

Mobility Forum 2014

Staying Ahead of the IT Security Landscape

Forum: 2 - 3 September 2014

Post Forum Workshops: 4 September 2014

Location: Raffles Dubai, UAE



Speakers' Interview

Mobility Forum 2014 speaks to some selected thought leaders who will be sharing their expertise at the forum this September in Dubai. Hear their perspectives on the latest trends and technologies.



IT Security Threat Landscape of 2015

Anil Prakash the Director General of India Security Council for ICT & Telecom spoke with us and shared his vision on the threat landscape of 2015. Get an insight on ITU's initiatives on the security challenges. Anil will be delivering the keynote address on The Mobile Security Landscape on 2nd September 2014.

1. What are your concerns on the current threat landscape?

- Reflecting on the security and threat landscape of 2013, one trend that stands out is the growing ability of malware authors to camouflage their attacks. Widespread dissemination of advanced botnet and exploit kit source code allows more malware authors to create innovative and diverse new attacks thus make it more lethal.

Cybercriminals have started to leverage online marketing as a way to promote and sell their services on the black market. In 2012, the Black Hole exploit kit broke new ground. But in 2013, Black Hole was replaced by several new exploit kits that grew out of it, borrowing some of its code. The resulting botnets are responsible for a sharp increase in ransomware attacks, with Cryptolocker being the prime malice. Modern malware is all about stealth. Advanced Persistent Threats (APTs), are one of the most vicious examples of a stealth threat, precisely target individuals, businesses, governments and their data. APTs are a sophisticated weapon to carry out targeted missions in cyber space.

2. What are ITU's initiatives on battling with security challenges?

Security is now widely recognized as critical importance to the future of electronic communications and operations. Without effective security, all systems and processes that rely on electronic communications are at risk and, as a consequence, large numbers of resources are now devoted to countering threats, protecting systems and recovering from successful attacks.

It has long been recognized that security is much more effective if it is designed into systems, rather than added on afterwards. It is also the case that, even systems that are well-designed from a security standpoint, relies on human operators that have some understanding of the threat environment and of the local policy requirements. ITU-T has initiated steps to address security issues pro-actively within its own Study Groups and also collaborates with other standardization bodies to battle with security challenges.

3. Tell us more about ITU's Global Cybersecurity Agenda's (GCA)

In response to its mandate as sole Facilitator of WSIS Action Line C5, the ITU Secretary-General, Dr. Hamadoun I. Touré, launched the Global Cybersecurity Agenda (GCA) on 17 May 2007 as a framework for international cooperation to promote cybersecurity and enhance confidence and security in the Information and Communication Technologies (ICT) industry. The GCA seeks to encourage collaboration amongst all relevant partners in building confidence and security in the use of Information and Communication Technologies. The GCA has benefited from the advice of an expert panel, the High-Level Experts Group (HLEG), on the complex issues surrounding cybersecurity. The HLEG is a group of specialists in cybersecurity, comprising more than one hundred experts from a broad range of backgrounds in policy-making, government, academia and the private sector.

Cybersecurity is one of the most profound challenges of our time. The rapid growth of ICT networks has created new opportunities for criminals to exploit online vulnerabilities and attack countries' critical infrastructure. Governments, firms and individuals are increasingly reliant on the information stored and transmitted over advanced communication networks. The costs associated with cyber attacks are significant – in terms of lost revenue, loss of sensitive data, damage to equipment, denial-of-service attacks and network outages. The future growth and potential of the online information society are in danger from growing cyber threats. Furthermore, cyberspace is borderless: cyber attacks can inflict immeasurable damage in different countries in a matter of minutes. Cyber threats are a global problem and they need a global solution, involving all stakeholders.

4. Your vision for 2015 - Security is no longer a "nice to have," but a must-have!

Advanced Persistent Threats (APT) attacks in 2013 were well-planned and well-funded; carried out by highly-motivated, technologically advanced, and skilled adversaries. Even after successfully accomplishing the mission, the APT continues to live on to gather additional information. Defending against the stealthy and persistent nature of APTs is a complex undertaking, and requires a coordinated approach on the systems as well as the network level. Businesses and governments rightfully concerned about privacy and protecting sensitive data now have to be more aware of troublesome security issues that could be found in critical infrastructure systems.

Incidents of attacks on these critical network infrastructure and control systems demonstrate vulnerabilities in the essential infrastructure of our society. Systems including the smart grid infrastructure could become more of a focus for cybercriminals in the coming year. The growing popularity of the "Internet of Things" (e.g., mobile devices, applications, social networks, and interconnected gadgets and devices) makes the threat landscape a moving target.

New threats arise with emerging technologies such as Near Field Communications (NFC) being integrated into mobile platforms. Innovative uses of GPS services to connect our digital and physical lives present new opportunities for cybercriminals to compromise our security and privacy. Such systems could yield attacks that have a very personal impact on each of us. In 2015 we need to start watching not just the evolution of existing attacks, but new types emerging that we haven't previously dealt with. A whole heart approach is needed by all stake holders like the Government, Computer Emergency and Response Team (CERT) and Companies to counter the security threat for a safe living world.

5. Please share your thoughts on how to minimise risk in this mobile era

The invention of the iPhone and subsequent rise of the smartphone era has added a whole new wrinkle to our increasingly digital society. Not only can we share the details of our lives on social media platforms like Facebook and Instagram, or pay our bills quickly and easily through online banking, but we can also have all of these of functions performed right in the palm of our hand. Unfortunately, the ease that comes with living or working off of our smartphones and tablets makes it that much easier for hackers to commit **ID theft**.

So how can businesses strike a balance between keeping their networks and data safe while empowering their employees? The key is security, and to get there, managers must thoroughly understand where they're falling short.

Here are four ways to evaluate your business's risks and vulnerabilities to mobile malware:

- **Audit Your Mobile Operating Systems**
- **Implement a Mobile Security Policy**
- **Practice Good [Security] Hygiene**
- **Adopt a Mobile Device Management (MDM) Strategy**

All of these tools are part of a comprehensive governing strategy known as mobile device management (MDM). Think of it like overall physical health: if security policy and hygiene are the equivalent of working out and eating healthy, MDM encompasses total wellness, including diet, exercise, preventative care, doctor visits and everything else you do to stay healthy.

Anil will be delivering the keynote address on The Mobile Security Landscape on the 2nd of September 2014. Register now and Seize the opportunity to meet up with Anil.



Cloud forecast for MENA

Andrew Grenville the Chief Executive Officer of Orixcom spoke to us and shared his thoughts on how using the cloud for delivery of services is an unstoppable and growing trend for very good reasons, and is revolutionising the market and opportunity. Whilst it's not suitable for all IT services and applications, and varies across sectors, we all need to embrace change and ride the wave, not try to resist it with old style business models. **Get with it or get left behind!** Andrew will be delivering the keynote address on **'Are you ready to embrace the Cloud?'** on 3rd September 2014.

1. With the increase of cloud adoption, what are some of the main road blocks faced by service providers?

Transparency and clarity – This represents a challenge for cloud service providers. Customers need to be able to easily understand, evaluate and compare the services that a potential service provider offers. There is a lot of confusing and conflicting information out there – often driven by the supplier's own agenda rather than the customer's own needs.

Security - There has been a perception that cloud and its delivery is unproven however this model has been around the IT industry in varying forms for 30 years. Technology has simply advanced to the point of making it easier to deliver. However customers need to ask tough questions about physical and electronic security, privacy, cloud provider policy etc.

Data Sovereignty – This has become a critical area in the adoption of cloud especially since the publicity around the Snowden revelations in 2013. Customers want to know where their data is physically held, how it is protected, who has access to their data and how they can get it back. Does it meet the laws, regulations or licence conditions of their industry or country?

Interoperability and openness – Many cloud systems need to connect to other cloud or non-cloud applications, as well as existing on-premise resources in a quick and cost effective way. Are you getting tied into your cloud provider or do they operate with open principles?

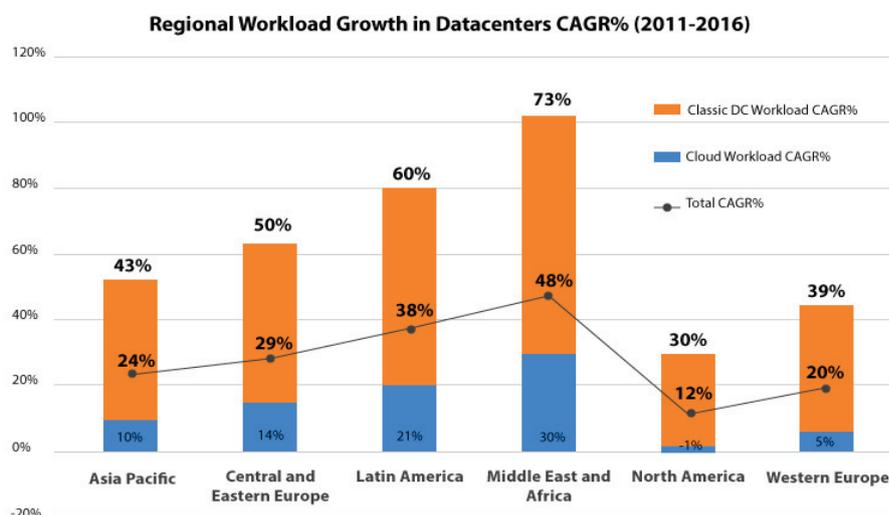
Cost – The cloud is cost effective, or at least that's what it's supposed to be. Are all the customer charges very clear and scalable or will they encounter hidden costs to trip you up? Cloud is meant to be a consumption based approach of delivering resources, make sure this is the case.

2. What is the cloud forecast for MENA?

The cloud forecast for MENA is extremely strong and healthy, both public and private. For workloads in public datacentres there is a massive 73% CAGR 2011-2016 according to Cisco Global cloud index (see graph below). Similarly Gartner predicts that from 2013 through 2017, \$3.8 billion will be spent on cloud services in MENA region and they predict IT spending on public cloud services in the region is expected to reach **\$1.1 billion in 2017**, up from an estimated \$511 million in 2013.

There are many drivers such as lack of traditional IT infrastructure, large SME growth with government support, strong GDP growth, trend towards opex vs capex.

Cloud is widely accepted and recognised as a key enabler that will support and transform the development of the MENA region - allowing everyone to access world-class cloud technology that is both powerful and affordable.



Cisco Global Cloud Index 2013

Source: Adapted from Cisco

3. Security challenges with the adoption of cloud

One of the biggest concerns around cloud that customers have is of data security and privacy. Security is the biggest pain point and roadblock to cloud computing adoption with 78% of those surveyed in the UAE by Orixcom citing it as a key factor in deciding which location and provider they would choose for their cloud services.

Ironically for a lot of enterprises, particularly the small to medium sized enterprises (SME) it is difficult to deliver best security practices in house, so using an external specialist can bring great benefits in security and is often much more secure than traditional IT infrastructure.

4. How can enterprises and service providers monetise on the cloud?

Enterprises and service providers can monetise on the cloud by extending and scaling the adoption of cloud services across industries, verticals, segments and even countries. It enables them to leverage the power of the cloud and embrace the opportunity to bring applications, services and products to new customers both large and small. Taking advantage of cloud technology they can provide world-class and affordable services to an untapped mass market that is hungry to start using cloud services to positively transform their lives.

Andrew will be delivering the keynote address on **'Are you ready to embrace the Cloud?'** on the 3rd of September 2014. Register now and seize the opportunity to discuss your cloud needs with Andrew.



Is Cloud Driving Mobile Growth?

Arun Tewary the VP (IT) & CIO for Emirates Flight Catering spoke with us and shared his thoughts on the Cloud. Arun will be delivering the Visionary Keynote address on **Impact of Technology on Society and Corporate** on the 3rd of September 2014.

1. Is cloud driving mobile growth or is mobile driving the growth of the cloud?

It is complimentary – both are exponentially accelerating each other's growth. Though there are no dependencies – both are growing independently.

2. The coming of the 3rd platform and what it means to the cloud business

3rd Platform is making cloud business one of the most revolutionary and dominating business segment.

3. What are the dangerous gaps in enterprise security?

The gaps are due to the lack of security awareness and changing security landscape with the ever changing speed of technology (mobile / cloud / social network computing).

4. How do you implement security measures in Emirates Flight Catering?

We have implemented policies compatible with 27001 and the security awareness program. I ensure that there is continuous monitoring of the network. We are always adapting and keeping up to date with changing technologies and are constantly building security measures around it.

5. What are the security challenges you foresee in 2015?

I would think the main challenges will be:

- Managing security while using cloud computing solutions
- Building security measures to accommodate mobile computing
- Security for unstructured data

Arun will be delivering the Visionary Keynote address on the **Impact of Technology on Society and Corporate** on the 3rd of September 2014. Register now and seize the opportunity to exchange ideas and solutions with Arun.



Mobile Forensics

Asif Iqbal the Fraud and Security Investigator and Founder of **Athena Labs** spoke with us and shared his thoughts on **Mobile Forensics**. Hear him discuss the challenges facing mobile Digital Forensics (DF) investigators. Asif will be presenting on **'Mobile Governance (mGov): Extending the Government to Everyone, AnyTime, AnyWhere'** on the 3rd of September 2014. Asif will also be conducting an interactive and hands on workshop on **Mobile Device Digital Forensic Investigation** on the 4th of September 2014.

1. What is computer forensics used for?

Computer forensics, a branch of digital forensics is science that is concerned with the collection, preservation and analysis of digital evidence from a computer system. These actions are done with the aim of providing evidence that is admissible in a court of law.

It can be used in different categories such as:

- Criminal investigation
- Domestic cases
- Corporate internal investigation

In the case of criminal investigation computer forensics can be used to prove if a crime was committed.

Evidence retrieved from emails, chat room transcripts, instant messaging, photographs and other digital evidence can be used to prove infidelity and abuse.

In the case of corporate internal investigation; computer forensics can be used to help investigate cases such as:

- Intellectual Property theft
- Industrial espionage
- Employment disputes
- Fraud investigations
- Forgeries
- Bankruptcy investigations
- Inappropriate email and internet use in the work place
- Regulatory compliance

2. Challenges facing mobile Digital Forensics (DF) investigators?

Mobile device forensics poses additional challenges to investigators because of the following reasons:

- There is huge diversity in the mobile hardware, so a lot of new models are coming out with newer hardware
- Along with hardware changes, software changes are also an ever increasing issue in mobile device forensics
- Regular updates to the mobile software creates an additional layer of challenge
- A huge number of different platform, demands an ever increasing skill set for forensic investigations

All of the above combined with short product cycles in mobility; prove mobile forensics to be a great challenge.

3. The importance of DF in today's era?

We are living in a Digital Age. Technology related crimes have increased tremendously and digital forensics provides crucial evidence to prosecute the culprits. Be it law enforcement at state level, or auditing or the investigations department, digital forensics forms an integral part of an investigation team.

4. Who uses IT forensics in the Middle East?

Users of IT forensics in the Middle East involve legal entities such as the police, military and government agencies in general. Large corporations are also using Digital Forensics to a great extent in recent times.

Asif will be presenting on **'Mobile Governance (mGov): Extending the Government to Everyone, AnyTime, AnyWhere'** on the 3rd of September 2014. Asif will also be conducting an interactive and hands on workshop on **Mobile Device Digital Forensic Investigation** on the 4th of September 2014. Register now and seize the opportunity to discuss your mobile forensic challenges with Asif.



Why is it important to have a MAM strategy in place?

Grant Allen, Technology Program Manager, Principal Architect, **Google** spoke with us and shared his thoughts on why it is necessary to have a MAM strategy in place. Grant will be presenting on **'Android Wear - Getting security right when developing for the wearable Android world'** on the 2nd of September 2014.

1. What are the dangerous gaps in enterprise security?

I think one aspect that deserves more attention is the nature of an enterprise itself in the context of approaching security. As we've seen with the huge and rapid adoption of mobile, BYOD and more, historic notions of what an enterprise is, and therefore what needs security attention, can change very quickly. This is where the more sophisticated security strategies help deal with the ever-changing security landscape.

2. Why is it important to have a MAM strategy in place?

In a nutshell, the right MAM strategy provides guidance, certainty and adaptability in the face of the unprecedented growth and diversity of apps in the enterprise, and the almost daily challenges to the enterprises when employees, customers, suppliers and partners adopt and use new mobile applications. One really doesn't want an ad-hoc or random process when assessing each new application. A good MAM strategy provides the consistency to know security policies and principles are being addressed.

3. What keeps you up at night?

In a positive way, I think about how to make good security practices easy for developers and users alike. In a perfect world, the best security approaches should also be the easiest with which to develop mobile applications, and the most intuitive to all the world's users.

4. Your vision for 2015

We've just passed 1 billion Android devices in the wild. My vision for 2015 would be the next 1 billion Android users enjoying the benefits of great apps from developers who've made good security the norm.

Grant will be presenting on **'Android Wear - Getting security right when developing for the wearable Android world'** on the 2nd of September 2014. Register now and seize the opportunity to discuss your Android challenges with Grant



Mobility Forum 2014

Staying Ahead of the IT Security Landscape

Forum: 2 - 3 September 2014

Post Forum Workshops: 4 September 2014

Location: Raffles Dubai, UAE

Limited Time Special!
Register by 12 Aug &
Save up to
US\$400

Hear from Senior Leaders from Major Companies Including Google, BlackBerry, IBM and Microsoft

Bringing IT Security Professionals from across the Globe Together

NOT TO BE MISSED

- Innovation showcase - **Faceoff: Android vs iOS**
- **2 highly interactive hands-on workshops on Live Hacking and Mobile Device Digital Forensic Investigation**
- **Power Breakfast on Day 1** – Speed Networking - Get introduced to peers and potential business partners
- **Nephophobia?** Understand how to avoid the 'toxic' cloud

FORUM SPEAKERS HIGHLIGHT - 2ND & 3RD SEPTEMBER 2014



Nader Henein
Regional Director,
Advanced Security
Solutions – Advisory
Division
BlackBerry



Arun Tewary
VP (IT) & CIO
Emirates Flight Catering



Grant Allen
Technology Program
Manager, Principal
Architect
Google



Girish Dhanakshirur
STSM, Master Inventor
IBM Mobile Foundation



Ajay Rathi
Head of IT
Meraas Holding



Anil Prakash
Director General
India Security Council
for ICT & Telecom



Justin Prince
Mobility Consultant
Technical Art Concepts
(TACME)



Haider Pasha
CTO & Head of Technical
Sales and Services
Symantec

POST FORUM WORKSHOP LEADERS - 4TH SEPTEMBER 2014

Workshop A: Mobile Security – Live Hacking Workshop



Tudor Enache
Principal Security Consultant
Help AG

Workshop B: Mobile Device Digital Forensic Investigation



Asif Iqbal
Digital Forensics, Fraud
and Security Investigator &
Founder
Athena Labs

Nephophobia – Analyse Your Fear of Clouds

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

SPEAKERS LINE-UP



Ilyas Kooliyankal
Director -
Information Security
(CISO)
**ADS Securities &
ADS Holding**



Girish Dhanakshirur
STSM, Master
Inventor
**IBM Mobile
Foundation**



Stewart White
Chief Executive
Officer
Akhet Consulting



Anil Prakash
Director General
**India Security
Council for ICT &
Telecom**



Asif Iqbal
Digital Forensics,
Fraud and Security
Investigator &
Founder
Athena Labs



Ajay Rathi
Head of IT
Meraas Holding



Nader Henein
Regional Director,
Advanced Security
Solutions – Advisory
Division
BlackBerry



Corbett Hoxland
Solutions Specialist
Mobility
Microsoft Gulf



Shah Sheikh
Co-Founder &
Security Solutions
Consultant
DTS Solution



Omid Mahboubi
Co-founder
**Middle East North
Africa Cloud Alliance
(MENACA)**



Vivek Srivastava
Senior Manager
– Global Product
Development
du



Andrew Grenville
Chief Executive
Officer
Orixcom



Arun Tewary
VP (IT) & CIO
**Emirates Flight
Catering**



**Muhammad Noman
Usman**
Network Manager
**Public Authority for
Consumer Protection,
Sultanate of Oman**



Grant Allen
Technology Program
Manager, Principal
Architect
Google



Haider Pasha
CTO & Head of
Technical Sales and
Services
Symantec



Tudor Enache
Principal Security
Consultant
Help AG



Justin Prince
Mobility Consultant
**Technical Art
Concepts (TACME)**

AGENDA AT A GLANCE

Day One – 2nd September 2014:

- Creating Business Driven Mobile Device Management (MDM) Strategies
- The World of BYOD – How Mobility can Transform your Business
- In a Hacker's World – Get updated on the different types of hackers and find out if you potentially can be the next victim!
- Technology Enabled Crimes – Be a Step Ahead

Day Two – 3rd September 2014:

- Mobile Application Management (MAM) – Take your Enterprise Mobile
- How Secure is your Cloud? Is Cloud Security just Hype or is it a Real Threat?
- XaaS – Know how to Select the Right Cloud

WHO WILL YOU MEET

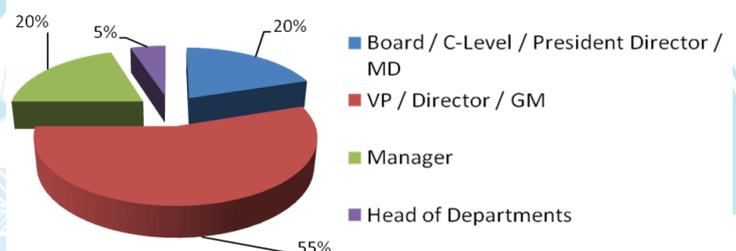
IT Professionals:

- Chief Technology Officers (CTO)
- Chief Security Officers (CSO)
- Chief Information Officers (CIO)
- IT Architects
- Forensic Analysts
- Security Architects
- Cyber Risk Managers
- Security Analysts
- Enterprise Architects
- Application Development
- Infrastructure and Operations
- Sourcing and Vendor Management
- Technology Product Management

VP, Directors & Heads of:

- Enterprise Mobility
- Service Platforms
- Cloud Services
- Application Development
- IT Departments

Seniority Level: 75% of Participants will be Director Levels & Above



Official
Media
Partner:



Supporting
Partner:



How to Ensure You are 1 Step Ahead of the Hacker?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

OVERVIEW - FROM THE MOBILITY FORUM TEAM

The **Mobility Forum 2014**, an inaugural event is a global gathering of leading security experts in Dubai.

Analysts predict that attacks will continue to become more innovative and sophisticated over the years. Unfortunately, while organizations are in the midst of developing new security mechanisms, cyber criminals are cultivating newer and smarter techniques to circumvent them. Can we ever be ahead of them?

Bring your own device (BYOD) trends in the workplace, data privacy in the cloud, privacy and regulation, cyber crime and the continued expansion and innovation of technology are the main security threats organizations are facing.

The evolution of technology is showing no signs of slowing down. Devices are becoming more efficient and employees are increasingly relying on their smart devices to conduct both corporate and personal business, moving IT security to the top of the agenda. CIOs are faced with the challenge of controlling security breaches of mobile devices which is complex due to the varying software and device types. Mobile platforms are very efficient to cater to the needs of the consumer but are slow in meeting enterprise requirements.

This forum aims to discuss the top IT security threats for 2015. From mobile applications to malicious website hacks to how to keep your cloud safe, this forum will highlight the challenges facing IT professionals and what keeps them up at night. Hear industry practitioners share their knowledge and expertise on the solutions that they have used to solve security threats they have faced.

Attend the **Mobility Forum 2014** and be where the security experts from around the globe will gather!

Book Your Seat Today!

Email: admissions@claridenglobal.com

or Call +65 6899 5030 (SG) / +44 (0) 20 7129 1222 (UK) today for immediate booking.

10 Reasons to Join us this September in Dubai:



Are you ready to Embrace the Cloud?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

FORUM AGENDA

DAY ONE - 2ND SEPTEMBER 2014, TUESDAY

09:00 **WELCOME NOTE**

09:05 **WELCOME ADDRESS BY CHAIRMAN**

Stewart White
Chief Executive Officer
Akhet Consulting

Stewart is a regulatory lawyer by background with more than 30 years of experience. He has worked in many jurisdictions in developed and developing countries advising both the public and private sectors in fixed, mobile and satellite.



09:20 **KEYNOTE ADDRESS: THE MOBILE SECURITY LANDSCAPE**

- Roadmap for the next 5 years
- Threat reports
- Pain points of CTOs
- Current threat landscape and counter measures

Anil Prakash
Director General
India Security Council for ICT & Telecom

With over 34 years of experience in the ICT industry Anil's work with International Telecommunications Union (ITU) has allowed him to play an influential role in contributing towards ITU's activities. Anil's intervention has led to path breaking policies by the Indian government such as national telecom policies and telecom cyber security policy.



10:05 **FUTURE TENSE – PRIVACY AND SECURITY IN MOBILITY**

- Mobile Security – what's the latest?
- Vulnerabilities and behavior that will shape tomorrow's breaches
- The state of mobile privacy, what's the price of FREE
- Laws and regulations coming to a legislature near you

Nader Henein
Regional Director, Advanced Security Solutions – Advisory Division
BlackBerry

Nader brings over two decades of tactical experience in the architecture, development and management of secure, scalable systems. Today, his role hinges on providing solutions to current challenges faced by BlackBerry's strategic customers in banking, governance, security and beyond.



10:35 **NETWORKING MORNING BREAK- POWER BREAKFAST**
SPEED NETWORKING SESSION – GET INTRODUCED TO PEERS AND POTENTIAL BUSINESS PARTNERS

11:20 **NEXT-GENERATION MOBILE SECURITY GATEWAYS FOR 3G & 4G NETWORKS**

- Security threats with the growing mobile demand
- New security threat vectors that are impacting the mobile network
- Layer 2 and Layer 3 MPLS security designing
- New security risks presented by the new Long Term Evolution (LTE) architecture
- VLAN design for a secure LAN

Muhammad Noman Usman
Network Manager
Public Authority for Consumer Protection, Sultanate of Oman

Muhammad Noman is an engineer with over 10 years of experience in O&M IP/MPLS core network, system configuration, monitoring, implementation & designing with 24x7 uptime. He leads the technical teams of IT network for day to day operations, monitors, enhances and presents the KPI's & SLA for the challenges faced.



Limited Time Special! Register by **12 August** & Save up to **US\$400**

What Keeps CIOs up at Night?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

FORUM AGENDA

CREATING BUSINESS DRIVEN MOBILE DEVICE MANAGEMENT (MDM) STRATEGIES

MDM is still in its infant stages. Many organizations do not seem to understand the need for MDM to be in place before encouraging BYOD. Analysts predict that by 2017 half of employers will not be required to supply devices to the employees. Enterprises would need to look into innovative programs that are not only meant for organizations. With more and more employees bringing in their own devices there is an urgent need to incorporate a MDM strategy.



11:50 BYOD - HOW TO MAKE IT WORK? DEVELOPING A SUCCESSFUL INITIATIVE

- How to initiate a BYOD process securely
- How to develop a secure MDM policy
- A look at the security policies and logistics involved

Illyas Kooliyankal
Director - Information Security (CISO)
ADS Securities & ADS Holding

Illyas brings with him more than 17 years of experience in the Information Technology and Cyber Security arena. He is a strategic thinker, who brings, out of the box and proactive initiatives towards protection of the organization and its assets, Illyas has developed and implemented effective information security management system for telecom and finance sectors.



12:20 NETWORKING LUNCH BREAK

THE WORLD OF BYOD – HOW MOBILITY CAN TRANSFORM YOUR BUSINESS

It is essential for IT professionals to be proactive and understand what the employees would like to use and find ways on how to make that possible. IT professionals have to embrace consumerization and look at strategic approaches, built around policies and management tools. One size does not fit all so policies need to be flexible and fluid to allow changes. Corporate IT has to change its mindset to better embrace mobility. This session will equip you with the right methodologies needed to implement BYOD, an in-depth look into the cost and benefits of BYOD.

13:30 CASE STUDY BY GOOGLE: ANDROID WEAR - GETTING SECURITY RIGHT WHEN DEVELOPING FOR THE WEARABLE ANDROID WORLD

- The Android security model
- New security considerations for Wearables
- The right security framework and approach for Wearables application developers
- Incorporating Wearables into an enterprise's MAM framework, what to look for, and what to avoid
- Google Play Services in your mobile application management strategy for Wearables

Grant Allen
Technology Program Manager, Principal Architect
Google

Grant has worked in the IT field for over 20 years, as a CTO, entrepreneur, enterprise architect, and data management expert. He is a frequent speaker on topics such as disruptive innovation, and mobile ecosystems like Android. Grant is the author of six books on mobile development with Android, and data management.



14:15 MOBILE FIRST – WHY CORPORATIONS ARE EMBRACING ENTERPRISE MOBILITY

- What corporations can achieve by embracing a Mobile First approach
- How personal devices and Bring your own device (BYOD) strategies are affecting the workplace
- Biggest mobile trends
- Business apps are here to stay

Justin Prince
Mobility Consultant
Technical Art Concepts (TACME)

Justin Prince, PMP is a mobility consultant and subject matter expert in the field of Enterprise Mobility Smart Government initiatives. Justin advises his customers on the latest trends in Mobility Solutions such as Business Apps, Enterprise Mobility Management and why corporations must embrace a Mobile-First approach.



14:45 ENTERPRISE MOBILITY, THE GOOD, THE BAD AND COST OF DOING NOTHING

- How can the enterprise mobilize their workforce
- What are the benefits of the modern mobile workforce
- What are we going to do about this Bring Your Own Device (BYOD) movement we are seeing
- Enabling mobility across the enterprise - The costs involved and more importantly, the cost of doing nothing

Corbett Hoxland
Solutions Specialist, Mobility
Microsoft Gulf

Corbett works with organizations that are using mobility to improve their products and services quicker than their competitors and to build a more satisfied and loyal customer base. His expertise lies in managing diversity in the enterprise and bridging the gap between the needs of the enterprise and the flexibility of the mobile workforce.



15:15 MOBILITY WITHOUT VULNERABILITY: COMPREHENSIVELY MANAGING YOUR BYOD VISION

- Enabling BYOD with a complete mobile adoption strategy
- Mobilize business process and workforce
- Protect corporate data and apps on mobile devices
- Creating a successful BYOD policy

Haider Pasha
CTO & Head of Technical Sales and Services
Symantec

Haider has extensive security expertise and has provided thought-leadership for strategic clients of both Cisco and Symantec across the US, Middle-East and Africa. Haider partners with the CIOs in major verticals, and helps in executing together on a multi-year architecture strategy such as Cloud, Big Data, and BYOD.



15:45 NETWORKING AFTERNOON REFRESHMENTS

IN A HACKER'S WORLD

"New security loopholes are constantly popping up because of wireless networking. The cat-and-mouse game between hackers and system administrators is still in full swing"

- Kevin Mitnick

Ransomware is an upcoming trend. Hackers now want monetary gains and are more malicious than they ever were! It is crucial for security companies to always be a step ahead.

Hackers are very innovative and are always devising new ways to attack the OS. How can this be prevented? By the end of the presentation you will be more knowledgeable about the different types of hackers and how they think when it comes to selecting targets. Based on several factors you will be able to find out if you potentially can be the next victim!

16:15 INNOVATION SHOWCASE – ANDROID VS iOS

This showcase will highlight the differences in the various OS. For an in-depth discussion and to learn about the different platforms available and how to ensure your policies are secure enough for the various OS, attend Mobile Security workshop on Day 3!

HOW TO ENSURE YOU ARE ONE STEP AHEAD OF THE HACKER?

- What and who in hacking? (different types of hackers)
- How hackers think (selecting targets and attacks)
- Are you a target?
- Security threats in the mobile landscape of organizations
- How the proliferation of new devices can rock the security of an organization
- Ransomware for mobile devices
- Mitigating the risks
- Q&A

Tudor Enache
Principal Security Consultant
Help AG

Tudor is an all rounded Security Analyst / Penetration Tester with expertise in analyzing and testing the security controls of web applications, mobile applications, network infrastructures and many more. His technical expertise consists of knowledge in code development, scripting, social engineering, web/mobile/network hacking, infrastructure attacks, cryptography, and software testing.



How Mobility Can Transform Your Business?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

FORUM AGENDA

TECHNOLOGY ENABLED CRIMES

Globalisation has caused the increase of technology enabled crimes. Cyber attacks have become common occurrences and they still continue to be a costly affair.



16:55 **MOBILE GOVERNANCE (MGOV): EXTENDING THE GOVERNMENT TO EVERYONE, ANYTIME, ANYWHERE**

- mGov security challenges
- Prevent hackers and ransomware
- Changing expectations of service from Governments: Smart Governments
- Mobile Governance (mGov): The next frontier
- Mobile Governance (mGov): Future and extensions into wearable computing including devices like Google Glass

Asif Iqbal
Digital Forensics, Fraud and Security Investigator, Founder
Athena Labs

Asif Iqbal is an IT GRC professional with over 14 years of experience in diverse technical, leadership, advisory and consultancy positions. Asif is an active researcher in mobile device security and forensic investigations. He has published 9 research papers on forensics to date.



17:30 **END OF DAY 1 OF THE MOBILITY FORUM 2014**

DAY TWO - 3RD SEPTEMBER 2014, WEDNESDAY

09:00 **OPENING NOTE**

09:05 **WELCOME ADDRESS BY CHAIRMAN**

Omid Mahboubi
Co-founder
Middle East North Africa Cloud Alliance (MENACA)

Omid has been evangelizing Cloud Computing for the past 5 years. He frequently speaks at IT/Cloud events and feverishly advocates best Cloud practices. Omid served as the Chief Evangelist in the most prestigious Cloud industry group, Asia Cloud Computing Association. He co-founded the MENACA aiming at providing a unified voice in the industry and accelerating the adoption in the region.

MOBILE APPLICATION MANAGEMENT (MAM)

There seems to be a need to shift focus to MAM as well. There is an increasing diversity of devices and this creates havoc for the IT department. There needs to be constant awareness and training for organizations to stay ahead.

09:15 **BUILD AND CONNECT APPS, DEVICES AND DATA: TAKE YOUR ENTERPRISE MOBILE**

- Challenges faced when connecting mobile employees
- Unique challenges mobile faces
- Connecting to mobile employees, partners and customers to the back office systems, data and networks in a trusted and secure manner
- Dealing skilfully with a highly fragmented environment with multitudes of devices, platforms, and networks
- Learn how you can take your enterprise mobile with open, cost effective development and unmatched ability to make the connections you need

Girish Dhanakshirur
STSM, Master Inventor
IBM Mobile Foundation

Girish has successfully led the creation of many incubations in the area of Mobile, Cloud and Appliance products. He has nine patents issued in his name and number of others filed at the patent office.



10:00 **NETWORKING MORNING REFRESHMENTS**

HOW SECURE IS YOUR CLOUD?

How can you be sure the information that you store in the cloud is secure? Well, you can never be a 100% sure. But there are preventive measures that you can have in place to protect your data. Cloud has now become the place where information is kept and where everyone exchanges information.

Security breach can come from within as everyone has access to the information. Data theft is a huge concern. It is crucial to establish and enforce policies for a cloud-based system.

Is cloud security just hype or is it a real threat? The sessions for today will focus on how to ensure your cloud are safe and why the need for policies to be implemented.

Do you need a Mobile Device Management system?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

FORUM AGENDA

10:30 KEYNOTE: ARE YOU READY TO EMBRACE THE CLOUD?

- The cloud forecast for MENA
- The challenges organizations face
- Are all clouds made equal?
- Can you really make use of the cloud?

Andrew Grenville
Chief Executive Officer
Orixcom

Andrew is one of the leading cloud market movers and telecoms execs in the Middle East region with over 28 years of experience in telecoms/IT across multi disciplines and roles. He's passionate about driving adoption of innovative platforms and services to provide tangible value to end customers.

orixcom

11:15 VISIONARY KEYNOTE: IMPACT OF TECHNOLOGY ON SOCIETY AND CORPORATE

- Evolution of technology in last 5 decades
- Noticeable changes in social behavior
- Impact on Corporate culture
- BYOD & changing role of the CIO

Arun Tewary
VP (IT) & CIO
Emirates Flight Catering

Arun has earned the reputation & title of "Enterprise Resource Planning (ERP) Guru" in the region. He has over 25 years of experience in IT domain during which he has been involved in and has led a number of complex ERP implementations both in India and in the Middle East. Arun has won numerous awards and has been ranked as one of the top CIOs in the Middle East for several years now.

12:00 INDUSTRY KEYNOTE: NEPHOPHOBIA - ANALYSE YOUR FEAR OF CLOUDS

- Are the existing Cloud models mature enough to comply with regulatory regimes
- Where is the data sitting at any given time
- How different is Cloud from other outsourcing initiatives that you are already engaged with
- Take control of your fear

Omid Mahboubi
Co-founder
Middle East North Africa Cloud Alliance (MENACA)

Omid has been evangelizing Cloud Computing for the past 5 years. He frequently speaks at IT/Cloud events and feverishly advocates best Cloud practices. Omid served as the Chief Evangelist in the most prestigious Cloud industry group, Asia Cloud Computing Association. He co-founded the Middle East North Africa Cloud Alliance aiming at providing a unified voice in the industry and accelerating the adoption in the region.

12:45 NETWORKING LUNCH BREAK

14:00 A HOLISTIC APPROACH TO IMPLEMENTING CLOUD SECURITY FOR AN ENTERPRISE

- The cloud security alliance framework in a nutshell
- Embedding cloud security SLA into contracts/procurement
- Cloud security technologies – Be in control of your data at rest and in motion
- Software defined perimeter – mulling the attack surface for cloud assets.

Shah Sheikh
Co-Founder & Security Solutions Consultant
DTS Solution

Shah is a dynamic, astute and professional individual with more than 10 years of industry expertise and experience. Having worked for a Service Provider, System Integrator and multiple Vendors he has extensive knowledge on complete project lifecycle focused around security solutions.

DTS SOLUTION
smart solution for the smart business

XaaS

Anything as a service (XaaS), is here to transform the way we work. Selecting the right cloud is still a challenge for many organizations. Find out how to choose the right type of service for your needs.

14:30 THE ENTERPRISE CLOUD – A REALITY OR A VISION

- There is no cloud without innovation
- SaaS/PaaS/IaaS- Which service to choose to initiate the cloud strategy
- Make a comparison and choose the first cloud step approach

Vivek Srivastava
Senior Manager – Global Product Development
du

Vivek has over 16 years of experience and has implemented and launched products and services in Managed Services, Unified Communications, Cloud Computing, MDM and M2M. He has worked extensively with global carriers such as du, Orange Business Services, Tata Communications, BT Global Services and Bharti Airtel.

Do you need a Mobile Device Management system?

2 - 4 SEPTEMBER 2014 | RAFFLES DUBAI, UAE

FORUM AGENDA



15:15 **CREATING A SECURE CLOUD ARCHITECTURE**

- Traditional security architecture vs. cloud security architecture
- Local vs. global regulatory requirement on security
- How the cloud architecture fits in the enterprise security architecture

Ajay Rathi

Head of IT

Meraas Holding

Ajay is responsible for building and maintaining a highly available, scalable and centralized IT infrastructure and builds applications to meet the growing requirements of the organization. He has over 20 years of experience in core IT experience across multiple verticals like oil and gas, investment, foods& beverages, hospitality, retail malls and property development.



15:45 **NETWORKING AFTERNOON REFRESHMENTS**

16:15 **PRIVACY IN CLOUD**

- Secure data management
- Big data management

16:45 **SECURITY AS A SERVICE (SaaS)**

- Secure mobile cloud
- Trends of internet-based security

17:15 **END OF DAY 2 OF THE MOBILITY FORUM 2014**

CAPITALIZE ON MOBILITY FORUM 2014!

Looking for a platform to raise your profile and ROI?

Leverage on our excellent sponsorship opportunities to strengthen and confirm your market position through consistent and continual branding awareness and networking opportunities with high level decision-makers. This is the ideal platform to foster strong relationships with the IT security industry.

Partnering through an Event Sponsorship will enable you to:

- **Get unparalleled industry exposure**
- **Position your company as a thought-leader**
- **Generate leads and set-up key meetings**
- **Reaffirm your position in the industry**

Please contact *Janis Tan* at **+65 6899 5036** or email janis.tan@claridenglobal.com to discuss potential sponsorship opportunities.

Workshops Timetable: Workshops will run from 9:00 am – 5:00 pm, with mid morning, luncheon and mid afternoon refreshment breaks included. Registration will start 30 minutes before each workshop commences.

2 highly engaging workshops will be held; **Workshop A** will focus on **Hacking** and **Workshop B** on **Mobile Forensics**. These workshops will be conducted by renowned trainers who have a lot of experience working with MNCs and government agencies from across the region. Register for these workshops to gain an abundance of knowledge and engage in discussions, share your challenges and leverage the opportunities these workshops aim to deliver.



WORKSHOP A: 09:00 - 12:30
MOBILE SECURITY – LIVE HACKING WORKSHOP

Workshop Outline

“Hacking is exploiting security controls either in a technical, physical or a human-based element.” - Kevin Mitnick

It is a hacker’s world out there. Hacking has very much become mainstream culture. It is crucial to understand how the hacker’s work and to ensure that your devices or websites are secured. This half day workshop aims to increase awareness for web security problems and to start discussing about impacts and defence mechanisms.

Tudor will focus on exploiting vulnerabilities in mobile applications while also showcasing common coffee shop attack vectors including SSL Strip. He will share case studies on how to dissect mobile malware and mobile OS security hardening. Attack scenarios in modern web applications will be covered and fully exploited during the workshop.

During the workshop attendees will be introduced to the world of hacking and information security and given the adequate knowledge they need to thwart cyber criminals. Attendees can learn how to hack and crack using the techniques and tools of real hack.

This workshop will ensure that the attendees will be able to prevent an intrusion before it ever occurs. Expect this to be an eye-opener for security problems in web applications for developers as well as project managers.

Live Hacking

- Coffee shop attack (SSL Strip)
- Exploiting vulnerabilities in mobile applications
- Attack scenarios in modern web applications
- Live hacking using common attack vectors:
 - Authentication Bypasses
 - SQL injection
 - Live cache poisoning
 - Bluetooth hacking
 - Web jacking attack

Case Study showcasing how to:

- Dissect mobile malware
- Mobile OS security hardening (iOS, Android, Blackberry)

About Your Workshop Leader



Tudor Enache
Principal Security Consultant
Help AG

Tudor is an all rounded security analyst and penetration tester with 5 years of professional experience in analyzing and testing the security controls of web applications, mobile applications, network infrastructures, WiFi access points, VOIP systems and more.

Tudor’s technical background is a complex ecosystem consisting of knowledge in the following areas:

- Code development
- Scripting
- Social engineering
- Web/mobile/network hacking
- Infrastructure attacks
- Cryptography
- Software testing

Bachelor in Computer Science and Master in Artificial Intelligence, Tudor Enache has a diverse but complementary career evolution which makes him a versatile security analyst. Combining software testing, code development, security testing and management skills, Tudor has managed to achieve a level of combined expertise which is rarely found on the security market.

Currently working as Principal Security Consultant at Help Ag Middle East, Tudor is reporting 0-day vulnerabilities, speaking at conferences in the region, and providing security analysis services to big names in the region such as: Ministry of Finance, Emirates Identity Authority, Qatar National Bank, Dubai Islamic Bank, Dubai Chamber, Dubai Smart Government and much more.

End Of Workshop A
Workshop B will commence after lunch at 13:30.



WORKSHOP B: 13:30 - 17:00

MOBILE DEVICE DIGITAL FORENSIC INVESTIGATION

Workshop Outline

As the IT world is evolving research indicates that there is a shift in device type. Mobile devices have over taken the PCs both in numbers and usage. The tremendous technological shifts in data, services, and resources usage and consumption make forensic investigations more complicated than ever. It is a challenge to keep up-to-date with the fast-growing pace and constant updates and changes of mobile devices. This has caused a change to the face of digital forensics. Given the proliferation of mobile devices, it is rare for investigators to conduct a digital forensic investigation that does not include a mobile device. For many, the device is a welcome source of evidence as investigators often struggle to place a suspect behind a keyboard of a computer.

Standardization is necessary and that is another big challenge forensic investigators face. In the mobile space, there have been attempts to bring together providers and device manufacturers. A set of standardized technologies, or guidelines, will definitely lower the cost and will ensure the process of recovering data for investigations is sped up. It is, however, a challenging task to create standards for such a huge group of manufacturers. Asif, the workshop leader will discuss the challenges faced and share his expertise in the field of digital forensics.

This workshop will give an overview and the history of digital forensics, the types of policies and procedures that need to be in place and various types of mobile forensics. Asif will walk you through mobile device digital forensic investigation in this highly engaging and interactive workshop.

Digital Forensics

- History and overview of digital forensics
- Various types of forensics
 - o Mobile Forensics
 - o Cyber Forensics
 - o Cloud Forensics
 - o Digital Content Forensics
 - o Social Media Forensics

Criminal Forensics

- Law enforcement
- Digital Forensics
- Crime Scene Investigation (CSI)

The Need for Policies

- Procedures
- Processes

Google Glass Forensic Investigation

- Google Glass as a tool for Law Enforcement

Mobile Device Forensics overview

- iOS(iPhone,iPad,iPod) Forensics
- Android Forensics
- BlackBerry Forensics
- Windows Forensics

Digital Forensics Lab

About Your Workshop Leader



Asif Iqbal

Digital Forensics, Fraud and Security Investigator & Founder Athena Labs

Asif Iqbal is an IT GRC professional with 14 plus years of experience in diverse technical, leadership, advisory and Consultancy positions. An MSIT (Cyber Security) graduate from Zayed University earned Distinction with Honors. Certified as CISSP, CISA, CISM, CGEIT, CFE, CobiT, ISO/IEC 20000, CEH, CHFI and many others with experience in IT service management, information security, business continuity management, disaster recovery, risk management, ISO27001, CobiT, cyber laws, audit and implementations, compliance & governance. Security, digital fraud and forensic investigations are his first love.

Asif works with government agencies and has conducted various workshops and has presented on BYOD, mGov, MDM, Security, Forensics and many others. Athena Labs works closely with law enforcement agencies across the Middle East.

Asif is also engaged in research projects with Zayed University. Recently Asif lead and mentored a team from ZU for the development of Smart apps for Ministry of Higher Education and Scientific Research (MOHESR) as part of the mGov(Mobile Government) initiative by the UAE Government and got appreciated. He is an active researcher in mobile device security and forensic investigations.

A few of his research publications include the following:

1. Windows Surface RT Tablet Forensics

Digital Forensics Research Conference 2014 (DFRWS 2014, Netherlands)
International Journal of Digital Investigation

2. Amazon Kindle Fire HD Forensics

5th International Conference on Digital Forensics & Cyber Crime (ICDF2C 2013, Moscow Russia)

3. The Study of the Interrelation between Law Programs and Digital Forensics in UAE Academia

The 2013 Information Security Curriculum Development Conference (InfoSecCD 2013, USA)

4. Forensic Artifacts of ChatON Instant Messaging Application

8th International Workshop on Systematic Approaches to Digital Forensics Engineering (SADFE 2013, Hong Kong)

5. A Novel Method of iDevice (iPhone,iPad,iPod) Forensics without Jailbreaking

The 8th IEEE International Conference on Innovations in Information Technology (Innovations 2012, Al Ain UAE)

End of Workshop B & End of Mobility Forum 2014!

See you in 2015!

REGISTRATION PAGE

Please complete this section.

Booking Contact (Approving Manager) Mr/Mrs/Ms: _____
 Job Title: _____ Department: _____
 Telephone: _____ Fax: _____
 Email: _____
 Organization: _____
 Address: _____
 _____ Postal Code: _____

I would like to receive more information on hotel accommodation using Clariden Global corporate rate.

Promotional Code (Optional): _____

Please register the following participant(s) for this Conference

(Please tick to select your Conference packages. You may tick more than one.)

1st Participant Name (Mr/Mrs/Ms): _____

Job Title: _____ Department: _____

Telephone: _____ Fax: _____

Email: _____ Date of Birth: _____

Conference Package Selected: _____

2nd Participant Name (Mr/Mrs/Ms): _____

Job Title: _____ Department: _____

Telephone: _____ Fax: _____

Email: _____ Date of Birth: _____

Conference Package Selected: _____

3rd Participant Name (Mr/Mrs/Ms): _____

Job Title: _____ Department: _____

Telephone: _____ Fax: _____

Email: _____ Date of Birth: _____

Conference Package Selected: _____

4th Participant Name (Mr/Mrs/Ms): _____

Job Title: _____ Department: _____

Telephone: _____ Fax: _____

Email: _____ Date of Birth: _____

Conference Package Selected: _____

GROUP DISCOUNTS

For registration for 2 participants, enjoy 10% discount on 2nd participant. For a limited time only by 12th August 2014, register 3 participants and the 4th participant will receive a complimentary seat. Complimentary seat will be registration of the lowest value.

CONFERENCE FEES

Conference Packages	1st Early Bird Fee (If payments and registrations are received by 15th July 2014)	2nd Early Bird Fee (If payments and registrations are received by 12th August 2014)	Regular Fee Nett
A: Conference + Full-Day Workshop	US\$ 3,295 US\$ 2,995	US\$ 3,495 US\$ 3,195	US\$ 3,595 US\$ 3,295
B: Conference Only	US\$ 2,595 US\$ 2,295	US\$ 2,795 US\$ 2,495	US\$ 2,895 US\$ 2,595
C: Conference + Workshop A	US\$ 2,995 US\$ 2,695	US\$ 3,195 US\$ 2,895	US\$ 3,295 US\$ 2,995
D: Conference + Workshop B	US\$ 2,995 US\$ 2,695	US\$ 3,195 US\$ 2,895	US\$ 3,295 US\$ 2,995
E: Workshop Only	US\$ 995	US\$ 995	US\$ 995



PLEASE NOTE:

The conference fee includes lunch, refreshments and conference documentation. Payments are required with registration and must be received prior to the Conference to guarantee your place.

CONFERENCE VENUE AND ACCOMMODATION INFORMATION

Raffles Dubai, UAE

Address : Sheikh Zayed Road, Wafi, Dubai P.O. Box 121800

: +9714 324 8888

Website : <http://www.raffles.com/dubai/>

4 WAYS TO REGISTER



Email: admissions@claridenglobal.com



Fax: +44 (0) 84 3218 0413



Call: +44 (0) 20 7129 1222



<http://www.claridenglobal.com>

PAYMENT METHODS

BY CHEQUE / BANK DRAFT :

Made payable to CLARIDEN GLOBAL INTERNATIONAL LIMITED and mail to: 3 International Business Park, #04-29, Nordic European Centre, Singapore 609927.

BY TELEGRAPHIC TRANSFER TO:

Bank Name: **Standard Chartered Bank**

Bank Code: **7144**

Bank Branch Code: **001**

Bank Address: **6 Battery Road, #01-01 Singapore 049909**

Bank Account No: **0107775042**

Bank Account name: **CLARIDEN GLOBAL INTERNATIONAL LIMITED**

SWIFT Code: **SCBLSG22**

Please note that all bank charges are to be borne by participants. Please ensure Clariden Global International Limited receives the full invoiced amount.

Note: Please include invoice number on all payment types and your company's name in your payment instructions for our reference.

CREDIT CARD:

To make payment by credit card, please call our client services hotline at +61 3 9909 7310.

HOW TO REGISTER AND PAY

An invoice and registration confirmation will be sent within 7 days, please contact us if you have not heard from us within 7 days. Payment can be made by credit card, by bank transfer (for bank account details, please see payment details section of booking form) or by cheque made payable to "Clariden Global International Limited" and posted to Clariden Global International Limited at: 3 International Business Park, #04-29, Nordic European Centre, Singapore 609927.

ALL PAYMENTS MUST BE RECEIVED IN ADVANCE OF THE EVENT.

ACCOMMODATION

Accommodation is not included in the conference fee but you will be entitled to use our corporate rate for your accommodation. Information will be sent with the registration confirmation.

CANCELLATIONS AND SUBSTITUTIONS

Once we have received your booking, the place(s) are confirmed. No refunds will be made for any cancellations, however, program credits of equivalent value only applicable for Clariden Global events will be provided. Credits can only be redeemed for 1 program and is valid for only one (1) year from date of issue.

Substitution with a qualified candidate is allowed by providing at least 5 working days of advance notice to Clariden Global. One time substitution is allowed with no charges. Subsequent substitutions will be charged 10% admin fee.

ALL CANCELLATIONS MUST BE RECEIVED IN WRITTEN FORM

PLEASE NOTE: Clariden Global International Limited reserves the right to change the content and timing of the programme, the speakers and the date and venue due to reasons beyond their control. If in the unlikely event that the course is cancelled, Clariden Global International Limited will refund the full amount and disclaim any further liability.

ENQUIRIES: If you have any queries about registration or payment please do not hesitate to contact our client services department on +44 (0)20 7129 1222.

PRIVATE DISCLOSURE STATEMENT: Any information provided by you in relation to this event is being collected by Clariden Global International Limited and will be held in the strictest confidence. It will be added to our database for the primary purpose of providing you with information about future events and services.

Visit us at www.claridenglobal.com for upcoming events

FOR OFFICIAL USE

FEE RECEIVED

REFERENCE C4099/TK/JN