

- How OT and IoT ecosystems are expanding the attack surface;
- Building observability and asset classification frameworks;
- Post-quantum and AI readiness for enterprise cyber resilience.

WATCH ONLINE

“It's not so much a security transition, but it's also a secure network transition... where customers have been struggling is integrating the concept of network and security because if you fail the network transformation, you'll fail the security transformation as well.”

Peter Molloy
Chief Growth Officer, ViewQwest

Adapting Global Cybersecurity to Diverse Markets

PayPal's **Phoram Mehta** on Aligning Cyber Strategies With Local Regulations

Cyberthreats know no borders, but regulatory and maturity levels differ across regions, says Phoram Mehta, vice president and head of international cyber risk at PayPal. He explores how a unified cybersecurity framework enables agility, compliance and digital trust across global markets.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Mehta also discussed:

- Using artificial intelligence for security efficiency and threat anticipation;
- Encouraging responsible AI adoption through enterprise-guarded tools;
- Implementing multifactor authentication and passkeys to balance security and convenience.

WATCH ONLINE

> "Resilience cannot be an afterthought. It has to be built in, something that we are looking at as we design our cloud modernization, cloud-native applications."
>
> ***-Phoram Mehta***

“You cannot be driving an AI strategy without thinking about cybersecurity for AI. We need to design for a world where platforms that didn't talk to each other now must - and where regulations must balance innovation and risk.”

Rashish Pandey
Vice President, Marketing, APAC, Fortinet

AI Governance Must Evolve for Non-Human Identities

Menlo Security's **Poornima DeBolle** on Securing AI Systems Without Slowing Innovation

Agentic AI is transforming enterprise operations, but managing non-human identities and ensuring security controls operating at machine speed are crucial to maintaining trust and control, said Poornima DeBolle, general manager of data security and chief technology and security officer at Menlo Security.

> "An agent can only do what it is limited to be able to do."
>
> ***-Poornima DeBolle***

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, DeBolle also discussed:

- Why enterprises must design systems that can keep up with AI's speed without compromising data protection;
- Why visibility tools must explain AI decisions, not just record them;
- How least-privilege and quick access revocation reduce risk.

WATCH ONLINE

"The most important thing in the moment is the trust in the broader population in all this change."

Royal Hansen
VP, Engineering, Google

Teo Xiang Zheng
Vice President, Advisory, Ensign InfoSecurity

Context Is Crucial in Cybersecurity

Ensign's **Zheng** on Why Compliance Alone Won't Stop Cyberattacks

Cybersecurity professionals with "boots-on-the-ground" experience say cyber defenders need contextualized threat intelligence - being able to understand the who, what and how behind an attack, said Teo Xiang Zheng, vice president at Ensign InfoSecurity.

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Zheng also discussed:

- The evolving role of CISO in business alignment and risk qualification;
- Where AI automation ends and human oversight begins;
- Enterprises that mistake compliance for resilience.

> "Contextualized cyberthreat intelligence in an organization and its business activities is very important for the management of risk appetite."
>
> ***-Teo Xiang Zheng***

WATCH ONLINE

"In the new era of cybersecurity, we need to take into account all the emerging technology moving from Industry 4.0 to 5.0."

Steven Sim Kok Leong
Chair, Advisory Committee, OT-ISAC

Vince Yap Lip Keong
President, ISACA Singapore Chapter

Cybersecurity Pros Must Master Risk, Not Just Tech

ISACA's **Vince Yap Lip Keong** on Risk Assessment Skills That Can't Be Learned Quickly

Cybersecurity professionals need risk management and communication skills alongside technical knowledge to navigate AI-driven threats, said Vince Yap Lip Keong, president of the ISACA Singapore Chapter. ISACA Singapore launches certifications and partnerships to address the evolving landscape.

> "The challenges that we are facing with human is that while technology is there to help, it also increases the complexity in managing cyber for the people."
>
> *-Vince Yap Lip Keong*

In this video interview with Information Security Media Group at the GovWare Conference and Exhibition 2025, Keong also discussed:

- How AI capabilities benefit both defenders and threat actors in cybersecurity;
- ISACA Singapore's collaboration with government agencies on AI frameworks and OT security;
- Emerging threats from deepfakes and synthetic media targeting corporate reputations.

WATCH ONLINE

“Shadow AI is real, and agentic AI is creating and dropping data across environments. If CISOs don't put the right controls in place upfront, they'll lose visibility - and with it, the ability to protect what matters.”

Todd Moore
Global Vice President, Data Security, Thales

ISMG Studio

About ISMG

Information Security Media Group (ISMG) is the world's largest media organization devoted solely to cybersecurity, information technology, artificial intelligence and operational technology. Each of our 38 media properties provides education, research and news that is specifically tailored to key vertical sectors including banking, healthcare and the public sector; geographies from North America to Southeast Asia; and topics such as data breach prevention, cyber risk assessment, OT security, AI and fraud. Our annual global summit series connects senior security professionals with industry thought leaders to find actionable solutions for pressing cybersecurity challenges.

Contact

(800) 944-0401
info@ismg.io

Sales & Marketing

North America: +1-609-356-1499
APAC: +91-22-7101 1500
EMEA: + 44 (0) 203 769 5562 x 216

BANK INFO SECURITY · CAREER INFO SECURITY · HEALTHCARE INFO SECURITY · GOV INFO SECURITY · infoRisk TODAY · CU INFO SECURITY · Data Breach TODAY · AITodayio · OT.today · PaymentSecurity.io · FraudToday.io · DeviceSecurity.io · CIO.inc · CyberEd.io · CyberEdBoard · CXO ADVISOR · CYBER THEORY · Xtra mile LIFECYCLE MARKETING · ATHENA · QC MEDIA · SUMMIT · custom events · roundtables · NULLCON · hardwear.io · ISMG Studio

ISMG

902 Carnegie Center · Princeton, NJ · 08540 · ismg.studio