~ Joint ASIS International (Hong Kong) Chapter

& OSAC Hong Kong Country Council ~

Bring Your Own Device (BYOD) & The Challenges in the Corporate Environment

Date: 7th June 2013

Sessions: Details as enclosed

Schedule: Start time in Macau from 13:45 hrs to 17:45 hrs (with coffee breaks)

Evening Schedule: 18:00 hrs, Poolside Cocktails and BBQ at the Sands Casino Hotel

Costs: Per Person **HK$600 (for ASIS & OSAC members), HK$675 (for non-members) (Does not include travel)**

Ferry Arrangements: Individual basis

Booking Form: As attached

Payment: ***Payment in full is required in advance***. *(If you book and don't show, you will still be charged in full).*

Contact Details: ASIS / OSAC members: Mr. Daniel Chui: email: daniel_chui@bat.com Cell: +852 9468 3445

Venue: Sessions will be held at **"Reflections" on the 6th Floor Sands Casino, Macau** (entrance via hotel main entrance)

Travel arrangements: Ferries leave HK Island (Shun Tak Centre) and Kowloon (China Ferry Terminal) every 30-40 minutes**,** details available at http://www.nwff.com.hk/ or http://www.turbojet.com.hk/eng/schedule/prd.html

Hotel: A special offer for a room at the Sands Hotel is also available and requires pre-booking. Please contact Daniel directly to follow up.

Reminder: You will require your HK Permanent ID Card or a Valid Passport

Language: English

Reservations: Please book and pay no later than **5th June 2013** using the booking form below

Remarks: Reservations are based on a *first come first served;* spaces are limited.

CPE Points: **3 CPE Credit. Notification of your attendance will be provided directly to ASIS International PCB**

Note: *If the event has to be rescheduled, due to unforeseen circumstances beyond our control, you will be informed 24 hrs in advance via e-mail.*

Conference Overview

The conference will highlight the challenges facing the corporate environment relating to Bring Your Own Device (BYOD). Also called bring your own technology (BYOT), bring your own phone (BYOP), and bring your own PC (BYOP) and relates to permitting employees to bring personally owned mobile devices (laptops, tablets, and smart phones) to their workplace and use those devices to access privileged company information and applications. The term is also used to describe the same practice applied to students using personally owned devices in education settings.

BYOD evolved in 2009 and is making significant in-roads in the business world, with about 44% of employees in developed markets already using their own technology at work. In most cases, businesses simply can't block the trend. Some believe that BYOD may help employees be more productive. Others say it increases employee morale and convenience by using their own devices and makes the company look like a flexible and attractive employer. International research reveals that only 20% of employees have signed a BYOD policy agreement with employers. BYOD has resulted in data breaches, the presence of proprietary applications and other data on devices; and BYOD's challenging relationship within an increasing 'Cloud' environment.

With benefits such as greater innovation, better work-life balance and improved productivity, it also increases pressure on corporate security IT to manage and secure devices and data. So what are the issues facing you with BYOD?

With such risks in mind, the Hong Kong and Macau Chapters of the United States Overseas Security Advisory Council (OSAC) and ASIS International are pleased to bring together leading industry security experts—Alen Lo, John Lin, Alan Jeffries and Phil Russo—to present practical methods and contexts in which organizations may manage and respond to such risks and security threats.

Topic	Speaker
Opening Address (1345 hours)	**Mr Mark Lewis, Regional Security Officer, U.S. Consulate General Hong Kong.**
Session 1 (1400-1445 hours): Over $250 million was stolen by the members of the "Eurograbber" botnet ring from internet users worldwide. **John will highlight the vulnerabilities and solutions to prevent organised crime and rouge employees from accessing privileged information, customer accounts and secured data.**	**John Lin** **John** is Chairman of OminBud Inc. and 2udg Inc. Since 2003 he has been leading his teams in developing communication and cloud operating environment security, also devising user authentication solutions to combat criminal activity by means of PKI, One-time Password (OTP), Cloud and the latest mobile / telecommunicatio applications. His companies hold a number of patents and awards, in 20 countries, relating to reversed sound and active OTP (AOTP) technology. **John** was recently invited to present at the 8th International Conference on Grid and Pervasive Computing (GPC 2013) and previously at the IEEE International Carnahan Conference on Security Technology (ICCST).
Session 2 (1445-1530 hours): Digital Forensic and Social Media Investigations. **Intellectual property theft, industrial espionage, hacking, blackmail via anonymous email & marriage asset investigations.**	**Phill Russo** **Phill** is an IT Forensic Expert based in Australia and providing investigation and litigation support services worldwide through his company, CIA Solutions. He is often called upon by investigators and law firms alike, where intelligence or evidence may be obtained via electronic devices including computers, smartphones or using the internet to identify anonymous email authors etc. He will also speak on why you should engage a forensic expert rather than just using an IT person within any such investigation. At the conclusion of his presentation he will open the floor to any "on the spot questions" and offer advice pertaining within his speciality of "Digital Forensic and Social Media Investigation." As a Cert IV qualified Instructor with experience instructing leading forensic companies (Access Data (FTK), Encase Guidance Software, and Perlustro), Phillip provides state of the art forensic instruction.

Session 3 (1600-1645 hours): BYOD: Personal and Professional use of Mobile Devices, Securing the Cloud Data Forensics.	**Alan Jeffries** **Alan** (AJ) provides Technical Surveillance Counter Measure Audits, I.T. Security Consulting, Digital Forensic Investigations and eDiscovery for corporate clients across the Asia Pacific region. Alan served in the British Army (Royal Corps of Signals) for 12 years prior to taking up employment with a leading risk mitigation company in Hong Kong as their in-house Technical Surveillance Counter Measures (TSCM) practitioner. He is recognised as a leading consultant in the fields of TSCM, Digital Forensic Investigations and eDiscovery, as well as mobile device forensics. A Certified TSCM practitioner, Certified Information Systems Security Professional (CISSP), and a qualified digital forensics examiner holding EnCase Certified Engineer (EnCe). Industry professional memberships include The American Society for Industrial Security (ASIS); International Information Systems Security Certification Consortium, Inc (ISC)2. High Technology Crime International Association (HTCIA) Founding President (2005, 2006, 2007).
Session 4 (1645-1730 hours): N2N Security – BYOD a Technical Focus.	**Alen Lo** **Alen** is the Principal Consultant at i-Total Security Consulting Ltd. He holds a M.B.A. from The Chinese University of Hong Kong and a B.Sc.(Hons.) from The University of Hong Kong. He is a Certified Information Systems Auditor (CISA), a Certified Information Systems Security Professional (CISSP), a Certified Information Security Manager (CISM), a Certified Ethical Hacker (CEH), an IRCA Certified ISMS Lead Auditor, and an itSMF ISO 20000 Auditor. Alen has over 14 years of solid experiences on information systems security, control and audit. During this period, he has been developing, implementing and assessing information systems security and controls for various financial institutions, government departments, telecommunications carriers, utilities companies, non-government organizations, academic institutions, manufacturing companies and trading conglomerates in Australia, Canada, China, Hong Kong, Korea, Indonesia, Japan, Korea, Macau, Mongolia, New Zealand, Pakistan, Saudi Arabia, Singapore, Spain, Taiwan, Thailand and United Arabic Emirates.
Closing Address (1745 hours)	**Mr Daniel Chui: ASIS International (Hong Kong) Chapter Chairman**

Booking Form

Fax to :- + 852 2893 6890

email to: peter.makant@aia.com

Topic: ***Bring Your Own Device (BYOD) & The Challenges in the Corporate Environment***

To: ASIS International HK Chapter

☐ I/ We shall attend the Joint ASIS (HK) Chapter and OSAC Country Council meeting in Macau on **7th June 2013** please find attached payment of HK $ _____

1) Bank Transfer

- **HSBC Account No.** 162-037352-001
- **Account Payee:** ASIS Hong Kong Chapter

2) Cheque Payment

- **Cheque payments to:** ASIS HONG KONG CHAPTER
- **Cheque to be posted to:** ASIS International. c/o Peter Makant, AVP, AIA Group Corporate Security, LG1 AIA Building, 1 Stubbs Road, Wanchai , Hong Kong

*Please send booking form along with soft copy of bank pay-in or transfer slip by fax or e-mail.
If paying by cheque please send cheque and booking form to Peter Makant (as above)

Receipt required: Yes ☐ No ☐ **CPE Points to be claimed** Yes ☐ No ☐

(softcopy receipt issued after the event)

Names of Participants	Contact e-mail address	ASIS International Membership Number
1)		
2)		
3)		
4)		
5)		

www.asis.org.hk
http://hongkong.osac.gov/