



at GovWare Conference  
and Exhibition 2024

*Trust and Security in the Digital Era*



# GovWare Conference and Exhibition 2024: Trust and Security in the Digital Era



The landmark GovWare Conference and Exhibition 2024, Singapore's premier cybersecurity trade event held as part of Singapore International Cyber Week, brought together a community of cybersecurity professionals, including policymakers, tech innovators and information security leaders, from across 80 countries.

Under the theme "Securing Dynamic Digital Road Maps: Relooking Signposts in Identity, Trust and Resilience," the conference spotlighted critical developments in Southeast Asia's cybersecurity landscape. The region is at a critical juncture, facing several key challenges:

- **Geopolitical tensions:** The ongoing strategic competition between the U.S. and China, coupled with major conflicts in Ukraine and the Middle East, has heightened cybersecurity concerns.
- **Emerging technologies:** The rise of generative AI, large language models, automation and quantum computing is reshaping both offensive and defensive capabilities in cybersecurity.
- **Regional collaboration:** The growing need for collaborative defense strategies, international cooperation and effective responses to disruptive innovations.

As the event's media partner, we established a video studio at the conference, capturing insights from distinguished speakers - including CEOs, CISOs, government leaders, researchers and legal experts - through 34 distinct, in-depth interviews. These industry experts discussed innovative approaches, collaborative thinking and industry vision for embracing emerging technologies and disruptive tools.

Comprehensive coverage from the GovWare Conference interviews is featured across our Asian news network, including [inforisktoday.asia](https://inforisktoday.asia), [bankinfosecurity.asia](https://bankinfosecurity.asia), [databreachtoday.asia](https://databreachtoday.asia) and other media sites. You will also see insightful panel discussions and Profiles in Leadership interviews featuring members of our CyberEdBoard community.

In these pages, you can find the thought-provoking interviews conducted by our seasoned editorial team, offering valuable takeaways into building trust and security in the digital era. These conversations reflect the collective wisdom of front-line practitioners and industry leaders shaping cybersecurity's future in the region, providing an in-depth view of the latest information and thought leadership from GovWare Conference and Exhibition 2024.

A handwritten signature in black ink, appearing to read "N. Geetha".

Geetha Nandikotkur

*Vice President - Conferences, Asia, Middle East and Africa*

*Information Security Media Group*

Visit us online for more ISMG at GovWare Conference and Exhibition 2024: [ismg.studio](https://ismg.studio)



# Video Interviews

Rigo Van den Broeck, <i>Mastercard</i> .....	4	Aarthi Sureshkumar, <i>BTSE</i> .....	12
Joseph Carson, <i>Delinea</i> .....	5	Ian Monteiro, <i>Image Engine</i> .....	13
Shishir Kumar Singh, <i>Advance Intelligence Group</i> .....	5	Anand Raghavan, <i>Cisco</i> .....	14
Steven Sim Kok Leong, <i>ISACA Singapore Chapter</i> .....	5	Ashish Thapar, <i>NTT DATA</i> .....	14
Tarun Samtani, <i>International Association of Privacy Professionals</i> .....	5	Gaurav Keerthi, <i>Ensign InfoSecurity</i> .....	14
Charmaine Valmonte, <i>Aboitiz Group</i> .....	6	Gerry Chng, <i>Singapore Computer Society</i> .....	14
Jenny Tan, <i>ISACA Singapore Chapter</i> .....	7	Vishak Raman, <i>Fortinet</i> .....	15
Anthony Lim, <i>Singapore University</i> .....	8	Andre Shori, <i>Schneider Electric</i> .....	16
Philippe Bletterie, <i>Alcatel-Lucent Enterprise</i> .....	8	Tara Wisniewski, <i>ISC2</i> .....	17
Derek Manky, <i>Fortinet</i> .....	8	Goh Eng Choon, <i>ST Engineering</i> .....	18
John Lee, <i>Global Resilience Federation Asia-Pacific</i> .....	8	David Siah, <i>Centre for Strategic Cyberspace and International Studies</i> .....	18
Amirudin Abdul Wahab, <i>CyberSecurity Malaysia</i> .....	9	Pascal Geenens, <i>Radware</i> .....	18
Ken Soh, <i>Athena Dynamics</i> .....	10	Lam Kwok Yan, <i>Nanyang Technological University</i> .....	18
Richard Bird, <i>Traceable AI</i> .....	11	Dawn Cappelli, <i>Dragos</i> .....	19
Jojo Nufable, <i>St. Luke's Medical Center</i> .....	11	Frankie Shuai, <i>UBS</i> .....	20
Kanishk Gaur, <i>Cybersecurity Expert and Threat Intelligence Researcher</i> .....	11	Mex Martinot, <i>Siemens Energy</i> .....	21
Philip Dimitriu, <i>Sophos</i> .....	11		





## Rigo Van den Broeck

Executive Vice President, Cybersecurity Solutions, Mastercard

# Why Cybersecurity's Core Focus Should Be Defending Data

Mastercard's **Rigo Van den Broeck** on Ensuring Cybersecurity in a Data-Driven World

The proliferation of data in today's hyperconnected world presents significant opportunities as well as risks. Rigo Van den Broeck, executive vice president of cybersecurity solutions at Mastercard, said that as the digital landscape evolves, companies must adapt their defenses to keep pace with both the growing data landscape and criminals using advanced tools such as AI.

---

"There's more personal data out there, and we also see more connections to data, so it becomes more accessible."

- *Rigo Van den Broeck*

---

WATCH ONLINE

## IT as OT's Shield: Visibility Matters in Converged Defense

Delinea's **Joseph Carson** on Why Digital Credentials Remain a Critical Vulnerability



As OT systems become more interconnected, traditional air gaps disappear, creating new risks, said Joseph Carson, chief security scientist and advisory CISO at Delinea. The convergence of IT and OT environments requires a stronger focus on protecting digital identities and access controls.

WATCH ONLINE

## AI Governance: From Framework to Implementation

Advance Intelligence Group's **Shishir Singh** on Building Trust Through Explainable AI



Organizations implementing AI must establish structured governance frameworks that prioritize AI explainability and balance innovation with control, while ensuring regulatory compliance and risk management, said Shishir Kumar Singh, group head of information security at Advance Intelligence Group.

WATCH ONLINE

CyberEdBoard | Member

## CISOs Must Own OT Security in Industry 4.0 Era

OT-ISAC Chair **Steven Sim** on Why Legacy Systems Need Modern Security Architecture



The growing convergence of operational technology with business networks creates new attack vectors requiring CISO attention. Smart building components and industrial systems now pose risks to critical business functions, said Steven Sim Kok Leong, chair, executive committee at OT-ISAC.

WATCH ONLINE

CyberEdBoard | Member

## AI Implementation Demands Governance Before Deployment

IAPP's **Tarun Samtani** on Building Strong Governance Framework for AI Integration



As organizations rapidly deploy AI applications, many bypass crucial governance frameworks. This rush to implement without proper oversight creates significant compliance and security risks, said Tarun Samtani, advisory board member at International Association of Privacy Professionals.

WATCH ONLINE

CyberEdBoard | Member



**Charmaine Valmonte**

Chief Information Security Officer, Aboitiz Group

## CISOs Must Shift From 'Department of No' to Enablers of Secure Business

Aboitiz Group's **Charmaine Valmonte** on Building Cyber Resilience With Culture Change

Security leaders face challenges in testing organizational readiness while maintaining 24/7 operations. The key is to transform security from a barrier into an enabler, empowering employees to become part of the defense strategy, according to Charmaine Valmonte, CISO at Aboitiz Group.

---

“We are the department to allow through certain processes so that the business can continue to function and continue to innovate securely.”


- Charmaine Valmonte

---

WATCH ONLINE

Cyber**EdBoard** | Member



A portrait of Jenny Tan, a woman with long dark hair and glasses, smiling. She is wearing a red blazer over a black top. The background is blurred, showing other people in a crowd.

**Jenny Tan**

President, ISACA Singapore Chapter

## AI Risk Frameworks Must Focus on Talent, Not Just Technology

ISACA Singapore's **Jenny Tan** on Adapting Risk Strategies for the AI Era

Traditional technology risk frameworks may suffice for AI threats, but organizations must strengthen their approach to talent management and workforce resourcing to address emerging challenges in artificial intelligence deployment, said Jenny Tan, president, ISACA Singapore Chapter.

[WATCH ONLINE](#)

---

“The part of the risk framework that organizations have to relook at is AI-driven and impacted areas - it's more about talent, workforce resourcing.”

- **Jenny Tan**

---

## Why Security Must Shift From Compliance to Risk Management

**Anthony Lim** of Singapore University on Securing Legacy OT Using AI



Adopting standards like ISO 27000 can help organizations align with national security goals and regional cooperation, but simply following compliance checklists falls short, said Anthony Lim, fellow, cybersecurity, governance and fintech, Singapore University of Social Sciences.

[WATCH ONLINE](#)

## AI May Be the Missing Piece in IoT Security Puzzle

**Philippe Bletterie** of Alcatel-Lucent Enterprise on Securing Networks With AI and Zero Trust



With the proliferation of IoT devices, organizations face mounting security challenges from varying security protocols and authentication methods. AI-powered automation emerges as a crucial tool for managing this complexity, said Philippe Bletterie, vice president at Alcatel-Lucent Enterprise.

[WATCH ONLINE](#)

## Strengthening Cybersecurity With Public-Private Partnerships

Fortinet's **Derek Manky** on How Collaborative Tools Can Improve Intelligence Sharing



Derek Manky, chief security strategist and global vice president for threat intelligence at Fortinet, shares the importance of public-private partnerships in cybersecurity. There's a lot of vetted interest and mutual benefit in such partnerships, and the will to move forward is strong, he said.

[WATCH ONLINE](#)

## Critical Infrastructure Struggles With Legacy OT Security

GRF's **John Lee** on Balancing Legacy Systems With Modern Security Needs



As OT becomes increasingly connected to the internet, critical infrastructure operators must rethink their approach to cybersecurity while managing legacy systems that were not designed with security in mind, said John Lee, managing director, Global Resilience Federation Asia-Pacific.

[WATCH ONLINE](#)

CyberEdBoard | Member



A portrait of Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia. He is a middle-aged man with short dark hair, a mustache, and glasses, wearing a dark suit, a light blue striped shirt, and a red tie. He is smiling slightly. The background is dark and out of focus.

**Amirudin Abdul Wahab**

CEO, CyberSecurity Malaysia

## Malaysia's Push for AI-Driven Cybersecurity Standards

CyberSecurity Malaysia CEO on New Legislation to Protect Critical Sectors

Malaysia is strengthening its approach to cybersecurity with new AI guidelines and the Cyber Security Act 2024. The AI guidelines focus on the ethical use of AI across sectors, said Amirudin Abdul Wahab, CEO of CyberSecurity Malaysia.

---

“People are both the strength and vulnerability in cybersecurity.”

- *Amirudin Abdul Wahab*

---

WATCH ONLINE

Cyber**EdBoard** | Member



**Ken Soh**

Group CIO, BH Global Corporation Ltd.

## Addressing Cybersecurity Challenges in Maritime Operations

BH Global's **Ken Soh** on Why Maritime Security Needs Its Own Playbook

The maritime industry faces several challenges from cyberattacks, pushing it to quickly adapt to an evolving threat landscape while complying with new regulatory requirements. Ken Soh, group CIO at BH Global, outlines key strategies to protect offshore operations from escalating cyber risks.

[WATCH ONLINE](#)

---

“First, just like a NIST framework, we need to know our asset. Once we know the asset, we know what we’re protecting.”

- *Ken Soh*

---

## The Cloud Security Paradox: New Tech, Old Thinking

Traceable AI CSO **Richard Bird** on the Need to Unlearn Old Security Habits



Traditional data center security approaches do not translate very well to cloud environments as cloud computing and Layer 7 applications have fundamentally changed the way organizations should implement security controls, said Traceable AI's Richard Bird.

[WATCH ONLINE](#)

## Beyond Silos: When AI Meets Healthcare Security

Jojo Nufable of St. Luke's Medical Center on the Importance of Closed-Loop Systems



Healthcare has become the number one target for cyberattacks, with organizations spending an average of \$11 million per ransomware incident, says Jojo Nufable, vice president at St. Luke's Medical Center. He shares why traditional security approaches fall short as AI-powered devices proliferate.

[WATCH ONLINE](#)

## Digital Growth Outpaces Security: A Growing Crisis

Cybersecurity Expert **Kanishk Gaur** on Growing Security Implementation Gaps



As India accelerates its digital transformation journey, the lack of security-by-design principles in its expanding digital infrastructure has created unprecedented cybersecurity risks, particularly affecting financial services and healthcare sectors, according to Cybersecurity Expert Kanishk Gaur.

[WATCH ONLINE](#)

## When Threats Double - Healthcare's Cyber Wake-Up Call

Sophos' **Philip Dimitriu** on Sector-Specific MDR Solutions for Healthcare Security



Healthcare ransomware attacks have doubled since 2021, with 37% of organizations taking up to a month to recover, according to Sophos' State of Ransomware in Healthcare 2024 report. Organizations must rethink their approach to cybersecurity as attack surfaces expand and skills shortages persist.

[WATCH ONLINE](#)



A portrait of Aarthi Sureshkumar, a woman with long dark hair, smiling. She is wearing a red top and a gold necklace. A small microphone is clipped to her top.

**Aarthi Sureshkumar**

Head-IT, GRC & Privacy, BTSE

## Privacy Programs Need Top-Down Approach for GDPR Success

BTSE's **Aarthi Sureshkumar** on Balancing Compliance With Operational Efficiency

Organizations face challenges in implementing privacy frameworks that align with GDPR requirements while maintaining operational efficiency. Integrating of AI technologies adds new complexities to data protection and privacy compliance, said Aarthi Sureshkumar, head of IT GRC and privacy at BTSE.

---

“Most can trace their roots to GDPR. To be compliant with it, you often are required to have a very robust and mature privacy framework.”

- **Aarthi Sureshkumar**

---

[WATCH ONLINE](#)



**Ian Monteiro**

Executive Director, Image Engine

## AI and Cybersecurity: Same Goal, Different Approach to Data

Image Engine's **Ian Monteiro** on Resolving the Security-AI Implementation Conflict

Security leaders face a fundamental challenge as AI and cybersecurity take conflicting approaches to data handling. This divergence requires organizations to rethink their security strategies while maintaining resilience, said Ian Monteiro, executive director at Image Engine.

[WATCH ONLINE](#)

---

“Cybersecurity and AI are diametrically opposite in the way they approach data. For the CISO who is increasingly involved in business transformation, you have to take two different perspectives.”

- *Ian Monteiro*

---

## Enterprise Security Leaders Navigate AI Privacy Concerns

**Anand Raghavan** of Cisco on Building Trust in AI-Powered Security Solutions



As enterprises adopt AI for security, privacy and safety concerns remain top barriers. Organizations need robust frameworks and guardrails to ensure responsible AI implementation while protecting sensitive data, said Anand Raghavan, VP of engineering - AI, Cisco.

[WATCH ONLINE](#)

## Enterprises Need New Security Controls to Combat AI Risks

**Ashish Thapar** of NTT DATA on Why AI Governance Must Include Security Guardrails



As AI adoption accelerates across enterprises, security leaders face unprecedented challenges in data protection. To assess AI-related risks effectively, it's essential to understand the business goals and the context of AI applications, said Ashish Thapar, cybersecurity head for APAC at NTT DATA.

[WATCH ONLINE](#)

## AI's Probabilistic Nature Demands New Security Framework

Ensign InfoSecurity's **Gaurav Keerthi** on Rethinking Traditional Governance Rules



The probabilistic nature of AI is forcing organizations to rethink traditional cybersecurity governance frameworks. "Once you move from algorithmic software to probabilistic software, your traditional rules of governance don't apply anymore," said Gaurav Keerthi, head of advisory and emerging business at Ensign InfoSecurity.

[WATCH ONLINE](#)

## Beyond the AI Hype: Building Sustainable Governance

SIG Chairman **Gerry Chng** on Interdisciplinary Collaboration and AI Integration



Organizations integrating AI systems should adopt process-driven frameworks that mirror established cybersecurity standards, said Gerry Chng, chairman of the Singapore Computer Society's AI Ethics & Governance SIG. The ISO SC 42 committee's 42,000 series provides a foundation for developing AI policies and standards.

[WATCH ONLINE](#)



A portrait of Vishak Raman, a man with dark curly hair, wearing a grey suit jacket over a light blue shirt. He is smiling slightly and looking towards the camera. The background is blurred, showing other people and blue lighting.

## Vishak Raman

Vice President of Sales, India, SAARC, SEA, and ANZ, Fortinet

# 'Era of Point Products Is Over' in Enterprise Security

Fortinet's **Vishak Raman** on Taking a Platform-Based Approach to Cyber Resilience

With ransomware attacks increasing 13-fold in early 2024, organizations need to shift from point solutions to a platform-based approach and focus on secure networking, unified SASE and security operations, said Vishak Raman, vice president of sales - India, SAARC, SEA and ANZ - at Fortinet.

WATCH ONLINE

---

“The era of point products is over, and what we are seeing is a platform-based approach. This platform-based approach with the convergence of networking and security is happening in secure networking.”

- **Vishak Raman**

---



**Andre Shori**

CISO, APAC Governance, Schneider Electric

## Building Cyber Resilience Across OT, IT and IoT Environments

Schneider Electric's **Andre Shori** on IT-OT Convergence and Secure by Design

Andre Shori, CISO for APAC governance at Schneider Electric, shares how aligning OT and IT under a unified cybersecurity framework is key to resilience. Our goal is to embed security across the product life cycle, he said, while highlighting the company's commitment to protecting customer assets.

---

“The best way to do that is inculcating a strong culture of cybersecurity, building knowledge, and having the right talent and level of expertise to be able to deliver on our promise of quality and security.”

- Andre Shori

---

WATCH ONLINE

Cyber**EdBoard** | Member

A portrait of Tara Wisniewski, a woman with curly blonde hair, wearing a black top and large silver earrings. She is smiling slightly and looking towards the camera. The background is dark and out of focus, showing some blurred lights and shapes.

**Tara Wisniewski**

EVP, Advocacy, Global Markets and Member Engagement, ISC2

## New Security Leadership Style Needed for Stressed Workers

ISC2's **Tara Wisniewski** on Gathering Emotional Intelligence, Building Out Job Skills

With 75% of cybersecurity leaders facing the worst threat landscape they've seen and 90% reporting workforce shortages, emotional intelligence has become crucial for effective leadership and team retention, said Tara Wisniewski, EVP of advocacy, global markets and member engagement at ISC2.

[WATCH ONLINE](#)

---

“Not only continuous learning, but also making sure that [their teams] have strong communication skills so that they can engage with the business.”

- *Tara Wisniewski*

---



## High-Security Engineering Expands Beyond Encryption

**Goh Eng Choon** of ST Engineering on How D'Crypt M&A Enhances Security Innovation



The acquisition of D'Crypt strengthens ST Engineering's cryptographic and high-security engineering capabilities while addressing evolving OT cybersecurity challenges in critical infrastructure sectors, said Goh Eng Choon, president of cyber at ST Engineering.

[WATCH ONLINE](#)

## AI Ethics: The Human Cost of Machine Intelligence

**David Siah** of Centre for Strategic Cyberspace on AI Challenges and Global Data Governance



Organizations face mounting pressure to address workforce displacement and ethical implications as AI reshapes cybersecurity, particularly in software engineering roles. The challenge extends beyond job displacement to critical concerns about data privacy and transparency, said David Siah of the Centre for Strategic Cyberspace and International Studies.

[WATCH ONLINE](#)

## Offline AI Models: The New Frontier in Cyberattacks

**Pascal Geenens** of Radware on Risks and Benefits of Downloadable AI Models



As gen AI evolves beyond cloud-based models, downloadable AI models present new opportunities for both cybersecurity defenders and threat actors. The ability of offline models to bypass traditional ethical guardrails creates unique security challenges, according to Pascal Geenens, director, Radware.

[WATCH ONLINE](#)

## Race Against Quantum Threats: Why Organizations Must Act Now

NTU's AVP **Lam Kwok Yan** on Why Current Encryption Standards Need Immediate Transformation



With quantum computers threatening to break current cryptographic systems sooner than expected, organizations must transform their security infrastructure. Quantum migration requires not just technological solutions but also talent development and risk assessment strategies.

[WATCH ONLINE](#)

A portrait of Dawn Cappelli, a woman with short, wavy blonde hair, smiling. She is wearing a black and white checkered blazer over a black top and a necklace with a small pendant. A lapel microphone is clipped to her blazer. The background is dark and out of focus, showing some blue and green light patterns.

## Dawn Cappelli

Director of OT-CERT (Operational Technology - Cyber Emergency Readiness Team), Dragos

# Busting the Air Gap Myth: OT Security's Blind Spot

**Dawn Cappelli** of Dragos on Breaking Down IT-OT Security Myths and Building Resilience

Organizations mistakenly believe their operational technology systems are air-gapped and immune to cyberthreats. Dawn Cappelli, director of OT-CERT at Dragos, discusses why these assumptions are dangerous security gaps and why organizations need to rethink their approach to OT security.


WATCH ONLINE

---

“At Dragos, that's what we do. We do only industrial cybersecurity, and we have never found an organization that is truly air gapped.”

- *Dawn Cappelli*

---

A portrait of Frankie Shuai, a middle-aged man with short dark hair, wearing a dark suit, white shirt, and a blue patterned tie. He is smiling slightly and looking towards the camera. The background is dark and out of focus, with some blurred lights.

## Frankie Shuai

Former Head of Cyber and Technology Risk, Singapore and ANZ, UBS

# How Zero Trust Is Redefining Enterprise Security

UBS's Former Director **Frankie Shuai** on Implementation Success and Challenges

As organizations adapt to hybrid work environments and increased cloud adoption, zero trust architecture has evolved from a theoretical framework to an essential security approach, said Frankie Shuai, former head of cyber and technology risk for Singapore and ANZ at UBS.

[WATCH ONLINE](#)

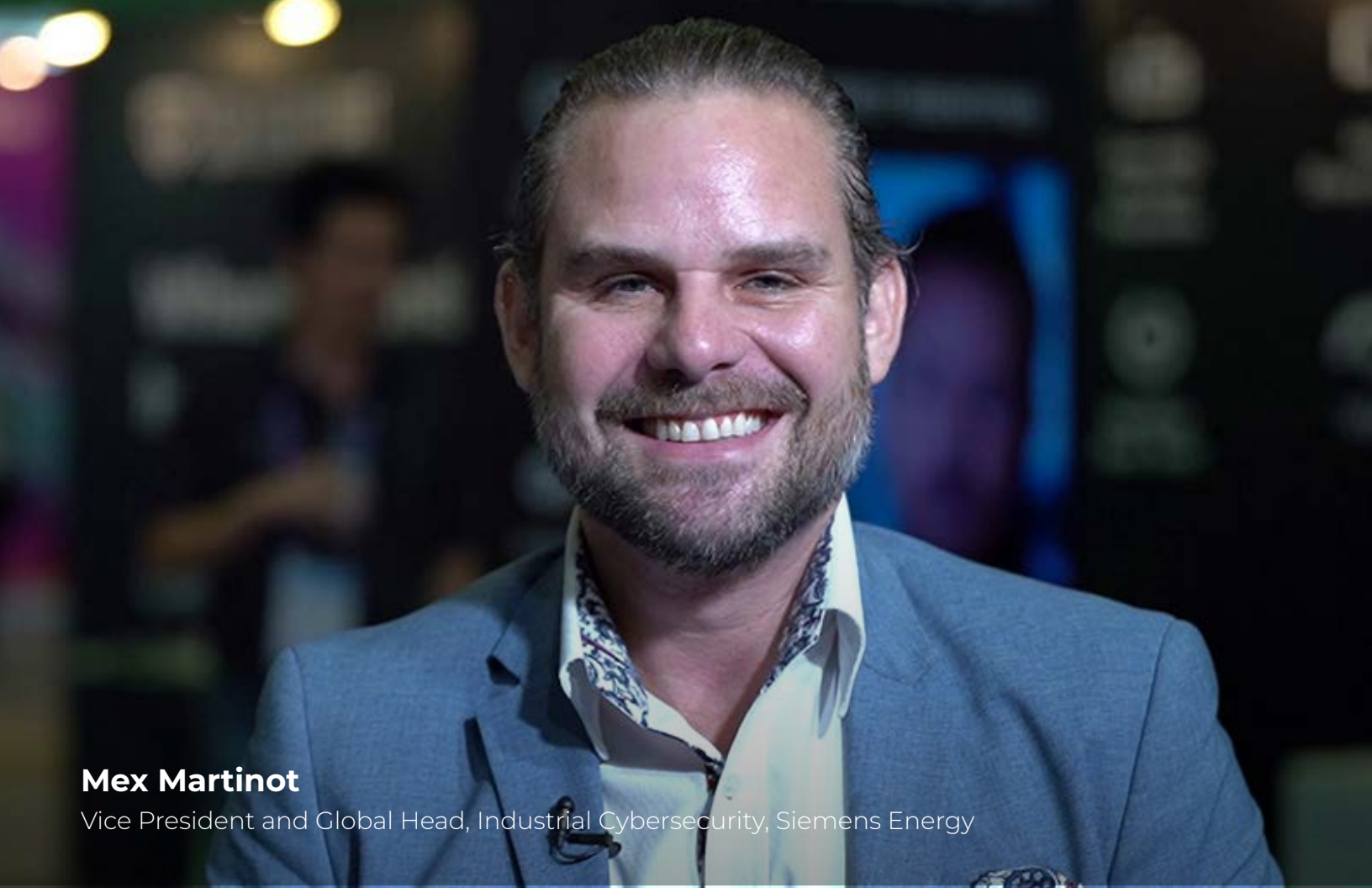
---

“When your data is sitting in your own data center, you can focus on your boundaries, make sure you have a solid parameter so that data sitting on data center may not be needed to be encrypted.”

- *Frankie Shuai*

---





## Mex Martinot

Vice President and Global Head, Industrial Cybersecurity, Siemens Energy

# Quick Wins vs. Long-Term: A New Approach to OT Security Risk

Siemens Energy's **Mex Martinot** on Phasing Security Controls for Industrial Systems

A "road map to resilience" approach helps organizations balance immediate, low-cost security improvements with complex, long-term risk reduction initiatives in industrial control systems, said Mex Martinot, vice president and global head of industrial cybersecurity at Siemens Energy.

---

"I came up with this concept called 'road map to resilience,' and it changes the definition if this is a high-priority issue versus it's a big investment."

- Mex Martinot

---

WATCH ONLINE

CyberEdBoard | Member

## About ISMG

ISMG is the world's largest media organization devoted solely to cybersecurity and risk management. Each of its 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, AI, OT, and fraud. Its 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

