CYBER SECURITY ASIA 2019

Building a Secure & Resilient Future-Ready Organization

4 - 5 November 2019 | Rosewood Hotel Phnom Penh, Cambodia

Each day, cyber threats become increasingly intricate and difficult to detect. The toll from attacks in Asia exceeded those in North America and the EU by about $20 billion each and accounted for more than a quarter of the $315 billion cost of attacks globally. Over the past year, we saw that with the rise of device connectivity came boundless opportunities for malicious hackers to attack device vulnerabilities. With the support of forward-thinking security strategies and technology solutions to match, the modern business can minimize potential risk and step into a digital future confidently.

Phannarith Ou
ICT Security Director
MINISTRY OF POSTS & TELECOMMUNICATIONS (MPTC), CAMBODIA

Dato' Ts Dr. Haji Amirudin Abdul Wahab
CEO
CYBERSECURITY MALAYSIA

Mark van Staalduinen
Blockchain & IoT Security
INTERPOL

Fabrice A. Marie
Group CISO
AIRASIA

Theo Nassiokas
APAC Cyber & Information Security Director
BARCLAYS

Parag Deodhar
Information Security Director
VF CORPORATION, HONG KONG

Doron Sivan
CEO
CRONUS CYBER TECHNOLOGIES, ISRAEL

Jorge Sebastiao
Chief Technology Officer
HUAWEI TECHNOLOGIES, UAE

Abhinav Mishra
Bug Bounty Hunter & Founder
ENCIPHERS, INDIA

Paul Jackson
MD, Cyber Risk Practice Head
KROLL HONG KONG

Shamane Tan
Executive Advisor – APAC
PRIVASEC, AUSTRALIA

Paul Craig
Head of Offensive Security
VANTAGE POINT, SINGAPORE

Dhillon Kannabhiran
CEO
HACK IN THE BOX, MALAYSIA

Ahmad Rizan Ibrahim
Partner
CONSULTING BOARD ASIA

Tarun Samtani
Global Data Protection Officer
BODEN, UK

Brian Hay
Executive Director
CULTURAL CYBER SECURITY, AUSTRALIA

Lim Chin Wan
Deputy General Manager
VATTANAC BANK, CAMBODIA

Abhijitt Mukharjji
MD & CISO
CYBERZEST GLOBAL, AUSTRALIA

Chris Cubbage
CEO
MY SECURITY MEDIA

Murari Kalyanaramani
Executive Director, Security Technology Services
STANDARD CHARTERED BANK

Exclusively by:

Media Partners:

Supporting Organization:

Strategic Partners:

Platinum Sponsor:

Gold Sponsor:

Exhibition Booth:

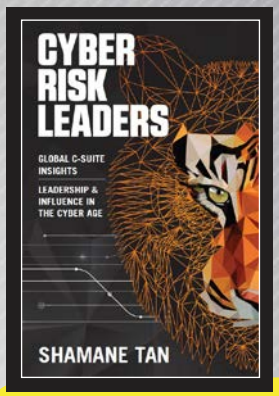
Overview

Security is not simply about having the right resources; it further requires organizations to reexamine their strategies in order to tackle unprecedented cyber threats. In a world in which agile new entrants are constantly disrupting industries, it is essential for organizations to equip themselves with mindset, knowledge, experience and tools that will keep their infrastructure and information safe. Those that do not will be less competitive - and even risk becoming obsolete.

Cyber attacks can impact any industry at any time. In fact, as more industries become increasingly connected to the Internet due to the Internet of Things, it is more essential than ever to consider if your organisation is cyber ready for 2019 and beyond.

We look forward to welcoming you and your peers at Cyber Security Asia 2019 Conference & we will help you navigate the Digital Danger Zone.

Is your organization ready to make the change?



Register before 27 September 2019 to get a complimentary -CISO book of the season **"CYBER RISK LEADERS"** *authored by* **Shamane Tan**

> *"Cyber Security is a shared responsibility, & it boils down to this: In Cyber Security, the more systems we secure, the more secure we all are"*
>
> ***Jeh Johnson***

DID YOU KNOW?

60% Digital businesses will suffer major service failures due to the inability of IT security teams to manage digital risk (2020)

90% Asia Pacific Companies have been hit by some form of Cyber Attack

40% Asian Government & Corporate Clients suffered from Ransomware Demands

72% CEOs Not Fully Prepared for Cyber Crimes or Attacks

$32.9bn APAC Cyber Security Market Expected to grow to **$32.9** billion by 2019

WHY ATTEND

- Everything You Need To Learn and Everyone You Need to Meet in The Cyber Security Sphere
- Discover the Security Use Cases, Business Models and Roadblocks that Can Support Your Digital Transformation
- Learn From International Thought-Provoking Cyber Security and Cyber Risk Experts
- Connect with Global technologist and Early Adopters to Expand your Network

WHO SHOULD ATTEND

- Chief Executive Officers
- Chief Operating Officers
- Chief Information Security Officers
- Chief Information Officers
- Chief Risk Officers
- Chief Technology Officers
- Cyber Security Professionals
- Heads of Digital Transformation
- Heads of Insights and Analytics
- Operation Risk Heads and Managers
- Technology Risk Heads and Managers
- Cyber Security Experts

DAY 1

7:45-8:40am **Registration & Breakfast**

8:45-9:05am **Opening Keynote: Sponsor Opportunity**

9:05-9:35am

Cambodia Cyber Security Landscape moving to Digital Economy

Cambodia has also been targeted. Our government system and private sectors also experience cyber-attack in the form of Advanced Persistent Threat (APT), Phishing, Malware hence compromised the system. Last year, we were experiencing DDoS attack in history that brought our several major ISPs down and effect most of online transactions in the kingdom. Incident response in timely manner, better coordination, technical capability and information sharing are the keys to minimize the big impact during the attack. However, due to lack of effective coordination mechanism with other countries, the challenge to handle the incident still remains. Phannarith discusses:

- Cambodia Digital Statistic and its landscape
- Cambodia government policy on Cyber Security
- Building tomorrow's cyber-workforce

Phannarith Ou, *ICT Security Director*, **MINISTRY OF POSTS & TELECOMMUNICATIONS OF CAMBODIA**

9:40-10:15am

Building a Successful Cyber Program

As security incidents accelerate in both frequency and severity, the transparency of the aftermath increases as well. Employees, Boards of Directors, and even the public are more aware of the potentially devastating nature of cyber attacks, and they want to know exactly what you're going to do about it. In this session, Dato' Amirudin shares insights gleaned from almost two decades working in cyber security for enterprise companies and the federal government. He explores the critical lessons learned over the course of a remarkable career, including his tips on building a world-class global Cyber Security program.

Dato' Ts Dr. Haji Amirudin Abdul Wahab, *CEO,* **CYBERSECURITY MALAYSIA**

10:15-10:35am **Morning Break**

Panel Discussion:

10:35-11:10am

Cyber Security Strategies & Policies: An APAC Perspective

The region has a greater share of the global economy than any other-and is poised to face some of the greatest cyber security challenges. But the Asia-Pacific is many nation-states, not one, and they are divided in both capacity and approach to how to prepare its businesses today for the cyber challenges of tomorrow.

- Hear from Asian experts on the challenges and opportunities that cyberspace presents, in terms of governance structure, legislation, law enforcement, business and social engagement with cyber policy and security issues.
- An overview of cyber security policy throughout APAC
- How can Governments work hand-in-hand to combat cybercrime in APAC?

Panelist:

- **Phannarith Ou**, *ICT Security Director*, **MINISTRY OF POSTS & TELECOMMUNICATIONS**
- **Dato' Ts Dr. Haji Amirudin Abdul Wahab**, *CEO*, **CYBERSECURITY MALAYSIA**
- **Mike Phone Myint**, *Director Risk Assurance*, **PwC MYANMAR** *(tba)*
- **Ahmad Rizan**, *former President*, **MIMOS** | *Partner*, **CONSULTING BOARD ASIA**

11:15-11:50am

Cyber Resilience: Practical Recommendations In Combating Cyber Threats

Now your financial institution is hacked and on the front page of news. Customers, Board, Press, and Regulators are hounding you by the minute. How you do prioritize proactive and reactive measures to mitigate the risks and minimize the impact of breaches. This session covers how an organization should plan and implement effective controls in response to the ever changing threat and regulatory landscape.

Murari Kalyanaramani, *Executive Director, Security Technology Services,* **STANDARD CHARTERED BANK**

11:50-12:25pm

Six Ways to Protect Your Organization from Insider Cyber Risk

Cyber risk discussions often center around how criminals, nation states, hacktivists and/or terrorists could breach perimeter defenses to carry out objectives such as data theft, denial of service and financial fraud. But what about the trusted employees, contractors and third-party suppliers that already have legitimate access to your systems and data? These are commonly neglected data breach vulnerabilities. To reduce insider risk, it is imperative that your internal policies, procedures and controls are as strong as your perimeter defenses. Paul discusses are some best practices that organizations of all sizes, in all industry sectors, should establish or strengthen to protect their organization

Paul Jackson, *MD,* **Cyber Risk Practice Head, KROLL, HONG KONG**

12:25-1:10pm

Security Risk of Industry 4.0

Industry 4.0 or the fourth industrial revolution is happening all around us, and is changing the landscape of business and economics. Digitally evolved business can now deploy a single mobile application and attract millions of customers in just a few days, physical premises are no longer required, and the number of staff needed is greatly reduced - while profits soar sky high. Although there is no doubt the future will be digital, what happens when security vulnerabilities compromise the very building blocks of Industry 4.0 and hold multi-billion-dollar enterprises to digital ransom or exploitation. This talk will address the security risks associated with Industry 4.0 and show examples of how application vulnerabilities and security failings can literally knock down the walls of a digital business.

Paul Craig, *Head of Offensive Security* I *Chief Hacking Officer,* **VANTAGE POINT, SINGAPORE**

1:10-2:00pm

Lunch

Panel Discussion:

2:00-2:35pm

Discovering the Digital Underworld: Privacy, the Dark Web, Tech & Democracy

You can't protect what you don't understand. In order to better anticipate how to secure our networks, we need to start thinking more like attackers. In this session, our panelists discuss how major breaches still happen in 2019, how criminals are making use of not only the dark web but also how they're leveraging next generation machine learning and artificial intelligence tools. These experts will share their insights into how technology is not only changing society in fundamental ways, but enabling the next generation of cybercrime while also bringing forth new challenges around surveillance, democracy and data privacy.

Moderated by:

- **Dhillon Kannabhiran**, *CEO*, **HACK IN THE BOX, MALAYSIA**

Panelist:

- **Craig Paul**, *Head of Offensive Security*, **VANTAGE POINT, SINGAPORE**
- **Abhinav Mishra**, *Bug Bounty Hunter & Founder*, **ENCIPHERS, INDIA**
- **Fabrice A. Marie**, *Group CISO*, **AIRASIA, SINGAPORE** *(tba)*

2:35-3:10pm

Mobile App Security: Examine the Complexity to Hacking Mobile Apps & How to Secure Them?

An attack surface for hackers, which is in hands of everyone, is continuously moving, contains sensitive user/organizational data, connects to different wifi. These are nothing but mobile applications. Users provide their most sensitive details like personal information, financial information, and health information to these mobile applications. But are these applications secure enough to handle such an amount of sensitive data? Let's look at some of the most common vulnerabilities in mobile applications, which may lead to full account takeover and in some case server takeover too. This talk will focus on some of the most common and emerging mobile application vulnerabilities, their root cause and also discuss how an organization can ensure such vulnerabilities are not affecting their products/apps.

Abhinav Mishra, *Bug Bounty Hunter & Founder,* **ENCIPHERS**, **INDIA**

3:15-3:50pm

Partners In Fighting Crime: Building Collaboration Between Business, Government, Academia, Community & Law Enforcement

Cyber Crime is a robust and rapidly expanding successful global business. And the only way it is going to be tackled is through collaboration by the good guys - business (both end-users and security vendors), law enforcement, academia, community and government. When attacks happen, they nearly always cross geographical borders and demand international co-operation within law enforcement. When a company is attacked the priority objective is to get back to business as soon as possible rather than hold up the business to enable police investigation. With reputations at risk there is often reluctance by organizations to share the lessons learned from an attack. And whilst vendors have highly skilled technical teams researching and actively defending against threats, this often gets lost amongst the snake oil of FUD marketing and media hype. So how can organizations cut through conflicting priorities to work together effectively to fight cybercrime? Brian will share perspectives on this topic to develop a roadmap to effective collaboration going forward.

Brian Hay, *Executive Director,* **CULTURAL CYBER SECURITY, AUSTRALIA**

3:50-4:20pm

Tea Break & Networking

4:20-4:55pm

I-AM-AI: The Future Of Artificial Intelligence Is Us

Organizations are increasingly leveraging Artificial Intelligence to enhance their cyber security strategy. From machine learning to deep learning to artificial intelligence; are we on the brink of unleashing robot overlords aimed at turning the human body into a battery? Not just yet! From AI in the movies to AI in real life, one thing is certain - AI IS going to eat EVERYTHING, but do not be afraid, be prepared.

Dhillon Kannabhiran, *CEO*, **HACK IN THE BOX, MALAYSIA**

5:00-5:25pm

Sponsorship Opportunity

5:25-6:10pm

Practical Analytics: A Hands-on Approach to Detecting Cloud- and IoT-based Cyber Threats

Our job as network and security professionals is to monitor and analyze systems for the unexpected. Cloud and IoT-based networking solutions and devices are now part of the infrastructure we secure. Let's take a deep dive into some of the tools, tips, tricks and traps that can help us identify how today's hackers exploit our systems. In this presentation, Jorge will provide insights and stories gathered throughout the world. He will discuss ways to identify and combat covert channels in today's networks, as well as ways to analyze and report these issues to your boss.

Jorge Sebastiao, *Chief Technology Officer*, **HUAWEI TECHNOLOGY, UAE**

DAY 2

9:00-9:35am

Cyber Crisis Communications

The application of contemporary crisis management principles and practices now requires an understanding of cyber security, incident response, cyber related legislation, including new legislation for mandatory data breach reporting and regulatory frameworks emerging in Europe, Asia and United States. This session will examine a number of case studies and insight into the formation and roles of the crisis committee, communication planning, cyber breach notifications and communicating with authorities, stakeholders and the public.

Chris Cubbage, *CEO*, **MY SECURITY MEDIA, AUSTRALIA**

9:35-10:10am

The Next Generation of CISO

As businesses evolve so does the role of the CISO, with security leaders needing to stay one step ahead of the game to ensure they meet the varying demands of the board and communicate risk and intelligence in a meaningful way, along with implementing all of the aspects required to build the very best holistic security infrastructure possible.

Examining our next generation of CISOs:

- How the role of the CISO has evolved
- Not all CISOs are equal
- Global perspectives and modern day challenges
- CISO Insights
- Navigating the Board and Executives

Shamane Tan, *APAC Executive Advisor,* **PRIVASEC** | *Founder*, **CYBER RISK MEETUP**

10:15-10:30am **Morning Break**

10:30-11:10am

How Exactly Can CIOs Mitigate Cyber Risk?

In a world where cyber threats seems to be getting more complex and prolific, this presentation removes the technical jargon and explains what cyber threats really are by identifying actors and motivations to real events, giving the audience a real sense of the challenge that awaits:

- It connects cyber events to real actors and geopolitical events reported in the press
- Provides a clear view of the real challenge regarding cyber threats, including motivations
- Explains how to go about quantifying cyber threats, in a defensible manner
- It identifies alleged state sponsored cyber threat actors alleged crimes committed

Theo Nassiokas, *APAC Cyber & Information Security Director,* **BARCLAYS**

11:10-11:45am **Sponsorship Opportunity**

Panel Discussion:

11:45-12:30pm

How to Present Cyber Security Risk to the Board and Convincing your CEO on Cyber Resilience as a Business Enabler

- How much damage are cyber criminals inflicting on the financial services sector at the moment and what be prepared for in the future?
- Cyber security as a strategic risk management issue. Does your board understand the cyber threats faced by your organization? How to gain their support and turn your cyber security strategy from a costly procedure to a business enhancer.
- The main steps of creating an effective cyber security strategy for the financial institutions. Which practical operational measures and IT solutions should you have in place to improve cyber security?
- Cyber security as'a people issue'. Ensuring a skilled workforce. How to educate your employees to deal with the new realities of cybercrime?

Panelist:

- **Theo Nassiokas**, *APAC Cyber & Information Security Director*, **BARCLAYS**
- **Lim Chin Wan**, *Deputy General Manager*, **VATTANAC BANK, CAMBODIA**
- **Murari Kalyanaramani**, *ED, Security Technology Services,* **STANDARD CHARTERED BANK**
- **Parag Deodhar**, *Information Security Director,* **VF CORPORATION, HONG KONG**

12:30-1:05pm

Three Steps To 95% Cyber Security

Catch, Patch and Match are the 3 worded mantra to get yourself 85% Cyber Secured. If we can catch the vulnerabilities and patch them while making it happen on a regular interval, we can block 50% cyber-attacks. Additionally, if we can ensure the default credentials are changed before applications, appliances or special purpose devices are taken into production, then we can further strengthen our shields by 25% more bringing us at 75% Cyber Security. For an extra 10% mark, organizations need to control their admin credentials while ensuring users are being provided access to their resources on 'Need to Know' basis. Abhijeet will discuss how to work around Vulnerability assessment, E-mail security and User awareness to make your organization 95% Cyber Secured.

Abhijitt Mukharjji, *MD,* **CYBERZEST** | *former CISO*, **DOWNER GROUP, AUSTRALIA**

1:05-2:00pm **Lunch**

Panel Discussion:

2:00-2:40pm

Robotics 2025 and Beyond – Crime Trends Coming:

Similar to the impact of drones, across all market verticals, the rise of the robot will be a new challenge with the obvious 'pros and cons' for consumers, corporations, governments and security providers. This session examines societal change, crime risk and establishing public policy and public space suitable for a safe digital transformation. This session will discuss:

- Robots will be part of the IoT and Industrial IoT landscape – what will be the associated cyber risks to consider.
- Robots and Drones present a risk of 'fireant' warfare" – what is the consequence of this risk in civil society.
- What public policy should be put in place for the convergence of AI/ML, Robotics and Human Computer Interface Technologies – and the cyber risk associated with these technologies.

Moderated by:

Chris Cubbage, *CEO,* **MY SECURITY MEDIA, AUSTRALIA**

2:40-3:15pm

Offensive Artificial Intelligence

World renowned web application security expert discusses how Artificial Intelligence will accelerate cyber attack sophistication, security measures bypassing and scaling up vulnerability and exploit Research & Development.

TBA

3:15-3:55pm

Building Your Organization Data Privacy Programme

- Determining the scope of data privacy in your organization and nurturing privacy champions
- Realigning your business strategy with privacy and data protection regulations
- Building a data protection programme for the first 100 days of initiation
- Driving change and instilling a culture of data compliance awareness

Tarun Samtani, *Global Data Protection Officer,* **BODEN, UNITED KINGDOM**

3.55-4.15pm

Tea Break

4:15-4:55pm

Developing an Enterprise-Wide Secure Cloud Strategy for the Business of Tomorrow

- Implementing and enforcing policies on cloud ownership, responsibility and risk acceptance
- Understanding which users, networks, risky third party applications, and devices are accessing an organization's cloud data
- Assessing the different cloud models to evaluate its different risk and control ramifications
- Defining and implementing the right security strategy, models and tools to secure the data on the cloud

Parag Deodhar, *Information Security Director*, **VF CORPORATION, HONG KONG**

4:55-5:35pm

Rebooting our Cyber Security Framework: What are We Not Doing Right?

- Where are the weak points in our current practices? Identification and counteraction
- Outlining and implementing new practices
- How does this development affect people, process and technology?
- What results can we expect to see, and what sort of timescale are we looking at?

Fabrice A. Marie, *Group CISO,* **AIRASIA**

5:35-6:10pm

Blockchain Technology: Detecting and Solving Cybercrime

The spotlight on compliance and regulation continues to intensify as cryptocurrency transforms the way people transfer value and move money. While headlines often focus on the use of cryptocurrencies for criminal activities, like money laundering and ransomware, the reality is that cryptocurrencies like bitcoin can be much friendlier to cops than they are to criminals when trying to trace the proceeds of crime or find stolen funds. In fact, blockchain technology can provide information and tracing capabilities not available with more traditional forms of payment like cash or even the traditional banking system. Utilizing these unique features inherent to blockchain technology, in particular immutable ledger, law enforcement and the blockchain industry have developed software analytic and investigative tools to trace funds and detect criminal activity that would otherwise be difficult to discern. Mark will walk you through detecting and solving different types of cybercrime and offer thoughts on the future of criminal use of cryptocurrencies.

Mark van Staalduinen, *Innovation Manager,* **TNO, SINGAPORE** | *Seconded Cybercrime Expert,* **INTERPOL**

Closing Keynote:

6:10-6.55pm

Transition to AI and Machine Learning in Information Security

- The complexity of hardening business processes
- The transition to huge computer systems: smart city, government systems and the required complexity.
- How to transition to AI and Machine learning addresses these needs

Doron Sivan, *CEO,* **CRONUS CYBER TECHNOLOGIES**

7:00-8.00pm

Evening Reception : CYBER RISK MEETUP

BIOGRAPHY

Phannarith Ou is the Director of Information and Communications Technology (ICT) Security of Ministry of Posts and Telecommunications of Cambodia. He is the former Head of National Cambodia Computer Emergency Response Team (CamCERT). He had been involved in the development of Cybercrime Law, E-Commerce Law, Cambodia ICT Masterplan 2020 and Digital Signature legislation. Mr. Ou has been invited to present in global conferences, forums and seminars and he is the ISLA-(ISC)2 award in 2016. In December 2012, he was awarded as one of the top 10 Chief Information Security Officers (CISO) in ASEAN by the International Data Group (IDG). In addition to his posts in the public sector, Mr. Ou has been the Assistant Professor at Build Bright University (BBU) on various subjects such as the Information Security and Privacy, E-Commerce and Cyber Laws. He is the founder of the first leading information security awareness website (www.secudemy.com) in Cambodia.

Brian Hay is the Executive Director of Cultural Cyber Security - a Thought Leader in the world of Cyber Security. He learned his craft not from the technical demands of the industry but rather by focusing on the activities of organised crime and cyber criminals. Prior to joining Unisys, Brian was General Manager, Security for Dimension Data, Australia. He was also the Detective Superintendent at Queensland Police for 35 years. Since 2004, he has worked extensively in the area of financial, identity and cybercrime. He was Commander of the Queensland Police Fraud & Cyber Crime Group, Chair of the Australia New Zealand Police Advisory Agency's eCrime Working Group, and member of the Federal AG's National Cybercrime Working Group. In 2009 Brian was the recipient of an international award from McAfee for efforts in combating cybercrime. Brian is also the recipient of the Australian Police Medal, and in 2010 he was the recipient of the National AusCERT Award for Individual Excellence in Information Security.

Chris Cubbage is the CEO of My Security Media based in Australia. He is a technology journalist, court recognised public safety expert and a specialist in crime and security, city operations, video surveillance systems, enterprise security and governance. Spanning a career of 28 years, with combined experience in high profile, international investigations and extending to corporate enterprise and public safety experience, Chris is a Certified Protection Professional with ASIS International, Certified Information Systems Auditor with ISACA, Registered Security Professional of Australasia, Graduate of the Australian Institute of Company Directors and holds an honours degree in Security Science with Edith Cowan University and diplomas in policing, criminal investigation and business management.

Dato' Ts Dr. Haji Amirudin Abdul Wahab is currently the Chief Executive Officer of CyberSecurity Malaysia, a strategic agency under the Ministry of Communication and Multimedia,Technology and Innovation. He has more than 25 years of ICT working experience in the telecom and IT sector in the Government as well as in the semi-government and private sectors. Through his leadership at CyberSecurity Malaysia, Dato' Dr Amirudin contributed to Malaysia's achievement in attaining number #3 rank in the world, in the 2014 International Telecom Union (ITU) Global Cyber Security Index and becoming the first World Trustmark Alliance Chairman to be reappointed to a second term. He was selected to receive ASEAN's Outstanding Chief Information/ Security Officer Award in 2014.

Theo Nassiokas is a cyber security and tech risk executive. He is Barclays International's Chief Information Security Office (CISO) and its Director of Asia Pacific (APAC) Cyber & Information Security. With his diverse experience ranging from law enforcement and criminal intelligence to risk and security strategy within government and financial services, and as an acknowledged authority in security, risk, compliance and e-fraud, Theo has publicly spoken on these topics on many occasions. Theo holds an MBA (Tech Mgt), certifications in general and information security management (CPP and CISM) and is a member of the Association of Banks Singapore (ABS), Standing Committee on Cyber Security (SCCS).

Parag Deodhar is the Director - Information Security for Asia-Pac at VF Corporation. In his earlier role he was the Asia CISO for AXA Group. Parag is a Chartered Accountant, Certified Information Systems Auditor from ISACA, US and Certified Fraud Examiner from ACFE, US. Parag has over 19 years' experience in Enterprise Risk Management, specializing in Operational Risk, Information Security, Business Continuity and Fraud Risk Management. He has worked in Cyber Security, Audit, Consulting and Program Management functions with multinational companies like AXA Group, KPMG and Tech Mahindra.

Paul Craig leads the offensive security "Tiger Team" at Vantage Point based in Singapore. Paul originally hails from New Zealand and is an avid hacker with a passion for the dark art of exploitation. Paul has been hacking professionally for the past 13 years and considers nothing impossible. Paul Craig works with Asia's strongest and largest banks to help raise their security bar and keep Singapore safe. He developed techniques and tools that are taught in the SANS Advanced Penetration Testing (SEC660) course and he has spoken at over 50 international security conferences world-wide.

BIOGRAPHY

Dr. Mark van Staalduinen's main interest lies in the understanding of cybercrime innovation driven by the current pace of internet technologies, like blockchain and IoT. As the founder of TNO's Dark Web program, he conducts cyber threat research and delivers training together with INTERPOL Global Complex for Innovation in Singapore. Besides his scientific profile, he has a strong focus on law enforcement. He is a seconded cybercrime expert to INTERPOL Global Complex for Innovation in Singapore. He is also the Innovation Manager at TNO with focus on Dark Web, Blockchain Security and Cybercrime. He received his MSc in Electrical Engineering from Delft University of Technology (DUT) in 2003. Full-time committed to internet-driven innovations in safety and security since 2012. From January 2016, Dr. van Staalduinen holds position at TNO Singapore to strengthen international partnerships in his capacity of deputy director of the Singapore office.

Jorge Sebastiao is the Chief Technology Officer for Huawei Technologies based in Dubai. He is also a seasoned managed services, cloud computing & security professional focused on business value and he brings experience, creativity, structure and innovation to the solutions in ICT. He has over 28 years of ICT experience, covering C-level on Cloud computing, Cyber Security, Physical Security, Managed Services, business continuity, and disaster recovery as well as governance, risk management, compliance, auditing, and certification. He has served many sectors including oil & gas, banking, financial, telecom, government, defense, healthcare, and education. Jorge created the process A6 of security: Assess, Architect, Apply, Administer, Awareness & Agility. He architects practical & business focused Cloud and Security solutions using standards & industry best practices.

Shamane Tan works with C-Suite executives to ascertain the best approach for uplifting the corporate security posture in a cyber age. She has successfully enabled businesses, as well as enterprises and agencies, to manage cyber risk. Shamane has a passion for disruptive technologies and the human factor. As the founder of Cyber Risk Meetups across Australia and Singapore, her events offer security enthusiasts and executives an important platform to impart and exchange innovative insights. Shamane is an advocate and business champion for professionals within the cyber risk sector and actively encourages people to look for new ways in which they can take a step forward.

Abhinav Misha is the founder of ENCIPHERS, a fast growing information security consultancy and training firm based out of India. Abhinav a.k.a. `0ctac0der` also head the penetration testing, training and other offensive security projects teams. He has an experience of 8+ years in penetration testing of web/mobile/ infrastructure and training. He started his career right after the college graduation in 2011, though he has been actively hacking (ethically) long before. When he hacked his college ERP application in 2010, he realized the potential of the skill and also the need to secure the internet. Since then, Abhinav have been helping organizations, by penetration testing their web/mobile apps, infrastructure, and training the teams. Abhinav has spoken at numerous security conferences, meets and events. Abhinav also holds multiple accolades and rewards for finding security issues through responsible disclosure/bug bounty programs.

Fabrice A. Marie is currently the Group CISO at AirAsia, overseeing Information Security for AirAsia group of companies, and helping with the fast digital transformation journey. Previously Fabrice worked as CISO of Lazada (Alibaba Group), CTO of Kibin Labs and IT Security Director of FMA Risk Management Solutions. He has over 20 years of experience in: Security Management & Risk management, capacity planning, prioritization of efforts to meet deadlines on budget, building teams from scratch, managing teams of security experts and developers, penetration testing, application secure coding as well as code reviews, infrastructure and cloud infrastructure security automation, intrusion Prevention Systems, "Firewalling" and "Application firewalling" innovative research, Internet payment systems, automatic risk management in the Banking, Telecom, Government, Military and security agencies. He is a regular speaker at regional IT security technical conferences as well a regular interviewee on television for IT security matters.

Dhillon Kannabhiran (@l33tdawg on Twitter) is the Founder and Chief Executive Officer of Hack in The Box. Prior to quitting his day job to lead the HITB team on crazy adventures around the world, Dhillon started off at the height of the dotcom craze as a technology journalist with PC World, ZDnet, MIS Asia and CNet. When the bubble burst, he moved on to a Malaysian telco as Chief IT Officer to spend his days in the world of Cisco AS5300s, in a land of packet switched networks at a time when Asterisk did not just mean '*'. Today, he spends his days surrounded by emails, spearheading all of HITB's strategic efforts and driving the HITB team crazy. And for 3 months every year, he cycles as much of The Netherlands as he can.

BIOGRAPHY

Tarun Samtani is the Group Data Protection Officer for Boden. Boden is a British clothing multi-channel retailer selling online, by mail order and with a high street presence, markets across UK, Europe, US, Asia and Australia. Tarun holds over 20+ years of experience across various sectors like Telecommunications, ISP's, Financial Services, Gambling, Retail and most recently Pharmaceuticals. He has a wealth of experience in Cyber security & Data privacy and is passionate about securing business information landscape. During the course of his career Tarun has been involved in the strategy & planning, design, architecture and implementation of a significant number of information security programmes. His specializations include strategic board advisory, building roadmaps planning through delivery of security / privacy programmes including building a security awareness culture, data security, GDPR and data loss prevention.

Murari Kalyanaramani is the Executive Director, Security Technology Services at Standard Chartered Bank. He has successfully built and managed global information & cyber security capability and led multinational and multi-location teams in global strategy & governance definition and implementation, industry partnership & outreach efforts, operational service delivery and transformational initiatives during his career with Standard Chartered Bank, British American Tobacco (BAT) and PricewaterhouseCoopers (PwC).He currently serves on the International Board of Directors for the Financial Services Information Sharing and Analysis Centre (FS-ISAC) and on the FS-ISAC Asia Pacific Strategy Committee. Murari has also been recently appointed as a financial services industry representative on the Singapore Cyber security Consortium which has been created for engagement between industry, academia and government agencies to encourage research, manpower training and technology awareness in cyber security He has also previously served on the ISACA International Professional Standards Committee (PSC), Professional Standards and Career Management Committee (PSCMC) and the Board of Directors for the ISACA Malaysia Chapter.

Mike Phone Myint is a seasoned technology executive with experience in Cyber security, Enterprise Risk Management, Business-centric GRC implementations and CX-centered Digital Experience Expert. He is a dedicated Project Manager with quality delivery focus. Mike has over 18 years of proven track record with a demonstrated history of working in the telco, ISP, education and financial services industry.

Lim Chin Wan challenges, informs and entertains his audiences on many of the key issues in banking security, in order to stimulate 'out-of-the-box' thinking to help organizations generate new visions, strategies, products and services. Chin Wan's technology and business experience spans over 15 years in the domains of strategy, operations, technology esp. security, web and mobile platforms for banks. He has successfully architected five banking products before joining Vattanac Bank. He founded iMocha Consulting in 2003 and started providing cash management software to CIMB Bank, Hong Leong Bank and AmBank. In 2003-2005, Chin Wan envisioned, designed, developed and delivered CIMB BizChannel, a PKI based digital signature product suite for cash management via the Internet; the first in Malaysia.

Doron Sivan is an information security expert and advisor to banks, municipalities, multi-national enterprises, and various Israeli government branches on analyzing scenarios of cyber-attacks on critical systems. He holds a BSc in Physics and an MBA, is the author of several books used by the Israeli Defense Forces (IDF) to instruct cyber intelligence units, and lectures in the prestigious 8200 IDF Intelligence Unit. Doron founded Cronus Cyber Technologies in order to provide a unique software based solution for automated Penetration Testing. His company is a global provider of machine-based penetration testing and predictive Attack Path Scenario™ (APS) solution called CyBot where their patented technology imitates human ethical hackers operating practices to discover, predict, analyze, and mitigate the risk of sophisticated global cyber attacks - all in real time. Cronus has also been awarded "Most Innovative MSSP Solution" by CDM and listed as "One of 12 companies transforming the cyber industry" by CBInsights.

Ahmad Rizan Ibrahim has over 30 years of management and consulting experience in the ICT industry experience worldwide. He is well versed in solution delivery to clients in the areas of strategic planning, M&A, technology design and implementation, package and custom development and operations management. Rizan was a partner with Arthur Andersen LLP during which he held the role of ASEAN Enterprise Application Head. He was also the President of MIMOS Berhad, Malaysia's national Applied Research and Development Centre, a strategic agency under the Ministry of International Trade and Industry (MITI). Currently he is a partner of CBA, a boutique alliance of senior consulting partners to help ease companies business entry into Asian growth markets.

BIOGRAPHY

Paul Jackson is Asia-Pacific Leader for Kroll's Cyber Security and Investigations Practice, based in the Hong Kong office. Over a career spanning more than 25 years of service in some of the region's highest levels of law enforcement and corporate enterprise, Paul has earned a stellar record of achievement as a cyber security practitioner, strategist, and thought leader. Paul was the APAC Head of Fraud and High Tech Investigations for JP Morgan Chase Bank. From 2012-2014, he relocated to New York where he served as the bank's Global Head of High-Tech/Cyber Investigations. In this role, Paul managed a global team of cyber investigators and responders throughout the United States, Europe, and Asia, focused on addressing the pressing needs of managing the evolving threats faced by a global financial institution.

Abhijitt Mukharjji is the CISO of CyberZest. A dynamic digital security evangelist with over 20 years experience in Security Leadership around Governance Risk and Compliance of Information Security, Cyber Security, ICT Management, Brand Protection, Cyber Crime Prevention and Cyber Forensic Investigations with qualifications like Masters in Computer Application (MCA), MBA in IT from Indian Institute of Management - Calcutta (IIM-C) India, LLB General Laws, Post Graduate Diploma in Cyber Laws & IPR Management from Indian Law Institute, New Delhi and Industry revered certifications like CISSP, ISSMP, CISA, PCI DSS QSA, PCIP, CEH, CHFI, PRINCE2P, ITIL, SABSAF and SCRUM Master.

Registration Contract

CYBER SECURITY ASIA 2019

Building a Secure & Resilient Future-Ready Organization

4 - 5 November 2019
Rosewood Hotel Phnom Penh, Cambodia

Confirm your seat with :

THOMVELL **+603 2260 6500**

Fees

Subsidized fee for SECUDEMY clients, associates & affiliates only

- ☐ Subsidized fee @ **USD300.00** by 25th October 2019
- ☐ Conference fee @ **USD450.00** after 25th October 2019
- ☐ Premier Plus @ **USD 1,800.00** for group of 5 delegates from the same company

(All fees are EXCLUSIVE of 10% VAT)

Details

Organization name:.....
Address:.....
Postcode:.....
Country:.....
Tel:.....
VAT Taxation number:.....

Delegate

1. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
2. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
3. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
4. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....
5. Name:.....
   Job title:.....
   Email:.....
   Telephone:..... Ext:.....
   Mobile:.....

Invoice

The Invoice should be directed to Mr / Ms / Dept:
Name:.....
Dept:.....
Tel:.....
Email:.....

Authorisation

Signatory must be authorized to sign on behalf of contracting organization

Name:.....

Job title:.....

Signature:.....

Email:.....

Telephone:.....

Mobile:.....

Venue

ROSEWOOD PHNOM PENH
Vattanac Capital Tower, 66 Monivong Boulevard,
Sangkat Wat Phnom, Khan Daun Penh,
Phnom Penh, Kingdom of Cambodia
Tel: +855 23 936 888

Hotel Accommodation:
Special rates have been negotiated with the hotel for conference delegates. Please make your bookings directly with the hotel and indicate that you are attending

CYBER SECURITY ASIA 2019

Method of payment

PAYMENT MUST BE RECEIVED BEFORE EVENT

Bank Transfer

Payment by bank transfer must quote the event code TVW4837 and delegate name. Transfer should be made to:

Account Name : ZOOKEEPER MEDIA CO. LTD.
Account No : 1010 1250 0000 6589
Bank Address : CIMB Bank, Olympia Branch, St 336, Phnom Penh, Cambodia

Cancellation

You may subsitute delegates at any time. THOMVELL INTERNATIONAL does not provide refunds for cancellations. For cancellation received in writing more than seven (7) days prior to the conference you will receive a 100% credit to be used at another THOMVELL INTERNATIONAL event for up to one year from issuance date.

THOMVELL INTERNATIONAL shall assume no liability whatsoever in the event this conference is cancelled, rescheduled or postponed due to a fortuitous event, Act of God and unforseen occurence.

3 EASY WAYS TO REGISTER

Thomvell International Sdn. Bhd.

8-1 Jalan Tun Sambanthan 3, 50470 Kuala Lumpur

+603 2260 6500

tcharles@thomvell.com | azlin@thomvell.com | karen@thomvell.com

For official use only

Received: Date..... Code: **TVW4837**