

21st November 2006
Chief Information Security Officers' Roundtable:
Managing Information Security Risk

22nd & 23rd November 2006
InfoSec World – Lapland 2006 Conference

24th November 2006
Security Threat Horizon - Roundtable

The Scandic Hotel, Rovaniemi, Lapland Finland

Join senior IT security peers from all corners of the world to discuss the most critical security challenges of the day & share visions of what it takes for truly successful leadership across security technology, architecture, applications & policy

Keynotes by:

Ari Uusikartano, Director for Information & Documentation, CIO, Ministry for Foreign Affairs, Finland

Seppo Sundberg, Chief Security Officer, Finnish State Treasury, Ministry of Finance

International Case Studies by:

Aaro Hallikainen, Chief Security Officer, Finnish Police IT Management Agency (FINLAND)

Aku Hilve, Chief Information Security Officer, Helsinki Police (FINLAND)

Andy Jones, Senior Project Manager, Information Security Forum (UK)

Dr. Arjen Lenstra, Head of the ISIS Security Center, EPFL, Former Senior Security Researcher, Lucent Technologies', Former Security Officer, Citigroup (SWITZERLAND)

Arto Kangas, Coordination Manager, Information Security Manager, Finnish Insurance Data Ltd, Board Member, Finnsecurity ry & Board Member, Finnish Information Processing Association

David Boye, Chief Security Officer, Saxo Bank, (DENMARK)

Dr. Frank Marsh, Global Information Security Manager, British American Tobacco (UK)

Jari Pirhonen, Head of Security, Samlink Ltd. & President, Finnish Information Security Association (FISA) (FINLAND)

John Meakin, Group Head of Information Security, Standard Chartered Bank (UK)

Marco Ricca, Associate Founder & Director, ilion Security SA (SWITZERLAND)

Marinó G. Njálsson, Consultant, Betri akvordun, (ICELAND)

Mark Concar, Director Data Security, American Express (UK)

Michael Colao, Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein (UK)

Petri Ala-Annala, Chief Information Security Officer, Helsinki Energy (FINLAND)

Phil Pinder, Executive Director, Management Controls Department, Goldman Sachs (UK)

Capt. Raghu Raman, CEO, Mahindra Special Services Group & Principle Partner, DBS Solutions

Richard Hollis, CEO, Orthus Ltd. (UK)

Dr. Thomas P. Braun, IT Security Officer, World Trade Organization (WTO) (SWITZERLAND)

Dr. Timo Karvi, Professor, Computer Science Department, University of Helsinki (FINLAND)

Tommi Vainio, Security Manager, Security Department, TeliaSonera Finland Oyj (FINLAND)

Dr. Uwe Aickelin, Senior IT Security Researcher, University of Nottingham (UK)

Vincent Bieri, CEO, NEXThink S.A. (SWITZERLAND)

InfoSec World - Lapland 2006

Protecting Information Assets & Infrastructure in an Always On World:
IT Security for Business & Government

21st - 24th November 2006



Gain 30 CPE Points

Official Conference Partner



MIS Training & the Rovaniemi Regional Development Agency Ltd. are delighted to invite you to participate in this exciting collaboration that will unite global information security communities



Exhibition Sponsor



Association Partners



Supporting Associations



Supported by



Media Partner





InfoSec World - Lapland 2006

21st - 24th November, Rovaniemi, Lapland, Finland

Gain 30
CPE
Points

Dear Colleague,

MIS Training Institute EMEA is delighted to invite you to attend this inaugural cutting-edge security conference, **InfoSec World - Lapland 2006** held in collaboration with the **Rovaniemi Regional Development Agency Ltd.**

An internationally significant ICT Security Cluster has been established in Rovaniemi, whose expertise concentrates on all sectors of security with the interface of information technology or its applications. Home to a number of business & public including organisations working in the field of security, including: the Police IT Management Agency, the Frontier Guard, Customs, Defence Forces, Police, Rescue Agency & the Finnish Civil Aviation Authority - this event combines local & international expertise.

Join your IT security peers from around the world to discuss the most critical security issues of the day & thrash out debates to share clear visions of what it takes for truly successful leadership in security - across networks, technology, architecture, applications & policy.

An international speaker panel will include Chief Information Security Officers (CISOs), CIOs & experienced Information Security Managers. With the support of prestigious local & global information security communities, including: Finnish Information Security Association (FISA), Finnsecurity Association, various ISSA & ISACA Chapters, the Information Security Forum (ISF), this is a unique gathering of security pioneers from business & government that you should not miss!

Official Conference Partner



Aurora Borealis Technology centre is hosted by **Rovaniemi Regional Development Agency Ltd. (RRDA)** which is a regional development agency functioning as the economic development unit of the Rovaniemi sub-region. It is owned by the city of Rovaniemi & the municipality of Ranua. RRDA's tasks are to produce, organise & develop business activities & to give support for the enterprises as well as educational institutions, municipalities & other public organisations in the region. RRDA supports starting enterprises, offers business incubator activities & manages the regional technology centre (Aurora Borealis).

The activity of the cluster of expertise concentrates on all sectors of security with the interface of information technology or its applications. The cluster develops new top expertise in the region & enhances ICT company activities in Rovaniemi. Rovaniemi is also home to a number of public administration organisations working in the field of security, such as the Police IT Management Agency, the Frontier Guard, Customs, Defence Forces, Police, Rescue Agency, Emergency Call Centre & the Finnish Civil Aviation Authority.

The University of Lapland & the Rovaniemi Polytechnic provide training, research & development services in the field. The intention is to increase research into data security & to direct more training as to the industry. Aurora Borealis Technology Centre is a centre based in the Rovaniemi district that combines high technology, international business activities, & the experience industry. The vision for the future is for the Centre to become one of the world's leading experience industry centres by the year 2010. The utilisation of ICT technology in tourism is implemented in Rovaniemi as part of Aurora Borealis Testing Lab Programme. The focus of testing is the applications' functionality, usability, & revenue-generation model. The initiated mobile testing programme is the first testing that operates in genuine conditions using real users with a concentration on tourism & experience services. Visit: www.auroraborealisrovaniemi.com/ www.rovaniemenkehitys.fi

Organised & Produced by



Founded in 1978, **MIS Training Institute** is the international leader in audit & information security training, with offices in the USA, UK, & Asia. Helping internal audit & information security professionals stay at the top of their game has always been at the core of MIS' mission. To that end, MIS has developed & focused its seminars, conferences, & symposia on the wide-ranging needs of internal & IT auditors & information security practitioners who are charged with controlling complex systems & business environments.

All MIS programmes are led by industry experts...hands-on pros who have been in the field & who practice what they teach. Attendees of MIS Training Institute events benefit from unbiased practices, proven strategies, & lessons learned in the real-world. MIS Training Institute is registered with the National Association of State Boards of Accountancy (NASBA) as a sponsor of continuing education on the National Registry of CPE Sponsors. MIS Training Institute sits within Euromoney Training, & is a division of Euromoney Institutional Investor Plc (FTSE250). Euromoney Institutional Investor Plc is part of the Daily Mail & General Trust (DMGT). www.mistiemea.com

Association Partners



Finnish Information Security Association (FISA) is the largest information security association in Finland. FISA is a non-profit association, which objective is to advance information security professionalism, awareness & best practices. Activities include member meetings, discussion groups, company visits, conferences, CISSP certification and participation of various information security programmes. See FISA (Tietoturva ry or TTRY in Finnish) web-site www.tietoturva.fi for more information or contact us via email info@tietoturva.org



The Information Security Forum (ISF) is recognised as the world's leading Information Security organisation & independent industry authority. Through its members, the ISF brings together & harnesses the knowledge & experience of over 280 major international business & government agencies to meet the increasing demand for practical, business-driven solutions to information security & risk management problems. Current ISF projects focus on a wide range of issues including security & legislation, identity management, patch management, information risk, & VOIP. This in-depth research eliminates the need for ISF members to develop their own in-house solutions & delivers rapid return on investment. The Information Security Forum is an independent, not-for-profit organisation, established in 1989. It is owned & governed by its members & managed by a professional team. For more information about the ISF visit www.securityforum.org

Supporting Associations



Finnsecurity ry is a registered security association in Finland. Finnsecurity's main goal is to raise security field's respect & develop its operation opportunities. Finnsecurity's aim is also to strengthen its members professional knowledge & make it easier for the members to co-operate with others. **Finnsecurity ry** has private members, legal members & community members. By 1.6.2005 the number of members was 579 & raising. The members can also take part in Finnsecurity's commissions' work to develop association's internal activities.

Finnsecurity ry organises different kind of security & safety events, e.g. FinnSecurity -exhibitions & FinnSec -fairs since 1978. FinnSec -fair has become the biggest & most important security & safety event in Finland & the first day is aimed specially at foreign visitors.



The Information Systems Security Association (ISSA)® is a not-for-profit international organisation of information security professionals and practitioners. It provides education forums, publications and peer interaction opportunities that enhance the knowledge, skill and professional growth of its members.



ITS Norway is a national ITS organisation (for Multimodal Intelligent Transport Systems and Services) with members from ministries, authorities, users, suppliers & research organisations. ITS in Norway was formally founded at the first General Assembly at June 15th 2004. An important task for the association is to build professional networks for its members. It is also important for the organisation to arrange contact with high-level strategy development & political fora. ITS Norway shall support the application of IntelligentTransportSystems in all modes of transport & shall improve Norwegian companies' opportunities in the global market. On behalf of its members the organisation shall work towards increased funds & better programmes for research & development, nationally & through EU Framework Programmes. ITS Norway is a member of the NITS, the Network of national ITS associations at ERTICO (ITS in Europe).



ISACA has become a pace-setting global organisation for information governance, control, security & audit professionals. Its IS auditing & IS control standards are followed by practitioners worldwide. Its research pinpoints professional issues challenging its constituents. Its Certified Information Systems Auditor (CISA) certification is recognised globally & has been earned by more than 48,000 professionals since inception. The Certified Information Security Manager (CISM) certification uniquely targets the information security management audience & has been earned by more than 6,000 professionals. It publishes a leading technical journal in the information control field, the Information Systems Control Journal. It hosts a series of international conferences focusing on both technical & managerial topics pertinent to the IS assurance, control, security & IT governance professions. Together, ISACA & its affiliated IT Governance Institute lead the information technology control community & serve its practitioners by providing the elements needed by IT professionals in an ever-changing worldwide environment. Members live & work in more than 140 countries & cover a variety of professional IT-related positions. ISACA has more than 170 chapters established in over 60 countries worldwide, & those chapters provide members education, resource sharing, advocacy, professional networking & a host of other benefits on a local level.



About Rovaniemi - The Gateway to Lapland

An international, developing town of business, administration & education, Rovaniemi is located at the confluence of Lapland's mighty rivers Kemijoki and Ounasjoki. The total population of the Rovaniemi sub-region is 63 000 inhabitants. As the capital of the province, Rovaniemi has maintained contact with the surrounding countryside but the urban infrastructure creates opportunities for development and is home to a number of businesses & public organisations working in the field of security. Within 10 km from the city centre you can find undisturbed nature or a busy international airport. Experience something exotic: playing golf under the midnight sun in summer or on the river ice in winter; trekking in Ounasvaara; atmosphere-rich riverboat cruise; visit to a reindeer farm or the thrill of the summer toboggan run. You can participate in a number of safaris, fishing trips, or take a day trip to the Ranua Wildlife Park with its over 50 species of Arctic animals. Weather - winter is a guaranteed success in Lapland. Permanent snow cover generally settles in October - November, after which the covering gets steadily thicker. Typical daylight hours in November are 08:00 - 17:30. www.laplandfinland.com

Exhibition Sponsor

TeliaSonera

TeliaSonera - The Nordic & Baltic telecommunications leader - holds strong positions in mobile communications in Eurasia, Turkey & Russia. We offer reliable, innovative & easy-to-use services for the transmission & packaging of sound, images, data, information, transactions & entertainment. We see simplicity & service as important drivers for creating long-term growth & value for our customers & shareholders. www.sonera.com

Tackle the full spectrum of real-world security challenges:

- Evaluate emerging security technologies & new services that have been successfully deployed
- Benchmark the legal challenges, pitfalls, auditability & compliance of managing enterprise & public security projects
- Trends in two-factor authentication & identity management deployments
- Cutting-edge techniques for hacking web applications & networks
- How to position security within your organisation to ensure investment & management support
- Day-to-day strategies for vulnerability management
- Common mistakes often made when conducting a risk assessment
- Open-source tools available - plus the costs & benefits
- Database leakage concerns from a legal liability standpoint

Via:

- New research presented by security experts from around the world
- Focused Government & Industry Sessions
- CISO Executive Roundtable - benchmarking & discussion event highlight
- Dedicated time for networking & building professional contacts at cocktail receptions & optional snow activities

Sponsorship & Exhibition Opportunities

Attendees at MIS Training's **InfoSec World - Lapland 2006** are senior decision makers within the information security community - from across business & governmental sectors. This gathering of normally elusive & difficult to reach executives is an excellent platform for companies to promote their brand profile, goals & secure market position. Given MIS' background in training, delegates typically comprise 90% 'end users' (e.g. CISOs, IT security managers, architects, network managers, auditors & system security professionals). All sponsorship packages include a number of free client places & discounts.

For more information, please contact Sara Hook on +44 (0)20 7779 7200, or email shook@mistiemea.com

Chief Information Security Officers' Roundtable

Tuesday 21st November 2006

Managing Information Security Risk for High Performance

There is often confusion & contradiction in how security is positioned within an organisation, in how investment is made & performance is measured. This roundtable will focus on the steps that need to be undertaken to gain management support & get to the bottom of the financial aspects of return on security investment (ROSI), including: the financial returns & ROSI approaches, details on how to collect & measure critical data. Benchmark the real experiences of other CISOs on the sound business reasons for carrying out risk assessments & recommended security risk tools. The sessions will be introduced by a short presentation from the given facilitator who will then lead group discussions & exercises.

Agenda

08:30 Registration & Coffee

09:00 Chairman's Welcome & Group Introductions

John Meakin, *Group Head of Information Security, Standard Chartered Bank* (UK)

09:15 Security Risk Management (SRM) Best Practices

- What is the current state of IT Security Risk Management?
- Challenges or barriers that must be addressed
- Defining SRM best practice - key processes, analytics & tools
- Steps for moving up
- Tried & tested applications & important lessons

Led by: Richard Hollis, *CEO, Orthus Ltd.* (UK)

10:15 IT Risk Management – Security Interaction with CTO, Chief Risk Officer, CIO, CEO, Legal

CASE STUDY

- What do we need to do to ensure that security is recognised as an enabler to high performance?
- A top to bottom approach
- Why your partners need to be onboard
- How to facilitate expanding your awareness program
- Embedding your security program in business processes

Led by: David Boye, *Chief Security Officer, Saxo Bank*, (DENMARK)

11:15 Morning Coffee Break

11:35 Ensuring that Security is a Business Enabler not a Barrier

CASE STUDY

Going on the web is a business issue & not just a technical challenge. A business integrated approach to risk assessment is essential to make sure that security is a business enabler & not a barrier. This inspiring case study will cover:

- Understanding your business risks
- Sources of threats
- Spectrum of security challenges
- Deter – avoid being a target
- Detect – how will you know
- Correct – what to do if all else fails

Led by: Dr. Frank Marsh, *Global Information Security Manager, British American Tobacco* (UK)

12:25 Lunch

13:45 Managing & Measuring Legal & Compliance Risks – The Law & Today's CISO

CASE STUDY

- Why do most compliance projects fail? Real life examples & possible remedies
- Overcoming conflicts in the law – e.g. between local data protection laws & the long-arm of S-Ox
- Integrating both security & privacy into outsourcing contracts

- How can you prioritise your compliance initiatives?
- What standards are the courts holding companies to when it comes to compliance?
- What can you do now to reduce potential company exposure?
- Tips for leveraging compliance to deliver maximum value

Led by: Michael Colao, *Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein* (UK)

14:45 Afternoon Coffee Break

15:05 Security as a Competitive Factor? Can We Measure It? Does It Matter? Getting Beyond Fuzzy Metrics & FUD

Good security is about good risk management. Learn more about how you can now better identify, visualise, & quantify information security risks.

- Positioning security within your organisation
- Making your business case & how to develop an action plan you can implement
- How to transform security risks from cost factors to investments
- Managing risk exposure & shared accountability
- Converging risk disciplines for security – how can this work?
- How do we bridge the gap between simple stakeholder expectations & the complex security reality?
- Measuring security governance frameworks
- Information risk management & analysis

Panelists:

David Boye, *Chief Security Officer, Saxo Bank*, (DENMARK)

Dr. Frank Marsh, *Global Information Security Manager, British American Tobacco* (UK)

John Meakin, *Group Head of Information Security, Standard Chartered Bank* (UK)

Richard Hollis, *CEO, Orthus Ltd.* (UK)

Michael Colao, *Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein* (UK)

Phil Pinder, *Executive Director, Management Controls Department, Goldman Sachs* (UK)

16:05 Roundtable Topic Tables

The group will now break into teams for specific discussions based on pre-agreed areas of priorities of the day. Each team will have the support of a facilitator & will present on the area to feed back to the main group following the session. This will include 30-minutes of group discussion, 20-minutes of developing the presentation to feedback, a 15-minute presentation of the key group findings from each team, followed by any questions.

17:35 Close of Roundtable

About the Roundtable Facilitators

David Boye, *Chief Security Officer, Saxo Bank*, (DENMARK) - was previously employed by Telia A/S as a quality management consultant & Hewlett Packard A/S as a security consultant. He currently holds the CISSP certification & is a qualified BS7799 lead auditor.

Dr. Frank Marsh, *Global Information Security Manager, British American Tobacco* (UK) - is a UK Member of the Council, & an elected member of the international Executive & Board of the Information Security Forum. He has over 25 years experience of IT & Information Management. Since 1994 he has specialised in the security of information, in all its forms both tangible & intangible. Frank has worked in a variety of environments including factory, both commercial & academic R&D, an operating company office & the global head office of British American Tobacco. In his current role Frank has global responsibility for the management of all aspects of information security, including providing advice to specialists in the IT, Security & other business functions within BAT globally. Frank also has responsibility for adding value through effective use of technology in support of Security operations worldwide. Another key challenge for Frank is the cross-training of IT staff & Security Managers to develop self-sufficiency, where it makes sense, in BAT's operating companies around the world. As part of BAT's commitment to public-private partnership, Frank has been a business representative at a number of meetings involving business, law enforcement & government representatives both in the UK & Europe.

John Meakin, *Group Head of Information Security, Standard Chartered Bank* (UK) - leads a global information security team at Standard Chartered Bank, one of the world's most international banks with 30,000 employees in more than 50 countries & a management team comprised of 70 nationalities. John has 18 years of experience in information systems security. His speciality is better modelling & managing the costs & benefits of security for large businesses, particularly enabling dynamic management & monitoring instead of traditional static prevention processes. Previously, John led systems security policy & strategy for Reuters, the Royal Bank of Scotland, Swiss Bank Corporation, & the investment-banking arm of Dresdner Bank. He has also provided information security consultancy support to several blue chip clients aimed at improving systems security & effectiveness. John has a Ph.D. in experimental solid state physics from Cambridge University, plays football regularly & builds computers in his spare time.

Michael Colao, *Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein* (UK) - has been with DrKw since 1999. He is the Director of Information Management. This role means that Michael is both the Global Head of Information Security for the Bank as well as the Global Head of Data Protection & Privacy. He has a strong side-interest in computer forensics & in the management of digital evidence. He graduated from the Massachusetts Institute of Technology in 1987 where he studied Mathematics & Computer Science. He has since lived in three continents & has lectured globally on security technology issues. Since 1996 has been working in Financial Technology in London.

Phil Pinder - has over 20 years experience in advising and training leading organisations in the audit of IT security, governance and control. Phil previously ran his own company before joining KPMG where he was responsible for advising clients on establishing sustainable processes to achieve compliance with multiple regulatory requirements, including Sarbanes-Oxley and Basel II. He has recently joined Goldman Sachs International as Executive Director in the Management Controls Division, responsible for auditing infrastructure, middleware and messaging services.

Richard Hollis, *CEO, Orthus Ltd.* (UK) - is a seasoned information security professional with over 25 years of private & public industry management experience. A Certified Information Security Manager (CISM), he possesses extensive "hands on" skills & experience in designing, implementing & managing comprehensive, cost-effective information security programs & architectures for hundreds of high-tech blue-chip companies across Europe. Richard is the Founder & Chief Executive Officer of Orthus Ltd. a European information security consulting firm headquartered in London specialising in rolling out efficient, product agnostic ICT security solutions. He also serves on several security technology company Boards & security industry advisory councils. A lifetime security professional, his career also includes serving as the Director of Security for Philips in Paris, Deputy Director of Security for the U.S. Embassy Moscow Reconstruction Project in Moscow & numerous sensitive security positions within the U.S. Government & Military in Washington D.C. & abroad. Richard has published numerous articles & white papers & has appeared providing commentary on various television channels. His expertise is regularly cited in national press & industry publications.



InfoSec World - Lapland 2006

Conference Day One

Wednesday 22nd November 2006

08:30 Coffee & Registration

08:45 Chairman's Opening

09:00 The Finnish Experience of Raising Awareness Around Security

KEYNOTE

This opening keynote will focus above all on the security training, awareness training activities & security management systems.

- Legislation
- Awareness planning & operations
- Security Instructions



Seppo Sundberg, *Chief Security Officer, Finnish State Treasury, Ministry of Finance (FINLAND)*

Mr. Sundberg has been a prominent member in the Government Information Security Management Board, VAHTI since 2000. The Ministry of Finance set this Board up for the co-operation, steering & development of government information security. Mr. Sundberg is responsible for co-ordinating & managing the security, including the Information Security, in the agency. Before joining The State Treasury in his current position, he served as the Chief Information Security Officer at the Population Register Centre, performing information security framework & guideline developments. The Population Register Centre received the Information Security Certificate, according to the BS 7799 standard, in 2002. He has background in personnel security, disaster recovery planning, wireless communication & digital signals.

09:40 The Future Of Security In The Context Of A Changing Business & Risk Landscape

- What is driving the need to change your security practices?
- What impact does this change have upon your security policies & technology?
- How do you engage your board, your risk & compliance



John Meakin, *Group Head of Information Security, Standard Chartered Bank (UK)*

10:20 Information Risk Management & Specific IT Security Challenges in an International Organisation

CASE STUDY

Preventing IT incidents & managing information risk at the WTO is an everyday challenge. Several case studies will show how the WTO approaches these challenges & employs innovative, pragmatic & efficient solutions, which can serve as inspiration for corporate executives.

- Global presence
- Diverse & mobile workforce
- Huge usability requirements
- Political stakes & "hacktivist" threats
- Administrative & cultural constraints

Dr. Thomas P. Braun, *IT Security Officer, World Trade Organization (WTO) (SWITZERLAND)*

11:00 Morning Coffee Break – Speed Networking

Participants are introduced to each other, which will give you the chance to meet everyone at the conference & exchange contact details. Please remember to bring your business cards!

11:20 Information Security & Open Source Strategy

CASE STUDY

- Open Source: what is it? Why do we use it?
- Experiences as a publisher & the security issues
- Exploding some myths about open source
- Identifying problems for the information security department
- Managing information not managing technology
- The regulatory problem
- How did we opensource it?
- What benefits have we accrued from opensourcing? At what costs?
- Does Open Sourcing work?
- A Risk-based approach



Michael Colao, *Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein (UK)*

12:10 Information Security Practices & Computer Crime Prevention

CASE STUDY

Computer crime is getting more professional & sophisticated. A normal good information security practice can help an organisation to prevent the risk in many ways. When an incidence occurs, an organisation can help the police investigation with a little planning & preparation in advance.

- Good information security practices are helping to prevent computer crime
- Getting prepared for computer crime prevention
- Steps to take when you suspect your organization may be a victim



Aku Hilve, *Chief Information Security Officer, Helsinki Police (FINLAND)*

12:50 Lunch

14:00 Protecting Customer Data & Identities - What Is The Reality?

- Who exactly is stealing identities?
- What tools & techniques are used?
- When did it become so easy?
- Where to find the data?
- Why create a fake ID: the benefits
- How to protect yourself & your company



Richard Hollis, *CEO, Orthus Ltd. (UK)*

14:30 Please Select Your Track

TRACK 1: Best Practice Information Security Management

14:35 The Human Factor: Opportunity or Threat for Information Security?

Regardless of the amounts spent on standard security solutions, all security policies are seeing the same phenomenon: a large portion of security (& insecurity) is in the hands of end users, who click on the wrong e-mail, write their passwords on pieces of paper, visit forbidden sites & give their credit card numbers to strangers. The issue of human risk prevention, perception, management & correction is the most complex one to handle in a global business security project.

- The human factor in the security puzzle
- Methodologies for assessment & management of insider's behavioural vulnerability



Vincent Bieri, *CEO, NEXThink S.A. (SWITZERLAND)*

15:10 How to Build a 24hr Information Security Service

CASE STUDY

This case study is based on a work group study of the Finnish Information Security Steering Board. When building a reliable 24/7 service there is much concern about personnel management & the technical environment for which the information security service is designed. The focus will be information security management. The study concerns how to build a 24hr information security service in governmental agency, but the same kind of questions arise when building a similar service in business.

Aaro Hallikainen, *Chief Security Officer, Finnish Police IT Management Agency (FINLAND)*

Mr. Hallikainen was the Finnish Police Data Security Manager from 2001 until 2004 & the Finnish police IT Management Agency's security manager 2005-2006. He has an M. Sc. in computer science, is a CISSP in good standing since 1999 & working in systems programming since 1981. He was on board of Finnish Information Security Association 2002-2004 acting as the CISSP contact person. He is a member of security management & information security sections of Finnsecurity ry, which is a registered security association in Finland.



TRACK 2: Special Focus: Identity & Authentication

14:35 .NET Identity & Authentication: The Developer's Point Of View

Speaker to be confirmed

15:10 Recent Trends in the Formal Verification of Cryptographic Protocols: Academic View

- The need to verify cryptographic protocols automatically or semi-automatically
- Theoretical approaches: process algebraic methods, strand space methods logics & hybrid methods
- Practical experiences, available software
- Conclusion: Still in the basic research phase or ready to apply?



Dr. Timo Karvi, *Professor, Computer Science Department, University of Helsinki (FINLAND)*

InfoSec World - Lapland 2006

Wednesday 22nd November 2006 continued

15:40 Preventing IT Security Breaches In TeliaSonera's Networks & Systems

CASE STUDY

- Telco industry specific laws & regulations & how government is setting requirements for information security in Telco business
- Utilising TeliaSonera internal CERT (Computer Emergency Response Team)
- Used processes to decrease risks in systems, networks & applications
- Using chosen IT-security measures as a tool & taking actions based on facts, not assumptions

Tommi Vainio, *Security Manager, Security Department, TeliaSonera Finland Oy*

16:00 Afternoon Tea Break

16:15 Holistic Information Security

KEYNOTE

The implications of lapses in information security are just beginning to be understood by corporates. Today, in addition to the productivity & competitive losses a company can incur, in several segments of industry – unwittingly – corporates could be abetting various kinds of misdeeds. In this session, Raghu Raman will use 'real' life examples to demonstrate how a corporate can come close to destruction due to lapses in its information security posture. At the tamer end, this leads to a loss of competitive advantage, & at the other, scrutiny from regulatory &/or internal security agencies. In addition to a commentary on how to recognise & curb infosec lapses in your organisation, this session will offer insights into what larger responsibilities corporates may want to consider towards the larger security environment.



Capt. Raghu Raman, *CEO, Mahindra Special Services Group & Principle Partner, DBS Solutions*

Capt. Raghu Raman has served the Indian Army for over 10 years during which he was a part of the elite Mechanised Forces. He did his computer studies in the Military College of Telecommunication Engineering and holds an Instructor's grading in Missile Guidance Systems, Weapons and Information Technology amongst others. He has been trained in the field of Hacking at Foundstone & is a member of the SCIP [Society of Competitive Intelligence Professionals]. Capt. Raman is a CISA (USA), CISSP & a certified BS 7799 lead auditor. Raghu Raman has been working in the field of Information Security since the last 16 years including stints with government security agencies & the United Nations. Capt. Raman has been a trainer & a speaker in the field of Information Security in numerous forums & he is also the author of several papers on the subject.

16:55 The Threat From Within - Top Vulnerabilities

This session will look at the risk of unauthorised access & misuse from within the organisation & the types of individuals & third-parties who may be responsible for their perpetration.

Often overlooked failings in policy, preventative & detective controls that facilitate such misuse will be discussed, followed by examples of countermeasures & their relative strengths & weaknesses.



Phil Pinder, *Executive Director, Management Controls Department, Goldman Sachs (UK)*

Phil has over 20 years experience in advising & training leading organisations in the audit of IT security, governance & control, & previously ran his own company before joining KPMG where he was responsible for advising clients on establishing sustainable processes to achieve compliance with multiple regulatory requirements, including Sarbanes-Oxley & Basel II. He has recently joined Goldman Sachs International as Executive Director in the Management Controls Division, responsible for auditing infrastructure, middleware & messaging services.

17:35 - Is Compliance Translating Into Improved Security? Challenges for Today's CISO

EVENING PANEL DEBATE & DRINKS RECEPTION

- How to exploit compliance overlaps & conflicts (e.g. Privacy Laws & the Sarbanes-Oxley Act)
- Impact of emerging EU privacy laws on the CISO
- How can IT best support your enterprise-wide compliance effort? What does it all come down to?
- Developing a risk-based approach to IT/IS strategy to achieve compliance goals & strong governance
- Turning security compliance into value
- How much compliance is enough? What new laws are on the horizon?

Panelists:

Arto Kangas, *Coordination Manager, Information Security Manager, Finnish Insurance Data Ltd, Board Member, Finnsecurity ry & Board Member, Finnish Information Processing Association*

Dr. Frank Marsh, *Global Information Security Manager, British American Tobacco (UK)*

John Meakin, *Group Head of Information Security, Standard Chartered Bank (UK)*

Marinó G. Njálsson, *Consultant, Betri akvordun, (ICELAND)*

Mark Concar, *Director Data Security, American Express (UK)*

Michael Colao, *Director, Global Head of Information Security, Dresdner Kleinwort Wasserstein (UK)*

Capt. Raghu Raman, *CEO, Mahindra Special Services Group & Principle Partner, DBS Solutions*

20:00 Close of Day One

InfoSec World - Lapland 2006

Conference Day Two

Thursday 23rd November 2006

8:30 Coffee & Registration

08:55 Chairman's Opening

09:00 Information Security & Change Management

KEYNOTE

- Change management & readiness to face change
- Good communications & understanding the group dynamics of change resistance
- Information security needs to be taken in account when building the processes
- What works best on paper –process is not going to work in practice if people don't follow the secure process willingly
- Outsourcing actions & processes – but maintaining responsibility of good information security principles
- Planning in advance for outsourcing & contracts based on business continuity issues

Ari Uusikartano, *Director for Information & Documentation, CIO, Ministry for Foreign Affairs, Finland*

Mr. Uusikartano is an active member of The Finnish Government Information Security Management Board VAHTI, which cooperates, steers & develops government information security in Finland. Ari has chaired many VAHTI work groups & is highly experienced information security professional.

09:40 Immune System Inspired Computer Security

INNOVATIVE TECHNOLOGY KEYNOTE

The 'natural' immune system is very good at what it does, so an 'artificial' immune system seems an ideal approach to protect computers. Unfortunately, early approaches based on so called 'negative selection' have only had limited success. However, immunologists have in the last few years fundamentally changed their minds about how the immune system works & a new 'Danger Theory' emerged. The question is - can artificial immune systems built around this new theory provide better protection? The answer seems to be yes....

- The need for adaptive / context aware anomaly detection
- Brief overview of relevant immunology
- Previous immunological approaches (negative selection) - how they work & what they could & could not do
- New immunological approaches (Danger Theory) - how they work & what is improved on previous methods
- Outlook for immune inspired computer security - what they might do in the future



Dr. Uwe Aickelin, *Senior IT Security Researcher, University of Nottingham (UK)*

10:20 White Hat / Black Hat Debate: What are Acceptable Ethics in Cyber-Space?

PANEL DISCUSSION

Determining who is a criminal & what constitutes a "crime" are still debatable topics in cyberspace, largely because the ethics & morality of a young cyberspace society are still being hammered out, plus the laws in the digital world have not caught up with the laws in the physical world.

- Do white hats provide a service or a disservice?
- Should security researchers who find vulnerabilities report them, or is the risk of prosecution too great?
- If the white hats hang up their hats, what will the ramifications be?
- How are the physical worlds & electronic worlds related?

Panelists:

John Meakin, *Group Head of Information Security, Standard Chartered Bank (UK)*

Marco Ricca, *Associate Founder & Director, Ilion Security SA (SWITZERLAND)*

Richard Hollis, *CEO, Orthus Ltd. (UK)*

Vincent Bieri, *CEO, NEXThink S.A. (SWITZERLAND)*

11:10 Morning Coffee Break



InfoSec World - Lapland 2006

Thursday 23rd November 2006 continued

TRACK 1: Infrastructure & Network Security

11:25 Software Security: Why It Fails & What Can We Do About It?

Software security audits & sending programmers to hacking courses are not enough to create secure software. Security must be "baked in" to the software during the whole software development lifecycle. Presentation explains the current security challenges & discuss about findings from security evaluation of a software development process. Recommendations to enhance the SDL are presented.

- Why software security fails
- Risk analysis based security
- Findings from security evaluation of a software development process
- Secure software development lifecycle

Jari Pirhonen, *Head of Security, Samlink Ltd. & President, Finnish Information Security Association (FISA) (FINLAND)*

Mr. Pirhonen, M.Sc., CISSP, CISA, is responsible for corporate security & customer security services. Samlink is a Finnish financial services provider. Jari has over 10 years experience in different areas of information security & currently he is broadening his knowledge towards corporate security issues in general. Because of Jari's application development background, software security has been one of his pet topics for several years. Jari is President of Finnish Information Security Association (FISA) & is active on other security forums as well. Jari is an experienced instructor & lecturer.

12:05 Wireless LAN Security Challenge in Real World

CASE STUDY

- Rock, Paper, Scissors - the CIA triad
- Overview of wireless LANs
- Our wireless LAN risk assessment - tailored solutions with tightest security
- Wireless data protection
- User and host authentication with 802.1x
- Hide and seek with certificates
- Lessons learned

Petri Ala-Annala, *Chief Information Security Officer, Helsinki Energy (FINLAND)*

14:00 Professional Hacking, Myths & Realities: A Step-By-Step Case Study

LIVE HACK

Organised, financed & targeted hacking attacks are nowadays carried out by governmental, private & criminal organisations for lucrative or political purposes (intelligence services, organised crime, industrial espionage, etc.). This presentation will attempt to present the main differences between small, common cyber-delinquency & high-profile criminality. Live demonstrations shall illustrate the principles exposed.

- Professional hackers: intelligence services, organised crime, industrial espionage
- High-profile criminality vs. small cyber-delinquency
- Targeted & financed attacks vs. mass, random offenses
- Operational cyber-risk theory outline
- Managing high-profile threats

Marco Ricca, *Associate Founder & Director, ilion Security SA (SWITZERLAND)*

15:00 Digital Rights Management (DRM) - Web, E-Commerce & Database Applications

Technologies & methods for controlling access to digital data & tracking their use. DRM supports mandatory access controls through cryptographic protocols & other protection measures. Producers of entertainment content, software & other forms of intellectual property use DRM technologies to limit the ability of both consumers & would-be thieves to copy & redistribute intellectual property.

- What is the next phase in the evolution of this technology?
- Protect consumer data from unauthorised use or redistribution?

Speaker to be Confirmed

12:45 Lunch

TRACK 2: Security Compliance & Policy

11:25 Mapping S-Ox Corporate Governance Legislation Against Best Practice in IT Security

CASE STUDY

- Implementing the latest regulations into your information security framework
- Building a cost effective information security program using ISO 17799 & equivalents
- Analysing the IT security status
- Defining a corporate information security policy
- Developing a framework for information security
- A hierarchy of policies, standards & guidelines: from abstract to technical measures
- Managing an information security management system for compliance
- Realising Basel II & Sarbanes-Oxley: the information security perspective

Mark Concar, *Director Data Security, American Express (UK)*

Mr. Concar has worked within the Financial Services Industry for the past 21 years, in Systems Development, as Internal Audit Director, & now in Data Security. Mark is responsible for Data Security within American Express Bank & the International Card Operations business units of American Express Bank. Working with the business, Mark & his team ensure that the technologies units & the company's multiple vendors comply with the various security policies & standards of American Express & are aware of the regulatory requirements towards security of each of the markets in which American Express is present.

12:05 Education & Awareness of IT Security Risks - Future of IS Professionals

CASE STUDY

- Target audience - whom are they & what needs for awareness do they have?
- Tools for spreading the word
- Maintaining awareness considering a moving threat picture
- Motivational factors: rewards & punishments
- Considerations in linking early warning information to the IT organisation

David Boye, *Chief Security Officer, Saxo Bank, (DENMARK)*

14:00 Being Legal - Tools & Tips to Help You Complying With Legislation From Across The World

CASE STUDY

This presentation will look at the challenges of identifying & complying with laws for organisations that operate across the world. It will present a process developed specifically to help information security professionals comply with different laws & will introduce a browser based tool that can be used to identify what laws have information security relevance.

Andy Jones, *Senior Project Manager, Information Security Forum (UK)*

15:00 IT Governance & Compliance Challenges for CISOs

Most companies face an enormous challenge of complying with various external requirements. Data privacy, document retention, operational risk management, Sarbanes-Oxley, & all kinds of supervisory authorities are taking more & more time from CISOs. Most feel this as unwanted problems instead of seeing it as a way to improve the competitiveness of their company. Using COBIT in combination with ISO 17799 has turned out to be a powerful & successful tool to solve many of the compliance issues involving information security management. You will focus on these points as well as looking at common external requirements.

Marinó G. Njálsson, *Consultant, Betri akvordun, (ICELAND)*

15:40 Afternoon Tea Break

16:30 The Cryptographic Compliance - Good or Bad?

Cryptology is not something Corporate Information Security Officers worry about as long as their company complies with the common industrial standards, implements well known best practices, & follows the recommendations of the usual governmental agencies. It becomes a bit of a concern, however, when the standards fall apart, there are no obvious best practices to follow, & the trusted agencies don't know what to recommend either or make recommendations that could prove hard to follow. In this presentation several recent cryptology-related events will be discussed that could make one think that there is reason for concern: the recent hash cryptanalysis, the vulnerabilities it leads to & their potential implications, & the Suite B of cryptographic protocols that was announced by the U.S. National Institute for Standards & Technology.

- Are there best practices in cryptography?
- Trusted agencies recommendations: how does one follow?
- Recent cryptology-related events & their implications: reasons to concern?

Dr. Arjen Lenstra, *Head of the ISIS Security Center, EPFL, Former Senior Security Researcher, Lucent Technologies', Former Security Officer, Citigroup (SWITZERLAND)*

17:10 Convergence of Federated Identity Management: Balancing Security & Privacy?

PANEL DISCUSSION

- What Are We Trying To Achieve?
- Identity federation: is it time to move on now?
- How can Identity Management improve other business services?
- Towards Single Sign-On (SSO) across identity domains
- Overcoming ROI obstacles & longer term business challenges
- Emerging technologies used for ID management

Panelists:

Andy Jones, *Senior Project Manager, Information Security Forum (UK)*
Cédric Renouard, *Associate, ilion Security SA (SWITZERLAND)*

- What are the top authentication weaknesses?
- Web Services framework & federated identity update
- Challenges involve documenting business practices & defining who gets access to what
- Top tips to avoid inadvertently exposing sensitive data to unauthorised parties
- What were the most challenging issues in the implementation of your identity management solution?

David Boye, *Chief Security Officer, Saxo Bank, (DENMARK)*

Mark Concar, *Director Data Security, American Express (UK)*

18:00 Close of Day Two

The Security Threat Horizon Roundtable

Friday 24th November 2006

Keeping Your Data Safe

Group-discussions will be introduced by a short presentation by the given facilitator, who will then lead the debate & exercises.

Facilitated by:

Andy Jones, Senior Project Manager, Information Security Forum (UK), **Cédric Renouard**, Associate, ilion Security SA (SWITZERLAND), **Marco Ricca**, Associate Founder & Director, ilion Security SA (SWITZERLAND), **Phil Pinder**, Executive Director, Management Controls Department, Goldman Sachs (UK), **Richard Hollis**, CEO, Orthus Ltd. (UK)

Agenda

07:45 Coffee & Registration

08:05 Chairman's Opening & Group Introductions

08:10 Reporting Key Findings of the Information Security Forum Threat Horizon Report

The Information Security Forum will unveil the key findings of the 2006 report, "Threat Horizon", based on the input of around 100 global organisations. The group will then benchmark these results against current operational priorities & strategic challenges – which will then form the basis for the day's discussions & objectives.

Andy Jones, Senior Project Manager, Information Security Forum (UK)

09:10 Uncovering Identity Theft & Fraud Techniques

It is easy & lucrative to steal or manufacture an identity these days. This session details the steps criminals take to steal existing or establish fake identities. Learn the steps to take to obtain a passport, drivers' license or national health care card. Know how it's done & understand what you can do to protect your identity!

- Who exactly is stealing identities?
- What tools & techniques are used?
- When did it become so easy?
- Where to find the data?
- Why create an fake ID: The benefits
- How to protect yourself & your company

Led by: Richard Hollis, CEO, Orthus Ltd. (UK)

10:10 Morning Coffee

10:30 VoIP: What Level of Security Can be Ensured?

- Myths & Realities of VoIP (In)Security
- VoIP definition & concepts
- Attack myths & realities
- Security solutions myths & realities
- Future & outlook (threats, standards, solutions, challenges)

Speaker to be confirmed

11:30 Managing the Risks of a Mobile Workforce: Laptops & PDAs

Laptops, mobile phones & PDAs have become a major risk factor for organisations. Yet business depends on mobility & mobile devices are here to stay. In this session you will scrutinise the inherent risks in securing executive laptops & PDAs & gain real-world tips for making mobility secure.

- Is there an increased mobile phone malware threat?
- Laptop security: encryption, lock-down, & more
- PDA risks & exposures
- Executive scams: at airports & on the road
- Key tips for controlling data with a mobile workforce

Cédric Renouard, Associate, ilion Security SA (SWITZERLAND)

Marco Ricca, Associate Founder & Director, ilion Security SA (SWITZERLAND)

12:30 Lunch

13:00 Hackers, Malicious Coders & Customer Data Breaches – The Latest Threats

- Targeted vs. random hacking attacks
- Full disclosure vs. anti disclosure
- Ten things they don't teach you about being a CISO
- The threat from within – top 10 vulnerabilities
- Client-side attacks & Trusted Computing

Panelists:

Andy Jones, Senior Project Manager, Information Security Forum (UK)

Cédric Renouard, Associate, ilion Security SA (SWITZERLAND)

Marco Ricca, Associate Founder & Director, ilion Security SA (SWITZERLAND)

Richard Hollis, CEO, Orthus Ltd. (UK)

Phil Pinder, Executive Director, Management Controls Department, Goldman Sachs (UK)

14:10 Responding to a Security Breach

Panelists:

Andy Jones, Senior Project Manager, Information Security Forum (UK)

Cédric Renouard, Associate, ilion Security SA (SWITZERLAND)

Marco Ricca, Associate Founder & Director, ilion Security SA (SWITZERLAND)

Richard Hollis, CEO, Orthus Ltd. (UK)

Phil Pinder, Executive Director, Management Controls Department, Goldman Sachs (UK)

15:10 Close of Roundtable

15:10 Optional Networking Activity

Reindeer Herding & Dog Sledding

From the hotel in Rovaniemi, the group travels by car to the Reindeer Park at the Arctic Circle. After harnessing a reindeer, we will then drive through the snow-covered forest. Travelling by reindeer is a unique way to experience the nature of Lapland & find our way to the Husky Farm. The arctic huskies are anxious to take the group for a short ride as soon as we arrive. After the ride, we have time to get a closer view of the huskies' life & training. Hot juice & a light meal typical of the region, is served by open fire. The group then returns to the Reindeer Park with reindeer. Because of the group size, half of the group travel by snow mobile & half by reindeer (we will then change transportation modes coming back). Transportation by car to the hotel. Snow cannot be guaranteed in November therefore MIS reserve the right to change the programme accordingly if there isn't any snow.

Supported by

Secretariate of Finnish Information Security Steering Group: Lapland - The Government Information Security Management Board VAHTI for cooperating, steering & developing Government information security. The results of VAHTI cooperation are also widely utilised in local government, private sector & in international cooperation as well, besides the Finnish Government.

ilion is a company based in Geneva, Switzerland, that specialises in information risk assessments, & mitigation strategies. The company is the only information risk pure-player in Switzerland, & is leading in its sector. It mainly works with banks, governmental/military organisations & multinational corporations: it helps them deal with the threats posed by high-level, organised & financed hacking attacks (carried out by foreign states, intelligence services, organised crime, industrial espionage, etc.).

NEXThink is a pioneer in the new & promising market segment of "Insider Threats Management" (ITM). NEXThink develops & markets REFLEX, an Endpoint Behaviour Management solution based on research initially conducted at the Artificial Intelligence Lab of the Swiss Federal Institute of Technology (EPFL) in Lausanne, Switzerland. REFLEX is a real time, self-learning, plug & play technology for an accurate Behaviour-based detection of security policy violations. REFLEX is especially tailored to manage behavioural vulnerabilities inside the corporate environment (identity thefts, misconfiguration, misunderstanding, mistakes, unawareness). The interactive phases of the NEXThink PDA (Policy Deployment Assistance) methodology help to deliver accurate and faster technical audit, to validate security policy & to measure the impact of awareness programs. The REFLEX solution & PDA methodology help to better control Information Security Management System (ISMS) efficiency. More information: www.nextthink.com

TietoEnator is consulting, developing & hosting its customers' digital businesses. TietoEnator is among the leading architects in building a more efficient information society. With over 15 000 experts, we are one of the largest IT services providers in Europe. Our leading-edge know-how is geared towards developing innovative IT solutions that realise & digitalise the visions of our customers. We work in close partnership helping them to manage & run their business better. We've chosen to focus on areas where we have the deepest industry expertise. The principal ones globally are banking, telecom, healthcare & forest. In these areas, we work hand in hand with many of the world's leading companies & organisations. We are growing with them & are now active in more than 25 countries. TietoEnator's shares are listed on the HEX Helsinki Exchanges & Stockholm'sbörsen. www.tietoanator.com

Media Partner

SecurityPark.net is the leading online News portal for the Security industry, with over 250,000 readers every month. Security Park publishes industry & product News on a daily basis, across the complete range of Security products & services: access control, biometrics, alarm systems, CCTV, computer / IT / network security, mobile security, manned guarding, perimeter protection, physical security, remote monitoring & surveillance. Security Park also publishes Security case studies, white papers & market reports, & provides a free job forum & classifieds service to security professionals. Please link to www.SecurityPark.co.uk





InfoSec World - Lapland 2006

21st - 24th November 2006, Rovaniemi, Lapland, Finland

EMT 2037

WEB

Registration Options

All Inclusive Package:

Conference, Roundtables & Snow Networking Activity (21st – 24th Nov) GBP £1,795

Other Options:

Conference & CISO Roundtable (Information Risk) (21st – 24th Nov) GBP £1,495

Conference & Security Threat Horizon Roundtable (22nd – 24th Nov) GBP £1,495

Conference Only (22nd & 23rd Nov) GBP £1,195

CISO Executive Roundtable Only (21st Nov) GBP £595

Security Threat Horizon Roundtable Only (24th Nov) GBP £595

Optional Extra - Snow Networking Activity (Evening 24th Nov) GBP £50

Special Group Savings Scheme. Phone for Details. Discounts cannot be used in conjunction with each other. Only one discount applies.

CPE Credits Available

To maintain Certified Information Systems Auditor TM (CISA®) & CISM certifications, ISACA's continuing professional education (CPE) policy requires CISAs & CISM's to earn 120 CPE credit hours over a three-year period. Attendees can earn up to 32 CPE credits by attending the Conference (18 CPE hours for the conference and an additional seven CPE hours for attending each day of an optional roundtables). For additional ISACA education opportunities, please visit the ISACA web site at www.isaca.org/conferences

Registration Information

The Conference Venue: The Scandic Hotel Rovaniemi, (Rovaniemi - Finland, Lapland) Koskikatu 23, Rovaniemi, 96200, Finland

Telephone: +358 (0)16 4606000 Fax: +358 (0)16 4606666

Scandic Rovaniemi welcomes you to Lapland. In the Rovaniemi area you'll be able to see all the wonders of Lapland, while the Arctic Circle & Santa Claus Village are only 8 km north of the hotel. Scandic Rovaniemi is located in the very centre of Rovaniemi, within walking distance of all services in the city. www.scandic-hotels.com/rovaniami

Room Prices: IBR (MIS Training Venue agency has negotiated rates for conference participants as follows:

68 euros per night (double room for sole occupancy)

83 euros per night (double room for double occupancy)

Please contact IBR for further information about the hotel & discounted rates www.ibr.co.uk/mis,

Tel: +44 (0)1332 285521 Fax: 0845 330 4982 (UK only) +44 (0)1332 287613 (outside UK)

Cancellation Policy: Should a delegate be unable to attend, a substitute may attend in his or her place. A credit card or refund, minus 10% administration charge, is available if written notification is received by 31st October 2006. Thereafter, no refunds will be given. MIS reserves the right to change or cancel this program due to unforeseen circumstances.

5 Easy Ways to Register

Tel: +44 (0)20 7779 8944

Fax: +44 (0)20 7779 8293

Email: mis@mistiemea.com

Web: www.mistieurope.com

Mail: Guy Cooper, MIS Training, Nestor House, Playhouse Yard, London EC4V 5EX UK

Customer Information

(please print or attach business card)

Title First name Surname

Title/Position Organisation

E-Mail Address (Required)

Address

Country Postcode

Telephone Fax

The information you provide will be safeguarded by the Euromoney Institutional Investor Plc. group whose subsidiaries may use it to keep you informed of relevant products and services. We occasionally allow reputable companies outside the Euromoney Institutional Investor Plc. group to contact you with details of products that may be of interest to you. As an international group we may transfer your data on a global basis for the purposes indicated above. If you object to contact by telephone , fax , or email please tick the relevant box. If you do not want us to share your information with other reputable companies please tick this box

Payment Method - Pay Online at www.mistieurope.com

(all fees must be paid in advance of the event)

Cheque enclosed Please invoice my company PO# (payable to MIS Training)

Please debit my credit card AMEX VISA MasterCard

Card Number Expiry

Cardholders name Verification Code

Please include billing address if different from address given

Please note that in completing this booking you undertake to adhere to the cancellation and payment terms listed below

Signature Date

Approving Manager Position

Please Send Me Information on:

Identity Management Summit 2007 (at WebSec), 26th & 27th March 2007, London, UK

WebSec 2007, 28th, 29th & 30th March 2007, London, UK

4th Annual CISO Executive Summit & Roundtable, 6th, 7th & 8th June 2007, Nice, France

Nordic Fraud & Anti-Corruption Summit, 23rd – 25th May 2007, Copenhagen Denmark

To Register Call +44 (0) 20 779 8944, Fax +44 (0) 20 7779 8293, Email: mis@mistiemea.com or Visit www.mistieurope.com