CONFERENCE PROGRAM

08:15 –08:50	Registration
08:50 –09:00	**Opening Remarks:** **Ir. Daniel Lai, BBS, JP** **Government Chief Information Officer (GCIO)** **The Government of the HKSAR**
09:00 –09:30	**Opening Keynote: Changing The Game - Adopting A New Cyber Philosophy** Information security has always been a high stakes game, one that demands a smart strategy, the right technology, and an unblinking focus on adversaries. Today, however, both the game and the opponents have changed. To win, businesses must play by new rules and bring advanced skills and strategy to the table. In this presentation, the speaker will share key findings from The Global State of Information Security Survey 2014 and discuss a new Cyber Security Philosophy that companies should adopt to stay ahead of Cyber Threats in this information age. Opening Keynote Speaker: **Mr. Ramesh Moosa** **Partner, Forensic Services** **PricewaterhouseCoopers**
09:30 –10:00	**Keynote 1: What is a Secure Cloud?** Security represents one of the biggest challenges for the Industry every year and is often a main concern with the adoption of Cloud technologies. This session will share insight to considerations of what constitutes a secure Cloud, in which to help consumers make informed decisions regarding their Cloud vendors. **Mr. Chris Levanes** **Director of Cloud Business Development, APAC** **CenturyLink Technology Solutions**

10:00 –10:30	**Keynote 2: Data Center Security: Beyond Traditional Protection** **Mr. C. K. Lam** **Director, Data Center Virtualization & Automation** **Advanced Technologies, APAC** **Juniper Netowrks**
10:30 –11:00	**Keynote 3: Using Big Data Analytics To Improve Security And Compliance** Many heads of Security Services struggled with an underperforming traditional SIEM to keep the organization both secure and compliant. Learn how Splunk turned to a big data analytical approach to SIEM to more effectively perform incident investigations, uncover known and unknown threats, and create the reports and evidence required by auditors. **Mr. Paul Pang** **Chief Security Strategist** **Splunk**
11:00 –11:15	**Morning Networking Coffee Break and Showcase Tour**
11:15 –11:45	**Keynote 4: Best Practices To Combat The Advanced Persistent Threat** The typical advanced attacker operates undetected for 243 days in a victim's network. When they are discovered, security teams often lack the investigative expertise, adversary intelligence and capabilities to formulate an effective response. Join Justin Harvey, Chief Solution Strategist at FireEye as he examines effective strategies to respond to computer security incidents using the latest case study illustrations. Attendees will also gain a better understanding of how Advanced Persistent Threats can impact organisations, the challenges faced and best practices to combat and respond, for a continuous threat protection" **Mr. Justin Harvey** **Chief Solutions Strategist** **FireEye**

11:45 –12:15	**Keynote 5: Innovative Approach To Protect Against Advanced Persistent Threats (APTs)**
	As high-profile targeted attacks expand and evolve, enterprises and government departments must guard against complex, often invisible threats. A protection that goes beyond the limitations of standard defenses to detect and analyze attacks in real-time, actively prevents network intrusion and contains threats will help organisations achieve a new level of defense against advanced threats. In this session HP will join Trend Micro to introduce an innovative approach to defeat targeted attacks.
	Mr. Kelvin Wee **APJ Regional Product Manager – HP ArcSight** **HP**
	And
	Mr. Tony Lee **Consultant** **Trend Micro**
12:15 –13:05	**Panel Discussion One: Maintaining Privacy And Security In The Cloud**
	Panel Chair: Mr. Geoff McClelland, Program Director, CIO Connect HK
	Executive Panelists: • Ms. Anna Gamvros, Partner, Baker & McKenzie • Mr. Joe Locandro, Director IT, Cathay Pacific Airways • Mr. SC Leung, Senior Consultant, HKCERT • Mr. Ted Suen, Head of IT, MTR Corporation • Mr. Iolaire McKinnon, Director of Technology, Security Consultancy Services, UBS

13:05 –14:05	**Executive Networking Luncheon Roundtable (By Invitation Only)** **Sponsored by CheckPoint & Dimension Data** **Topic: Today's Security For Tomorrow's Threats** **Mr. Allan Wong** **Director, Professional Services** **Dimension Data**
14:05 –14:50	**Panel Discussion Two: Managing The Evolving World Of Mobility** **Panel Chair:** Mr. Michael Mudd, Managing Partner, Asia Policy Partners LLC **Executive Panelists:** • Mr. Peter Mo, Head of IT Greater China & Head of Technology Risk Management APAC, Credit Suisse • Mr. Dominic Polisano, VP & Deputy CISO, Hong Kong Exchanges and Clearing • Mr. Francis Fung, CTO, Midland Realty • Mr. Stephen Langley, Deputy CIO, IT, Corporate Affairs, Securities and Futures Commission
14:50 –15:20	**Keynote 6: Intelligent Cybersecurity For the Real World** To truly protect against all possible attack vectors, IT professionals must accept the nature of modern networked environments and devices and start defending them by thinking like defenders responsible for securing their infrastructure. Critical to accomplishing this is first understanding the modern threat landscape and how a threat-centric approach to security can increase the effectiveness of threat prevention. The session will begin with a detailed review of the most common threats, as well as an overview of how both open source technologies such as Snort and ClamAV play a role in protecting enterprise environments. Enterprise security administrators and architects, CISOs and even CIOs will also benefit from learning about advanced malware protection and network security platform approaches that protect their environments across the attack continuum - before, during and after an attack. **Mr. Amitpal Singh Dhillon** **Senior Evangelist, APAC** **Sourcefire**

15:20 –15:50	**Keynote 7: Data Center Security – The Third Pillar Of Enterprise Security**
	The threat landscape has changed dramatically in the past decade, from pranksters to extremely sophisticated operations. Yet security spending is not keeping pace with today's modern threats. While endpoint and network security solutions are the first and second pillars of enterprise security, you cannot conduct business safely without the third pillar – data center security. This session will introduce Imperva SecureSphere comprehensive, integrated security solutions for the data service, enabling your organization to safely realize the benefits of the hyper-connected world.
	Mr. David Chou **North Asia Technical Director** **Imperva**
15:50 –16:20	**Keynote 8: Future Shock: How Distributed Enterprises Should Completely Rethink Security**
	No single change in enterprise computing will have a greater impact on end-user security than the rapid dissolution of the enterprise perimeter. Users are increasingly working in very distributed environment which is built up by a lot of small branch offices and laptop globally. Despite this fact, the majority of enterprises continue to employ traditional security solutions that rely on appliances or host based software - solutions that cannot consistently outside the corporate network. Enterprises need to completely rethink their approach to end user security in this new paradigm.
	Mr. Dolsen Lee **Technical Director, APAC** **Zscaler**
16:20 –16:30	**Afternoon Networking Coffee Break and Showcase Tour**
16:30 –17:00	**Keynote 9: Compliance Does Not Equal Security**
	Recent breaches like the ones at Target and South Korean banks have proven that simply passing a PCI audit doesn't mean customer data cannot be compromised. Being compliant is important, but it's not enough to mitigate probable attacks and protect critical information. Organizations need to focus on securing the business first, then documenting the process to prove compliance, not the other way around.

Information as of March 25, 2014

	In order for organizations to move from a compliance-focused to a risk-focused security program, they need to think like an attacker (not an auditor) and understand the threat landscape. Today's attacker is opportunistic, meaning the victim was targeted because they exhibited a weakness that the attacker knew how to exploit. This reality, combined with a disappearing perimeter – desktops, laptops, tablets and mobile devices all have access to the internet and are potentially introducing threats into your network – means attackers are taking advantage of your weakest links: the user. **Mr. Philippe Alcoy** **Technical Director, APAC** **Rapid 7**
17:00 –17:30	**Panel Discussion Three: Formulating A Comprehensive IT Risk Management Strategic Road Maps For 2014 And Beyond** **Panel Chair:** Ms. Eva Kwok, Director, Enterprise Risk Services, Deloitte **Executive Panelists:** • Mr. Micky Lo, Head of Information Risk Management, APAC, BNY Mellon • Mr. Daniel Cheung, Head of IT Security & Risk, IT Change & Control, Daiwa Capital Markets • Mr. Ricky Tang, Head of Information Security & Risk Control, Fubon Bank • Mr. Calvin Lam, Director of Information Security, Shangri-La International Hotel Management
17:30	**End of Conference**