



# MANAGING SECURITY IN ENTERPRISE NETWORK

SECURING YOUR NETWORK FROM WITHIN

13<sup>th</sup> & 14<sup>th</sup> November 2006, Sheraton Imperial, Kuala Lumpur

## WORKSHOP LEADER



**AHMAD ELKHATIB**  
Security Consultant  
Pointsec Mobile Technologies,  
UAE

### Secure expert advice from the following organisations:

Asia Pacific Advanced -  
Networks (APAN)

Siemens Multimedia -  
SIG<sup>2</sup>, Singapore -

Malaysian Communication and -  
Multimedia Commission (MCMC)

Net-Square Pvt Ltd, India -  
DigiCert -

Maxis Communications -

This strategically focused event will provide delegates with in-depth knowledge in:

- ◆ **Integrating** a proactive network monitoring system
- ◆ **Building** a secure communication network
- ◆ **Increasing** mobile device security
- ◆ **Gaining** insights on Information Technology security laws
- ◆ **Unifying** threat management for increasing hostile environment
- ◆ **Tackling** identity access management issues
- ◆ **Identifying** best practices in network security
- ◆ **Measuring** Return On Investment of security expenditure

Today's business environment is becoming very complex, and to manage network security in that environment is also becoming tough. Just to gain visibility into all of the areas of risk in an organisation is a challenge in itself, and understanding what all of the vulnerabilities are adds another layer of complexity.

As the role of enterprise networks keeps expanding in its support of both internal and external connectivity in the form of emerging internet, intranet and extranet applications, network connections are being exposed more and more seriously to malicious as well as unintentional security breaches. Network security becomes an ever increasingly critical element of enterprise network designs and implementations.

A typical network security exercise involves the planning and designing of a company's networks and information technology (IT) security infrastructures. This ensures the protection of its valuable applications, sensitive data and network resources from unauthorised access that results in either intentional or unintentional misuse or malicious alterations of the company's assets.

Complete IT security means being able to integrate information about the asset with security details. The security of all networks, wired and wireless can be improved by employing the four pillars of network security—firewall, antivirus, intrusion-detection systems (IDS) and intrusion-prevention systems (IPS). Networks are the lifeblood of businesses today; they are the nervous systems of organisations across the world.

**“Total cyber crime losses in 2005 were \$30.1 million, the majority of losses are due to viruses, unauthorized access to network and theft of proprietary information.”**

Source: - CSI/FBI Computer Crime & Security Survey

Researched & Produced by

**KNOW|edge**  
group of companies

For Reservations & Enquiries, call - (603) 2170 1588  
or email us at [admin@knowledgegroupco.com](mailto:admin@knowledgegroupco.com)

0830	<b>Registration &amp; Welcome Coffee</b>	1500	<b>Hacking Methodology and Incident Handling</b> <ul style="list-style-type: none"> <li>■ Recognising hackers and understanding their reasons for hacking</li> <li>■ Explaining internal and external factors as to why intrusions happen</li> <li>■ Tracking down network hackers</li> <li>■ Developing immediate and consistent measures to be taken</li> <li>■ Coordinating CERT (Computer Emergency Response Team) efforts with the organisation's network security system</li> </ul> <b>Umesh Nagori</b> Vice President of Business Development <b>Net-Square Pvt Ltd, India</b>
0900	<b>Opening &amp; Welcome Remarks by Chairperson</b>	1600	<b>Afternoon Refreshment</b>
0915	<b>Integrating a Proactive Network Monitoring System</b> <ul style="list-style-type: none"> <li>■ Setting a target and objective to achieve optimum security</li> <li>■ Constant monitoring of the network system</li> <li>■ Maximising awareness in network security</li> <li>■ Why are CEOs not prioritising network security?</li> </ul> <b>Dr.Sureswaran Ramadass</b> Head <b>Asia Pacific Advanced Networks (APAN), Malaysia</b>	1615	<b>CASE STUDY - FRAUD MANAGEMENT</b> Ami Azrul is responsible for developing IT systems strategic and operational plans in support of the overall mission and business strategy. Having worked for both Malaysian CAs, Ami Azrul is also advisor on evaluation, selection, implementation and maintenance of CA system, ensuring appropriate investment in strategic and operational systems. <b>Ami Azrul</b> Chief Technology Officer <b>DigiCert</b>
1015	<b>Building Up a Secure Communication Network</b> <ul style="list-style-type: none"> <li>■ Trusting your organisation's existing network</li> <li>■ Recognising the evolution of network security</li> <li>■ Discussing new security strategies to overcome network threats</li> <li>■ Identifying best practices for end-to-end defense in-depth</li> </ul> <b>Syed Mohsin Syed Mohammad</b> Manager, Solution Management <b>Siemens Multimedia</b>	1645	<b>Identity Access Management - The Weakest Link in Network Security</b> <ul style="list-style-type: none"> <li>■ Information security: Confidentiality, Integrity and Availability</li> <li>■ Trends and developments in online identity theft</li> <li>■ Moving towards a more pervasive identity access management in future</li> <li>■ Introduction of biometrics technology</li> <li>■ Centralising security with a single log on</li> </ul> <b>Suresh Ramasamy</b> Manager, Security Operations <b>Maxis Communications</b>
1115	<b>Morning Refreshment</b>	1745	<b>Closing Remarks by Chairperson</b>
1130	<b>Analysing Cyber Forensics in Network Security</b> <ul style="list-style-type: none"> <li>■ Understanding 'Chains-of-Evidence'</li> <li>■ Examining bulks of electronic mails, documents and other data</li> <li>■ Dealing with deleted, hidden or password-protected data</li> <li>■ Ensuring completion of examination and all available data</li> <li>■ Determining if the electronic evidence be admissible in Court</li> </ul> <b>Aloysius Cheang</b> President <b>SIG<sup>2</sup> Singapore</b>	1800	<b>End of Day One</b>
1230	<b>Addressing Mobile Device Security</b> <ul style="list-style-type: none"> <li>■ Increasing workforce mobility</li> <li>■ Analysing how data gets lost</li> <li>■ Realising the importance endpoint security</li> <li>■ Understanding laws and regulations affecting data protection</li> <li>■ Overviewing technical architecture of encryption solution</li> </ul> <b>Ahmad Elkhatib</b> Security Consultant <b>Pointsec Mobile Technologies,UAE</b>	<p style="text-align: center;"><b>'PIKOM: More To Security Than Meets the Eye',</b></p> <p>Most Malaysian businesses lack a proper corporate It policy when it comes to network security, said the Association of the Computer and Multimedia Industry of Malaysia (PIKOM). An example would be when an employee uses a company laptop to connect to the Internet outside the office. The laptop might be hacked and infected by viruses.</p> <p>The company's IT policy might require that all laptops be quarantined and scanned for infection before allowing them to be connected to the company's internal network, thus preventing virus infiltration. Many IT administrators should also not think their networks are secure just because they have a firewall in place. Many forget that security has to be (enforced) on both sides of the fence.In fact, about 80% of security incidents occur internally. There is no escape from going through the painstaking process of identifying the specific point of failures to determine the level of protection needed by a business.</p> <p><b>Source: The Star, 10 November 2005</b></p>	
1315	<b>Networking lunch</b>		
1415	<b>Implementation of Policies and Information Security Governance</b> <ul style="list-style-type: none"> <li>■ Addressing security issues and challenges</li> <li>■ Initiatives in safe and secure networking</li> <li>■ Implementation of information security policies</li> <li>■ Embracing information and network security governance</li> </ul> <b>Mohd Ali Hanafiah</b> Head, Content, Consumer and Network Security Division <b>Malaysian Communication and Multimedia Commission (MCMC)</b>		

**FULL DAY INTERACTIVE WORKSHOP**

**Session One**

**Establishing a Wireless Security in Network**

- Countering wireless hacking
- Securing a Voice over Internet Protocol (VOIP) network
- Camouflaging network by setting up a fake IP address

Session goal: Numerous security problems can result from wireless networks. In this session delegates will be provided with in-depth understanding on Internet Protocols and on countering attacks from a wireless device.

**Session Two**

**Implementing a Proper Security Framework to Mitigate Risks**

- Adopting International Framework for Network Security - ISO 27001
- Comparing the current standard with ISO 17799
- Discussing security in the system development lifecycle

Session goal: Despite the spectacular cases of external break-ins, most damage to computer systems and data comes not from malicious outside attacks, but rather from simple mistakes or the unauthorised or unintended actions of legitimate users. This session will focus on implementing a proper framework to improvise network security within your organisation.

**Session Three**

**Unifying Threat Management for Increasing Hostile Environment**

- Identifying information and network security threats encountered by businesses today
- Working towards obtaining rapid response to curb emerging threats and rising incidents
- Increasing challenges in managing security and mobility

Session goal: An effective threat management program will provide security teams with the efficiency they need to counter emerging threats. Delegates will attain detailed insights into the network security threats and challenges faced by organisations today.

**Session Four**

**Analysing Intrusion Prevention Systems (IPS) vs. Intrusion Detection Systems (IDS)**

- Understanding architecture of the network security system
- Learning the effectiveness of intrusion protection system
- Looking back at intrusion detection system

Session goal: Announcements that IDS will soon be dead and IPS is the answer to most security issues left the information security industry in a state of confusion. This session will highlight both the IPS and IDS systems to provide detailed understanding for the delegates

**Session Five**

**Implementing an Effective Risk Management Strategy**

- Understanding the fundamentals of risk

management in network security

- Valuing the amount of security required in measuring the ROI on security expenditure
- Developing strategies in e-security risk management

Session goal: Although security remains a top IT spending priority, companies often focus on the wrong issues. This session will provide a detailed approach on the strategies that can be implemented to efficiently managed risks in IT security.

**Session Six**

**Mastering Best Practices in Network Security**

- Assessing risks by conducting a comprehensive risk analysis
- Defining boundaries with third party sourcing
- Relying on multiple solutions to derive competitive advantage
- Taking the right measures to improve security for information and access
- Creating awareness to avoid human error
- Introducing a new class of network log on devices using biometrics

Session goal: When the success of a project is critical, an insurance is needed to ensure that it will be done right. This session will assist delegates in understanding the best practices in network securities to maximise the performance of the organisations

**YOUR WORKSHOP LEADER**

**AHMAD ELKHATIB**  
 Security Consultant

**Pointsec Mobile Technologies**

Ahmad Elkhatib is currently a security consultant with Pointsec, a leader in mobile device security and encryption. Previous to that Ahmad was an Information Security consultant at InnokAT where he helped top enterprises in the region by designing and implementing their security strategies. Ahmad also worked at iDEFENSE where he started as a Vulnerability Research Engineer with iDEFENSE Labs. He later worked as a Malicious Code Analyst as part of the Malicious Code Team. Ahmad also was involved in wireless network security at British Telecom.

Ahmad holds a degree in Computer Engineering from the University of Michigan - Ann Arbor. He is a member of the Information Systems Security Association and is BS7799 and CISSP certified and has presented at various security conferences around the world including HackInTheBox, MEITSEC, and PAKCON.

**COURSE TIMETABLE**

Registration	0830
Workshop commences	0900
Morning refreshment	1030
Workshop resumes	1045
Luncheon	1300
Workshop resumes	1400
Afternoon refreshment	1530
Workshop resumes	1545
End of workshop	1730

**2-day event fee**

- 2-day event @ RM3688 per delegate
- Early bird @RM3288 per delegate before 29<sup>th</sup> September 2006  
 ( Price is not inclusive of 5% Government Tax)
- 10% discount for 3rd and subsequent registration (Premier Value)

**Method of Payment :**

Crossed cheque / bank draft to be made payable to **PROFESSIONAL KNOWLEDGE CENTRE (M) SDN BHD** and courier to **B-13-5, Megan Avenue II, 12, Jalan Yap Kwan Seng, 50450 Kuala Lumpur, Malaysia**

**Hotel accommodation:** Please contact Sheraton Imperial at 03 - 2717 9900 and mention our event to enjoy privileged room rates.

**Note :** It may be necessary for reasons beyond control, to change the content and timing of the event, our speaker(s) or venue, every effort will be made to inform participants of the change.

**Please note that payments must be received within 5 days upon issuance of invoice.**

**Please complete this form immediately and fax this to  
 Fax to : 603 2166 5451**

Name : \_\_\_\_\_

Position : \_\_\_\_\_

Name : \_\_\_\_\_

Position : \_\_\_\_\_

Name : \_\_\_\_\_

Position : \_\_\_\_\_

Organisation : \_\_\_\_\_

Address : \_\_\_\_\_

Town : \_\_\_\_\_

State : \_\_\_\_\_

Postcode : \_\_\_\_\_

Tel : \_\_\_\_\_

Fax : \_\_\_\_\_

Email : \_\_\_\_\_

The Invoice should be directed to Mr/Ms(Dept):

Name : \_\_\_\_\_

Nature of Business : \_\_\_\_\_

Name of Authorising Manager : \_\_\_\_\_

Title : \_\_\_\_\_ Dept: \_\_\_\_\_

Signature : \_\_\_\_\_

This booking is invalid without a signature

**WHY YOU SHOULD ATTEND**

Managing security risks is a continuing challenge because of the growing reliance on information technology. Although information technology brings benefits of improved information processing and communication, however, it also increases the risks of computer intrusion, fraud and disruption. Organisations have been struggling to find efficient ways to ensure that they fully understand the information security risks affecting their operations and to implement appropriate controls to mitigate these risks.

With the aid of regional and local case studies, this timely event will provide delegates with an excellent platform to learn and network with leading professionals from various organisations. As a conclusion, delegates will be provided with clear guidelines on how to secure their network from unauthorised access.

**WHO SHOULD ATTEND**

Network Directors & Managers, IT Directors & Managers, Network Architects, Security Engineers, Chief Technology Officers, Data Analysts, Chief Information Officers, Chief Security Officers, IT System Directors/Managers

**BUSINESS OPPORTUNITY**

This event will offer you an opportunity to gain preferential access to the senior executives in your target market to network and learn from each other. It is an excellent platform to meet decision makers face-to-face to create business opportunities and to enhance your corporate image in the market. Our events are not overcrowded exhibition where you need to compete with over 100 exhibitors. This is a targeted business strategy event where you get to meet the senior decision makers. For further details, please contact Anushah Pillai at 603-2170 1588 or email anushah@knowledgegroupco.co

**TERMS & CONDITIONS**

**Knowledge Group** does not provide refunds for cancellations. For cancellations received in writing more than 14 working days prior to the conference you will receive a 50% credit to be used at another **Knowledge Group** event for up to six months from the date of issuance. For cancellations received less than 14 working days prior to the event no credits will be issued. In the event that **Knowledge Group** cancels an event, delegate payments at the date of cancellation will be credited to a future **Knowledge Group** event and will be valid for up to six months from the date of issuance. Where **Knowledge Group** postpones an event, delegate payments at the postponement date will be credited towards the rescheduled date. If the delegate is unable to attend the rescheduled event, the delegate will receive a 100% credit representing payments made towards a future **Knowledge Group** event and will be valid for up to six months from the date of issuance. No refunds will be available for cancellations or postponements. However, a complete set of documentation will be sent to you. Substitutions are welcomed at anytime. **Knowledge Group** is not responsible for any loss or damage as a result of a substitution, alteration, cancellation or postponement of an event. Nor will any liability attach to **Knowledge Group** if this event is altered, rescheduled, postponed or cancelled due to unforeseen occurrence. For the purposes of this clause, an unforeseen occurrence shall include, but shall not be limited to: an Act of God; governmental restrictions and/or regulations; war or apparent act of war; terrorism or apparent act of terrorism; disaster; civil disorder, disturbance, and/or riots; or any other emergency. Please note that speakers and topics were confirmed at the time of publishing, however, circumstances beyond the control of the organizers may necessitate substitutions, alterations or cancellations of the speakers and/or topics. As such, **Knowledge Group** reserves the right to alter or modify the advertised speakers and/or topics if necessary.