

# Draft Programme – CISO 360 Asia & Oceania

Timings are not yet fixed. Input to topics and recommendations for speakers are very welcome.

## Day One: Wednesday 25 September

07:30 Coffee and Registration

### GLOBAL HORIZON, INNOVATION AND INVESTMENT

08:00 **Chairman's Opening Global Risk Horizon**  
Marcus Alldrick, Former CISO, Lloyd's of London and Principal Senior Advisor Risk, Compliance (UK)

08:00 **Leveraging security and innovation for a sustainable future**  
Government Representative – to be announced

08:30 **Keynote**

09:00 **Keynote Leveraging security and innovation for a sustainable future**

09:30 **Case study Innovation in information security management - AI for Good and Bad**  
From spear-phishing to deep fakes cyber criminals are leveraging artificial intelligence to attack users' trust. With organizational digital transformation CISO role is transforming into Chief Trust Officer. In addition to current traditional responsibilities a CISO has to be an innovation manager, an early adopter of the 'State of the Art' technologies and related processes in order to fully understand their opportunities and risks. Are you ready to transform? In this keynote I will share a few tips and hints for successful transformation.  
Dr Viktor Polic, Head of Information Security and Assurance Services Unit, International Labour Organization (ILO), United Nations, (Switzerland)

10:30 **Panel Big Questions - Cyber defence, privacy and trade-off predictions. What is technology's current emerging role in international diplomacy? Predictions**  
Technology is embedded in everything. There are no boundaries anymore. Engaging the audience with some of the big questions challenging leaders today. Hear inspiring insights from scientists, policymakers, inventors and business pioneers.

- Should cybersecurity technology be a strategic concern within international diplomacy?
- Cyber sanctions - Do institutions have the political will to act?
- As technological advances continue to outpace operations, legal and policy, how can we build trust in technology?
- How can we manage in a world plagued by disinformation?

Led by: Aloysius Cheang, Board Director and Executive Vice President for Asia Pacific, The Centre for Strategic Cyberspace + International Studies (Singapore); Lady Olga Maitland, Founder, UK Defence and Security Forum and Chairman, Copenhagen Compliance (UK)

11:00 Morning Coffee Break

11:30 **Panel Cybersecurity Ecosystems – Investment for innovation and to strengthen resilience**  
Infrastructure and global initiatives need to be underpinned by a culture that nurtures and embodies innovation to build a thriving startup ecosystem. To successfully implement and build an entrepreneurial ecosystem, many countries, including Singapore, are turning towards the Israeli start up ecosystem model.

- Global governance structure. Do we need an "ICT 20" - what is the body we bring together in a global crisis?
- What are we doing to architect and secure to drive digital transformation?
- Initiatives to strengthen talent and innovation and to successfully build an entrepreneurial ecosystem in cybersecurity
- What responsibility should security play in driving innovation? How do we apply innovation to counter cyber threats?
- What is the right level of prescriptive law and regulation for cyber risk?
- Which technologies and subsectors will be the most attractive to venture and corporate investors over the next year?
- What are the differences in the way financial institutions assess potential investments in cybersecurity?
- What are the benefits to corporates that actively engage with the start-up market?

12:00 **Case study National future strategy planning**

Irene Corpuz, Manager, Strategy and Future Department, HCT Government Entity (UAE)

- 12:20 CISO 360 Think Tank: Digital strategy and innovation - CISO as the Enabler**  
 The CISO 360 Think Tank provides the opportunity for CISOs to benchmark lessons learned and tried and tested approaches to deal with 4 areas within a wider subject matter. In this case, the key artefacts of innovation: AI/ML; Big data analytics; Cloud; Mobile/IoT. This includes sharing successes with peers as well as failings. Two table facilitators will make detailed notes for contribution to the tangible takeaway. This report will be distributed to all attendees following the event with the combined thoughts and conclusions from CISOs from international companies. Table questions for feedback to the audience:
- How are we bridging risk and vulnerabilities with the rest of the business?
  - What role are these technologies currently playing?
  - How does DevSecOps fit within the business risk strategy for this technology?
- Roundtable 1: Artificial Intelligence/ Machine Learning**  
**Roundtable 2: Big data analytics**  
**Roundtable 3: Cloud** - When Cloud is your Security Friend: When should you as a CISO be encouraging the rush to the Cloud – When it makes it easier to secure your most valuable assets and/or make it easier to deliver the extreme rigour in detection and response that today's threat environment demands. And how do you explain that to your top management?  
**Roundtable 4: Mobile and IoT**

**13:00 Lunch**

## SECURITY LEADERSHIP, GOVERNANCE AND LINES OF DEFENCE

- 14:00 Case Study Developing scenario analysis as a cyber risk tool**  
**Tobias Gondrom, Group CISO, UOB (Singapore)**
- 14:30 Keynote Tips from the front-line and the Boardroom**  
 When is enough, enough: How do you know when to stop investing in more security? Can you invest too much? How do you respond when the CEO asks when “security will be done”?  
**Dr John Meakin, Director, Cyber Transformation, HSBC (UK)**
- 15:00 Case Study 360 Cyber Resilience and Cyber Risk Management**  
 A roadmap of achieving a resilience posture - by weaving security across the organization from IT, Business Continuity, Disaster Recovery, Business under the umbrella of Risk.  
**Eng. Manan Qureshi, APAC Head of Security Strategy, Risk & Compliance Practice, IBM Security (Singapore)**
- 15:30 Afternoon Tea Break**
- 16:00 Audience Q&A Panel What are the 3 things that companies and CISOs/CIOs do wrong when it comes to cybersecurity? How do we take our cybersecurity strategies to the next level?**  
 A new era for CISOs, CIOs, CSOs discussion on the current biggest responsibilities, priorities and challenges.
- What are the biggest security threats your organisation faces over the next year?
  - What needs to be done today to prepare for tomorrow?
  - What are the most effective strategies you are using right now?
  - How do we move from a legacy world to a new world?
  - How do we take our own cybersecurity strategy to the next level?
  - Convergence - changing the mindset from the leaders to the end users. How we approach and perceive cybersecurity.
- Panellists: Chuan-Wei Hoo, CISO, ST Engineering (Singapore) and CISOs, CSOs and strategists**
- 16:30 On Stage Interviews Governance is a team sport – 3 lines of defence to build resilience, privacy and trust**  
 An on-stage discussion with prominent GRC c-suite about what are the key governance and compliance challenges going forward
- Who are the risk owners, how can they protect themselves and their organisations?
  - Do we need more regulation and common standards or is the answer internal alignment on good practice security risk management?
  - Risk appetite – 5-6 priorities. Regular review process
  - How do we more effectively align risk across our companies?

- How do we sift the wheat from the chaff to determine which technologies are delivering on their promise to enhance security? Auditing and Risk Management of Emerging Technologies
- Integrating cybersecurity and operational risk to meet regulatory compliance
- Taking a risk-based approach to cyber defence - How do you train your risk programme towards the new risks?
- Board directors - can spend on new technologies but 70% people/30% technologies. People and processes is not expensive but requires leading by example and priority
- Supply chain risk - with so many vendors how do we make good supplier choices?

**17:00 Panel How do we build truly diverse, authentic and inclusive risk and security teams?**

We need to diversify the composition of our teams and therefore the way that we identify roles, amend the way we recruit to include differences of life experience, age, ethnicity, gender, sexuality, workability and neurodiversity, whilst recognising that all differences should be positive, not negative. If we have any chance of thinking like the criminals to build organisational resilience, we need to diversify our teams and therefore way we recruit and build our teams.

- What can we do to encourage diversity and inclusion? Is positive discrimination levelling the playing field?
- Is the alleged lack of cybersecurity skills a pipeline challenge or a bias challenge?
- Are we committed to evolve rather than to stand still when we talk about diversity?
- Authenticity - why covering remains a necessity
- Thinking outside the box - can your culture support this person to enable them to do their best? If everyone thinks the same, decision-making is faster and more agile but is it right?
- Check and balance - a diverse and inclusive culture
- What are emerging key skills for a security professional, beyond the obvious?
- Organisational security education and training

**Including: Marcus Alldrick, Former CISO, Lloyd's of London (UK); Irene Corpuz, Manager, Strategy and Future Department, HCT Government Entity (UAE)**

**17:30 Close of Day One**

**18:00 Reception and Cultural Activity**

## Day Two: Thursday 26 September

08:55 **Chairman's Re-opening**

### FINANCIAL CRIME, CYBERCRIME, THREAT INTELLIGENCE

09:00 **Keynote Business process governance in operational risk - How can we leverage opportunities?**  
**Dr Guan Seng Khoo**, Board Adviser, **Fintech Companies** (Former Head of ERM/GRC, **Alberta Investment Management Corporation - AIMCo**) (Singapore)

09:20 **Case study Data fraud and theft – analytics, intelligence and investigations**  
**Chuan-Wei Hoo**, CISO, **ST Engineering** (Singapore)

09:40 **Keynote How to Transform your SOC (Security Operations Centre) for Maximum Efficacy**  
**Edvinas Pranculis**, Vice President, Global Sales Operations, Data Protection Officer (DPO), **SOC Prime Inc.** (Lithuania/ U.S.)

09:50 **Panel Ethical dimensions and practical challenges of ML/AI applications and other advanced technologies - facial recognition**

Defining the current state of ML and AI technologies and sharing current case studies in cybercrime prevention and information security management.

- Balancing AI with Human Intelligence in the SOC: How not to get blinded by the hype and ensure that AI/ML is used selectively and intelligently – as a really useful enhancement for your most valuable security resource (the people)
- Which are the core ethical principles and practical challenges for designing and implementing ML/AI applications?
- Protecting businesses and organisations against harmful practices and cyber enabled crime – How can AI be used in order to understand human behavior better at an organisational level and successfully predict mistakes and deliberate insider compromises?
- Adversarial machine learning intelligence – Is Adversarial Machine Learning being used currently in order to develop and challenge ML/AI systems in cybersecurity and if so how?
- How do these technologies align with the potentially conflicting interests and aims of law enforcement, businesses and governments and where do you see points of friction arising in future developments of security focused ML/AI?

**Panellists: Dr Guan Seng Khoo**, Board Adviser, **Fintech Companies** (Former Head of ERM/GRC, **Alberta Investment Management Corporation - AIMCo**) (Singapore)

10:20 **CISO-CSO 360 Roundtable Converged Threats and Solutions – Cyber-Physical-Operational Technology**  
Destructive strains specifically target industrial and manufacturing firms - at times forcing production plants to switch to manual control or exacting long-term damage on systems that control physical equipment. To date, used by financially motivated criminals, this type of attack could be used by state-sponsored critical infrastructure hackers with national geopolitical agendas in mind.

11:00 **Morning Coffee Break**

11:30 **Panel How can we ever strike a balance between attackers and defenders as our surface areas keep expanding?**

Attackers opponents and access to cheaper tools and there is an imbalance because the defenders have more work to do than the attackers. They are not opponents. Will we always be at the mercy of attackers if we cannot better leverage regulation, policy, intelligence sharing and technology?

- How can companies develop a responsive approach to deal with cyber criminals who continuously evolve their tactics?
- What type of cyberattacks will threaten your company over the next year?
- AI & Machine Learning to combat corporate crime - seen and unseen threats
- Keeping ahead of fraud & financial crime
- What factors will determine which companies will become the best protected and most resilient players in the industry over the next few years?
- Blockchain technology– where are we today?
- How can innovation enhance protection, detection and response processes?
- Asymmetric cyber warfare - we have policy, lawyer. How do we turn trust and sharing into a technology?
- Data explosion, analytics and threat intelligence - How can we take leverage opportunities?

## RISK MITIGATION – WHAT IS YOUR PLAN B

### 12:00 **CISO 360 Think Tank CISO View on Risk Mitigation, Assessment and Testing**

The CISO 360 Think Tank provides the opportunity for CISOs to benchmark lessons learned and tried and tested approaches and practical use cases to deal with 4 areas within a wider subject matter. From AI to crowd sourcing, credit scoring methods to traditional pen-tests, hear directly from the CISO directly what CISOs think a comparison of what pen-testing options are available today, costings and how this can impact cyber insurance. Crowd sourcing, credit scoring methods, traditional pen-tests... What are CISOs using? What is working, what isn't? A cutting-edge comparison of what testing options are available today, costings and impact. Two table facilitators will make detailed notes for contribution to the tangible takeaway. This report will be distributed to all attendees following the event with the combined thoughts and conclusions from CISOs from international companies. Table question examples for feedback to the audience:

- What are the most dangerous emerging threats we are seeing?
- What do we see as the insurance implications of various pen testing models?
- What role are new technologies currently playing in testing?
- How does this fit within the business risk strategy?

**Roundtable 1: Crowd Sourcing and Bug Bounties**

**Roundtable 2: Testing and AI/ML**

**Roundtable 3: Testing and Business Risk Strategy**

**Roundtable 4: Emerging Threats and New Technologies**

### 13:00 Lunch

### 14:00 **Case study Insider threat**

**Alex Quintieri, Group CISO, FWD Insurance (Hong Kong)**

### 14:20 **Group Scenario Planning Catastrophic risk**

**Dr. Sally Leivesley, Director, Newrisk Ltd, A Founder Member, The Exercise Group7 (UK)**

### 15:00 **Keynote Cyber insurance market updates – meaningful risk management and prevention. What is our Plan B?**

Technology is embedded in everything. There are no boundaries anymore. There is no more a plan b. how do we increase business resilience. What is our plan B? If our data is corrupted. We need a good baseline with meaningful data in a changing landscape.

- What does a good plan B look like?
- How does a cyber event take down a nation's financial system?
- As technological advances continue to outpace operations, legal and policy, how can we build trust in technology while remaining accessible?
- Which technology solutions are proving most effective for insurance cyber risk management?

### 15:20 **Case study How do we calculate the real cost of catastrophe? Putting hard numbers to hidden losses that lurk beneath the surface**

To protect against threats to corporate value, many companies rely too heavily on insurance coverage. The function of the CFO is to protect the value of the company. One of the most insidious threats to corporate value is sudden disruption from events like fire, hurricane, flood, earthquake, or cyberattack — disruption that is ostensibly insured. There's always a portion of that kind of loss that's uninsured! How do we out numbers on this?

- Hidden Losses - investor panic and stock plummets erasing % of the enterprise's value
- Formerly nebulous risks - quantifying the risk of uninsured loss can help CFOs make better strategic decisions before learning the hard way
- Quantifying the risk of lost enterprise value in a disruption effectively calculates the true value of resilience
- Modeling the Total Loss: Customer Loss; Lost growth; Lost investor confidence
- Using financial models to win investment in security!

**CFOs, CISOs..**

### 16:00 Close of Day Two, Afternoon Tea and Goodbyes

# Testimonials

View video from our most recent CISO 360 Congress [here](#)

- “Excellent event, opportunity to meet like-minded professionals, sharing risk, worries, tools, best practices with CISOs from other industries sharing same issues, great eye opener, looking forward to the next event”, **CISO, MS Amlin**
- “Nowhere else will you find such relevant content for CISO’s, shared by leaders in their fields”, **Director Security Engineering, Inmarsat**
- “The best speaker line-up of any security conference!”, **Head of UK Security, AXA**
- “Pulse have raised the bar when it comes to planning and running conference events. Other organisers should take note.” **CISO, Channel 4**
- “Great speakers, great venue, intelligent discourse, Pulse CISO 360 Congress has it all!” **Director of Information Security EMEA, Canon Europe**
- “The CISO 360 conference brought together a collection world leading experienced security leaders who shared their knowledge and experience with their peers in an open and collaborative manner under The Chatham House Rule. This was complimented with case studies from selected top tier partners and organisations to provoke further debate and discussion during the talks or later during 1x1 networking conversation. The presentations; case studies; and strategy sessions were practical and relevant because they were born out real world security challenges faced by Global CISO’s across multiple sectors. I found the open knowledge sharing; networking; and presentations were very valuable to either validate existing approaches or provoke fresh ideas by getting a different perspective.” **Global Head of Information Security Architecture & Transformation, Royal Bank of Scotland**
- “Refreshing views of security topics for knowledge improvement!” **CISO, Credibom**
- “Top class speeches and presentations at the CISO 360 Congress in Barcelona! Thanks for such a worthwhile and enjoyable time” **Blueliv**
- “By far the best event for 2018 I have attended. I always make an effort to attend CISO 360 as it is not just an event, it is a trusted community that comes together from around the world!” **Group CISO and Group DPO, MS Amlin**
- “A unique opportunity to share challenges thoughts and ideas with trusted friends, and gain valuable insights.”, **President, (ISC)2 Scotland Chapter**
- “CISO 360 is a must attend conference to keep up to the latest trends, best practices as well as main security concerns within the cybersecurity landscape” **GRC Specialist, Euronext**
- “I’m very pleased to be part of this extraordinary event – very important to exchange ideas and hear experiences and ideas from peers across sectors!” **Corporate Security Manager, Logista**
- “Marvellous event, well-run, packed with useful content you can use”, **Technology Services Head of Security, DWP**
- "The conference is full of expert speakers. You wouldn't want to miss any of them. Particularly on the Boardroom/ Roundtable discussion (last day), it is like a strategic planning and facing the board of directors, but with less pressure. Excellent!" **Section Head - Planning & IT Security, Western Region Municipality - UAE Government**
- “Pulse organised a fantastic CISO 360 Congress, which brought together some of the world's most successful CISOs to discuss pressing cyber security issues and share experiences. The agenda was diverse, with senior professionals from across the globe sharing their experiences, and great networking sessions were facilitated by the organisers with good food and flowing conversation. I would highly recommend CISO 360 and look forward to this conference going from strength to strength!” **Freaky Clown, Co-Founder, Head of Ethical Hacking, Redacted Firm Ltd**
- "Pulse Conferences stand out for being up to the minute with developments and concerns. First rate speakers and an agenda that is total appropriate and informative. Excellent buzz and networking." **CEO Copenhagen Compliance; Founder, Defence and Security Forum**
- "Thank you, Pulse Conferences, for a great event. CISO 360 combined interesting varied talks with fantastic networking opportunities, facilitating very interesting thought-provoking conversations" **Co-Founder, Socio-Technical Lead, Redacted Firm Ltd**
- "I found CISO 360 Congress a great place to share ideas about current and future problems" **Head of Section, GMV**
- “Excellent conference! Brilliantly put together. Looking forward to the next one.” **Director, Bridewell Consulting (Official Sponsor)**