8th Annual

WEBSEC 2005

i-SECURITY WORLD CONFERENCE

Driving information security in today's web-enabled enterprise

Gain 37 CPE Points!

Case Studies from:

- Alliance & Leicester plc.
- Barclays Group
- Bradford & Bingley plc.
- BT
- Cable & Wireless
- European Patent Office
- Experian
- Genworth Financial, Payment Protection Insurance
- High Tech Crime Unit
- Homeloan Management Limited
- MCI
- Merrill Lynch International
- Munich International Airport
- London Borough of Newham Council
- NMBS - Belgian Railway
- Reuters
- Royal Mail
- Standard Chartered Bank
- TIM Hellas Telecommunications
- Vodafone
- Winterthur Insurance Group
- Wolverhampton City Council
- World Intellectual Property Organization

3 Tracks, 3 Days, 5 Debates, Over 50 Speakers on the Top Web-Based Security Trends & Tactics, including:

- Live Hacking & Auditing Demos: Web Apps, VPNs, Wireless
- Hear Patch and Identity Management Strategies that Really Work!
- New Case Studies on How to Ensure a Reliable and Undisrupted Network
- Tried and Tested Tools to Wipe out those Hackers, Spammers, Spoofers and Phishers

Conference
15th, 16th & 17th March 2005
London, UK

Workshops
14th & 18th March 2005

Supported by:

CLUSIS · Information Security · INFOSECURITY MAGAZINE · ISACA UK Chapters · virus BULLETIN · Information Security Bulletin · INFORMATION SECURITY FORUM · ISSA · MAG SECURS

Sponsored by:

F-SECURE

Organised by:

MIS TRAINING

Register NOW at www.mistieurope.com

WEBSEC 2005 Optional Workshops

08.30 Coffee & Registration • 09.00 Workshop commences • 10.30 Morning coffee • 12.30 Lunch • 15.30 Afternoon tea • 17.00 Close

Pre-Conference Workshops: Monday 14th March 2005

Workshop 1: Practicalities of Information Security Management **

Led by: **Charles V. Pask**, *Managing Director,* **ITSEC Associates Ltd**

Information security is only as weak as the way it is managed. As a manager responsible for delivering trusted services across the IT environment, get up to date with the security elements that make up the Enterprise Security Model. The technical aspect of information security is only one side of the story. Best practice information security needs strong management to understand the bigger issues, establish good security policy and practice, and plan for a rapidly changing future. This workshop is designed to give the information security manager, the tools necessary to create, mould and deliver a consistent and cost-effective quality information security service to your organisation.

What will you learn?

- Key current issues in information security management
- How to implement and manage a security programme
- How to develop an organisation-wide security culture
- Policies, standards, procedures, and guidelines: creating a strong foundation through policy; distributing and maintaining policies, standards, and procedures; specific policies for Internet information security
- Performing a risk analysis of your network environment
- Surveying the security features of: automated policy managers; intrusion detection systems; remote access methods; add-on security products
- How to identify common information security vulnerabilities and tools
- Detecting and reacting to computer crime, accidents and errors
- Contingency planning and reputation management
- Legislation and standards
- The future of information security in the organisation

About Your Workshop Leader: **Charles Pask** is responsible for delivering global IT security and IT audit services, including public training courses, in-house training courses, conferences, symposiums, and consulting. Previously, he was a Director with MIS Training, and Director of Information Security Institute (ISI) European and Middle East e-Security Services. Mr. Pask has over 20 years' experience in IT, IT audit, and IT security, and was the Information Security Manager for Alliance & Leicester plc prior to joining MIS. Mr. Pask has been a member of the ITSEC Common Criteria team working with the DTI, and a committee member of the APACS Security Advisory Group and the LINK Security Group.

Workshop 2: Network Security for Today ***

Led by: **Vincent Bieri,** *Security Marketing Manager (EMEA),* **Cisco Systems**

What will you learn?

- Basics of attacking today's networks
- How to secure networks with firewalls
- Facts behind host and network intrusion detection/prevention systems
- VPN technology and architectures for secure communications
- Specific network security concepts, security of wireless, voice, storage, switches and routers
- Security realities, trends and myths: open discussion time

About Your Workshop Leader: **Vincent Bieri** has worked for Cisco for the last 7 years in various technical and business development positions. As part of this role Vincent developed a number of training programmes for Cisco's customers, partners as well as Cisco employees. Vincent holds an Engineering degree in Computer Science from University of Applied Science of Fribourg in Switzerland.

Workshop 3: Vulnerability Testing Tools & Techniques ***

Led by: **Ken Cutler**, *Vice President - Information Security,* **MIS Training Institute**

Effectively auditing today's network technology can be a daunting challenge. In this intensive workshop, you will learn how to systematically enumerate and test the security of important hotspots within a complex network. Through a series of detailed case studies and demonstrations, you will receive the necessary guidance to build a versatile and powerful cyberspace audit toolkit to test for security vulnerabilities that are frequently exploited by hackers and other intruders.

What will you learn?

- How to define audit objectives and develop an overall work plan for external and internal network vulnerability testing
- Resources for keeping current on the latest vulnerabilities and hacker exploits
- How to select the necessary hardware and software to build an effective vulnerability testing workstation
- Through live demos: Tools and techniques to enumerate and test the security of wired and wireless networks
- Strategies for effective corrective action programs to address the large number of vulnerabilities detected in most organisations

About Your Workshop Leader: **Ken Cutler** is the Vice President of Information Security at MIS Training Institute, where his responsibilities include directing MIS' infosecurity public training programs and setting the strategy for MIS' information security certificate programs. Mr. Cutler was formerly with American Express Travel Related Services where he had world-wide responsibilities for security standards, awareness programs, risk assessments, and security consulting services. Previously, he served as the CIO for Moore McCormack Resources. He also headed up the security program at Martin Marietta Data Systems.

Technical depth is indicated for each workshop as follows:
Low * Medium ** High ***

Post-Conference Workshops: Friday 18th March 2005

Workshop 4: Security Governance, Maturity and Metrics **

Led By: **George Thompson**, *Director IRM Security and Continuity* & **Nick Bleech**, *Principal,* **KPMG LLP (UK)**

The workshop will take an in-depth look at security governance, its elements and relationships and how governance within your organisation relates to the Information Security Management System. You will investigate what is required for security governance to be effective and provide benefits to the business.

What will you learn?

- What steps are required to achieve security governance
- How to use an understanding of security maturity to develop appropriate security programmes for your organisation
- How to develop metrics for measuring the effectiveness of governance and security operations in your organisation

About Your Workshop Leaders: **George Thompson** has extensive advisory experience in security management programmes, processes and architectures. With 14 years experience in the security and networking arena, George works with major clients creating security management frameworks and the strategies for the implementation. George's security experience covers the spectrum of security including corporate security policy and governance, IT security policy, procedures and standards, security reviews of process and technology, application security assessments, security architecture development and deployment.

Nick Bleech is Principal Advisor for Security Management within the firm's Technology Advisory Services practice, providing authoritative advice and challenge on strategic security issues to Heads of Security and IT in leading UK and International clients. He has 25 years IT experience, 18 in information security, with extensive security experience in Financial Services, Energy, Manufacturing, Government and Telecommunications. He is a Board member of the Jericho Forum, and a co-author of the European ITSEC, which was a precursor to the ISO Common Criteria for Information Security.

Workshop 5: Enforcing Internal IT / Web Surfing Policy's: How To Design And Implement A Clear Web Usage Policy **

Led by: **Jeremy Barker,** *Technical Director,* **Orthus Ltd**

This workshop will include a hands-on session to show the effectiveness of current network and desktop policy enforcement tools. You will leave with an in-depth understanding of the aspects of privacy, security, and liability that need to be covered in policies and tactics to be able to develop a security policy and process architecture to support your organisation's web applications.

What will you learn?

- What you must prevent to be compliant with current legislation
- How to monitor and enforce internet and desktop policies
- How to prevent staff from carrying out on-line transactions
- How to prevent staff from using unauthorised devices on your network
- Proving it!

About Your Workshop Leader: **Jeremy Barker** gained experience as an analyst programmer in commercial security applications, before moving into systems programming. He joined Digital Equipment Company (DEC) as a pre-sales security software specialist, progressing to Senior Consultant and after 5 years he became Manager of the UK Benchmark Center in DEC UK Headquarters. At the forefront of technology with a heavy involvement with customers at the highest technical level for a further 5 years, Jeremy co-founded speed-trap a security policy management software solution. He was the creator of the award winning technology behind Prophet, speed-trap's flagship product. Jeremy is responsible for several patent applications, three of which have already been granted.

Workshop 6: Hacking & Auditing Web-based Applications ***

Led by: **David Rhoades**, *Principal Consultant,* **Maven Security Inc.**

From sign-on to sign-off, and everything in between, this workshop goes beyond typical web server configuration tips to show you how to test your web-based application for security flaws ranging from the subtle to the severe. Step-by-step you will go through how to identify security weaknesses for web-enabled services that could be exploited by remote users. Some of the key areas covered include:

- Information Gathering Attacks - how hackers read between the lines• User Sign-On Process - user-name and password harvesting, resource exhaustion
- User Sign-Off Process - are users really signed off?
- OS & Web Server Weaknesses: buffer overflows and default material
- Encryption: finding the weakest link
- Session Tracking: URL rewriting, basic authentication, and cookies; strengths and weaknesses; session cloning, IP hopping, and other subtle dangers; a recipe for strong session IDs
- Authentication - server, session, transactional
- Transaction-level issues: hidden form elements; unexpected user input; GET vs. POST; JavaScript filters, Improper Server Logic

About Your Workshop Leader: **David Rhoades** is a principal consultant with Maven Security Inc., which is headquartered outside Washington DC and provides information security assessments and training. David's expertise includes web application security, network security architectures, and vulnerability assessments for networks and telecommunication systems. Past customers have included domestic and international companies in various industries, as well as various U.S. government agencies. David has been active in information security consulting since 1996, when he began his career with the computer security and telephony fraud group at Bell Communications Research (Bellcore).

To register: email **mis@mistiemea.com** or fax **+44 (0) 20 7779 8293**

WEBSEC 2005 Conference Programme
Day One: Tuesday, 15th March 2005

08.30 Coffee and registration

09.00 Opening Remarks From The Chairman

Ken Cutler, *Vice President - Information Security*, **MIS Training Institute**

09.10 Keynote: Tearing Down The Walls *

In a connected world, companies need to be able to share data with customers, partners and suppliers. They also need to allow more flexible modes of connection into their own networks from a variety of connecting systems. As a result the traditional 'hard perimeter' is no longer an appropriate approach to security. In this plenary session, John Meakin, a founder member of the Jericho Forum, will show you how this new group is working to influence vendors to provide the security solutions that you will need over the next few years. Leave with a better sense of the implications this will have short-term and longer-term for security within your organisation.

John Meakin, *Group Head of Information Security*, **Standard Chartered Bank**, *Co-Founder*, **Jericho Forum**

Technical depth is indicated for each session as follows:
Low *
Medium **
High ***

10.00 Keynote: The State of Information Security and the Nation *

This session will discuss from an independent view on the role of the information security services and software/hardware industry in helping business with protection and privacy. You will learn that far from just selling software, hardware and services, consulting firms and providers must help their clients meet their business objectives by providing help with more than just advice, training, change management and education, integrated and interoperable environments - an holistic approach!

Ray Stanton, *Global Head of Security Practice,* **BT**

10.30 Morning Coffee Break

STREAM 1: Policy, Risk & Governance

Legal, Governance & Compliance Challenges

10.45 Security & Sarbanes-Oxley: How To Implement A Formal Control Environment *

CASE STUDY

Discover how this leading insurance group implemented formal IT controls within a large IT organisation. You will hear proven tips on how to realign your security strategy to meet this law.

- Project setup and implementation issues
- What where the challenges? How can you learn from these?
- How can you take advantage of the business opportunities?

Claus Norup, *Head Risk Management & International IT,* **Winterthur Insurance Group**

11.45 Basel II: How To Tackle The Real Information Security Impacts *

CASE STUDY

The lessons for the management of risk and information security professionals should be learned now, and projects will undoubtedly act as a framework for the risk management in other areas. Hear how you can best prepare your IT security systems to meet these requirements.

- Novel approaches to preparing for Basel II
- How do you integrate this into the overall IS infrastructure?
- Databases for both internal and external current and historical data
- Assess threats and vulnerabilities in the existing IT environment: applications, networks, operational procedures and policies
- What are the regulatory requirements of Basel II relating to internet and web security?

Speaker to be confirmed

14.00 Successfully Implementing The Latest Regulations Into Information Security Management: S-OX, Basel II

PANEL

- Sarbanes-Oxley and IT security: Best practice approaches
- Are you ready for similar EU governance directives?
- Top tips for dealing with pushy auditors
- Provisions you can make for an ever-changing regulatory landscape
- Is compliance a blessing in disguise?

Facilitator: **Charles V. Pask**, *Managing Director,* **ITSEC Associates Ltd.**
Panellists: **Claus Norup**, *Head Risk Management & International IT*, **Winterthur Group, Chris Potter**, *Partner*, **PricewaterhouseCoopers LLP, Richard Hollis**, *CEO*, **Orthus Ltd.**

STREAM 2: IT Infrastructure Security

Key Security Tools to Protect Your Assets

10.45 Security Policies? Ugh, Just Give Me A Firewall **

Start | Programs | Firewall | Rules | Add rule | Permit all hosts destination port 4695/tcp. Um, why did you just do that? Surprisingly (or not), security policies in many organisations are hidden, reflect thinking ten years ago, or simply don't exist. This session will help you understand why it is important to have a security policy, how to encourage end-user participation, and provide suggestions on what makes up a good policy, including:

- Was there a business justification for creating that hole?
- Was the decision backed up by your security policy?
- You do have an up-to-date, regularly reviewed policy, right?

Stephen Lamb, *Lead Information Security Specialist*, **Microsoft**

11.45 Local Government Infrastructure Security In The Age Of Internet And Partnerships **

CASE STUDY

- Moving towards a single log-on
- External access and proven protection
- Flexible working/ security
- Locking-down the desktop
- Proven patch management strategies

Richard Steel, *Head of ICT,* **London Borough of Newham**

14.00 Locating and Securing Your Network Backdoors ***

- Protecting and testing maintenance ports on switches, routers, and other network devices
- Simple Network Management Protocol (SNMP): friend or foe?
- Practical procedures for using wired and wireless techniques for locating wireless access points
- Moonlight audits, war-games dialling, port scanning, SNMP probes, and other clever ways to locate unauthorised modem and remote control backdoors

Ken Cutler, *Vice-President, Information Security,* **MIS Training Institute**

STREAM 3: Enterprise Application Security

Real World Identity & Access Management

10.45 Architecting Identity & Access Control Management Systems ***

- Defining the key control points for identity and access control management: identification, authentication, authorisation, auditing, policy compliance
- Essential policies and administration infrastructure necessary to support the technical infrastructure
- Techniques for gathering the necessary IT and organisation information
- Using a Security Management Cycle to determine solution sets for diverse organisations
- Practical benefits and pitfalls of enterprise identity and access control solutions

Ken Cutler, *Vice-President, Information Security*, **MIS Training Institute**

11.45 Responding To Identity Theft, Internet Fraud, ATM Fraud And Phishing Attacks **

- How to approach the risks and controls of increasingly sophisticated techniques
- 'Phishing' - what can be done realistically?
- Advances in verification tools, and trends that you should be aware of now
- How is your organisation approaching these new threats?
- Responses and authentication strategies to tackle the latest 'phishing', scams
- Biometric identity cards update

Phil Cracknell, *Chief Technology Officer,* **netSurity Ltd**

14.00 Secure Coding Principles: Protecting Your Key Assets and Personally Identifiable Information **

A revolution is occurring with security and web applications. Networks and Internet applications have been expanding and increasing in use. You will learn:

- How has this increase impacted your organisation?
- What are you doing today to protect your key assets?
- How to include security as part of your software development lifecycle process
- How to be pro-active with secure coding guidelines.

Demetrios "Laz" Lazarikos, *Director*, **Reddshell (USA)**

12.45 Lunch

15.15 Afternoon Tea Break

To register: email **mis@mistiemea.com** or fax **+44 (0) 20 7779 8293**

The programme may change due to unforseen circumstances. MIS Training reserves the right to alter the venue and/or speakers.

WEBSEC 2005 Conference Programme
Day One: Tuesday, 15th March 2005

15.30 Email And Internet Scams And Attacks: What Legal Responses Can You Deploy? *

With the steady increase in Internet scams, phishing attacks and emails seeking to mislead or defraud customers and users, this talk will look at the legal options available to companies whose customer and users are targeted by such scams and attacks. As well as outlining the relevant legal principles, the talk will give you practical tips to maximise your chances of success in taking action in response.

- What specific legal rights may be infringed: defamation, passing off, trade mark infringement, computer misuse, ISP notice and take-down procedures
- What are the practical legal options open to victim companies? Consideration of dispute resolution, injunctions and litigation
- The extent to which ISPs and other intermediaries may be legally liable
- How to persuade them to take action quickly!

Mark Taylor, *Partner*, **Lovells**

15.30 Building A Secure Portal Environment **

CASE STUDY

This case study is the story of an ongoing project at a major Belgian government related company. You will not hear a nice success story with a happy ending, but will learn how sometimes one has to make the best of a set of sub-optimal solutions. The presenter will share what he has and has not been achieved while building this portal environment. You will hear the reasons why. The case study is sometimes the story of fighting against forces that stick frenetically to non-flexible standards, but most of the time it is the story of fighting for looking at the overall security picture and for sensible and managed standards.

- Network security architecture
- Patch management, secure coding security testing, intrusion prevention
- Application level firewall
- Systems hardening, intrusion detection
- Security clearing
- Good access control management
- Global repository and user provisioning

Toon Mordijck, *ICT Security Manager,* **NMBS - Belgian Railway**

15.30 Who Holds The Keys To Your Kingdom? What You Should Know About Encryption **

- Why your effort in understanding cryptography should go further than passing a professional certification
- How the latest advances in cryptography affect your company
- An easy-to-understand guide on the most innovative cryptographic solutions: elliptic curves, quantum cryptography, identity-based encryption, key splitting, etc.
- A probe into the hidden dangers of today's cryptosystems
- Key management issues: how can you prevent your ideal cryptographic solution turning into a real nightmare?

Eduardo Solana, *Independent Specialist on Information Security and Cryptography Lecturer,* **University of Geneva, Switzerland**

16.30 Bugs, Worms, Trojans, Holes: Taking Control Of Software Patch Management

PANEL

- How to go about establishing a process for patch management
- How the big enterprise management vendors fit in
- Is patching part of something bigger?
- Is it best built into configuration or security management?
- How will customer-supplier partnerships develop in the future?
- What are the next biggest threats?

Facilitator: **George Thompson**, *Director IRM Security and Continuity,* **KPMG**
Panellists: **Mikko Hypponen,** *Director, Antivirus Research,* **F-Secure Corp., Vincent Bieri**, *Security Marketing Manager (EMEA),* **Cisco Systems, Ken Cutler**, *Vice-President, Information Security,* **MIS Training Institute, Chris Potter**, *Partner,* **PricewaterhouseCoopers LLP**, **Jason Hart**, *Head of Security,* **Whitehat**

17.30 – 19.30 WebSec Drinks Reception

WEBSEC 2005 Conference Programme:
Day Two: Wednesday, 16th March 2005

08.30 Coffee and Registration

09.00 KEYNOTE: Implementing The Jericho Vision **

David Lacey, *Director of Information Security,* **Royal Mail**

STREAM 1: Policy, Risk & Governance

Risk Controls & Planning

09.45 Measuring Information Risk: Best Practice At Alliance & Leicester **

CASE STUDY

Identify what has worked, and which new methods for measuring risk information security professionals should be focusing on.

- How can you approach information risk metrics?
- What measurement methodology worked and which tools where effective?
- Developing and sending out a positive message
- What are the benefits and pitfalls of the approach?
- What are the next steps?

John Pendleton, *Security Policy & Standards Manager,* **Alliance & Leicester plc**

10.30 Risk Analyis Vs. Risk Management: Before You Can Manage, You Must Understand **

CASE STUDY

- Layered approach to Risk Assessment: Enterprise, Project and System levels
- Quantitative and qualitative approaches
- Using Risk Analysis to maximise the benefit from scarce resources
- Iterative approach: How detailed do you need to go?
- Risk Assessment as a process, not a tool
- Ensuring the correct right skills mix
- Linking information security with other Risk Analysis models in the organisation
- You cannot manage what you don't understand

Paul Flanagan, *Information Security Officer & Crisis Management Leader,* **Genworth Financial, Payment Protection Insurance**

STREAM 2: IT Infrastructure Security

Enterprise Security Architectures

09.45 Resilience & Intelligence ***

With the raft of regulatory and legislative requirements now present, what is the business benefit?

- What regulations and laws that affect your business
- Achieving business buy-in
- Current status
- Resilience and regulation
- Building resilient systems with existing building blocks
- Choosing the best strategies
- What does the future hold?

David Lilburn-Watson, *President,* **High Tech Crime Unit** *and Principal Consultant*, **BCRM Ltd.**

10.30 Don't Leave It All To Your Firewall! Detecting And Preventing Hidden Breaches **

CASE STUDY

You will take away proven tactics to approach the practical and human issues of security, as well as the technical risks and some possible solutions.

- Security loopholes and back doors that circumvent your firewalls
- How can information flow in and out of your business undetected?
- How Trojans can slip in to your network
- Detecting the hidden breaches
- Designing to detect, mitigate and prevent breaches

Peter Taylor, *Information Security Manager - Group Risk,* **Bradford & Bingley plc.**

STREAM 3: Enterprise Application Security

Advanced Email Management

09.45 Spam Rules! Controls & Advanced Email Management **

CASE STUDY

- Spam trends and economic impacts
- Spamming techniques
- Key selection for spam control solutions
- What can you do: controls that work
- The future of spam

Lilia Vogt, *Head of Information Security,* **World Intellectual Property Organization**

10.30 Spoofing And Beyond: Methods & Investigation ***

PANEL

- How are basic and advanced e-mail spoofing techniques performed?
- What is phishing?
- Investigating e-mails to find the original sender
- Simple Mail Transfer Protocol (SMTP)
- Normal and spoofed headers
- Using open relays and open proxies
- Anonymisers and tunnels
- Log file analysis
- Mitigating email and instant messaging risks

Panellists: **Dave Brunswick**, *EMEA Spokesperson,* **Anti-Phishing Working Group**, *and Technical Director,* **Tumbleweed EMEA, Armando Leite**, *Head of Security Testing & Assessment Group,* **KPMG Technology Advisory Services**

To register: email **mis@mistiemea.com** or fax **+44 (0) 20 7779 8293**

WEBSEC 2005 Conference Programme
Day Two: Wednesday, 16th March 2005

11.15 Morning Coffee Break

11.30 Anti-Terror Laws, Data Retention & Interception Of Communications *

Both the UK government and the EU are considering whether to introduce further anti-terror legislation and to increase regulation in the area of data retention.

- What the current legal landscape in relation to terrorism and interception of communications looks like
- What data retention arrangements companies are currently required to have in place
- When the police and other agencies can require companies to decrypt and/or disclose data which they hold
- What procedures companies should have in place to avoid committing offences such as "tipping off"
- The interrelationship with data protection, human rights and freedom of information legislation
- New and proposed legislation in this area

Conor Ward, *Partner*, **Lovells**

11.30 UNIX Security: Getting The Basics Right: Advanced Common Sense **

CASE STUDY

A talk on the practical controls that you have to take to secure critical UNIX environments and protect your data and the ability to do business. You will focus on the many types of controls that need to be employed against a array of UNIX specific threats.

- Why should you care about UNIX security?
- What are the threats? Mistakes, Code, Insiders, Outsiders, Fraudsters and Hackers
- Key controls: supported Hardware/Software, Patching, Inventories, Authentication and Logging
- What are the proven benefits?
- Doing business making money and keeping the regulators happy!

Rob Gordon, *Team Leader, EMEA Technology Audit,* **Merrill Lynch**

11.30 Hacking Web Applications In 60 Minutes

HACKING DEMO

Although numerous commercial and freeware tools assist in locating network-level security vulnerabilities, these tools are incapable of locating application-level issues. This session will demonstrate how to identify security weaknesses for Web-enabled services that could be exploited by remote users. With numerous real-world examples, this course is based on fact and experience, not theory.

- Tackling the latest web server exploits
- How attackers manipulate HTTP and HTML to locate web application vulnerabilities
- Real-world web application weaknesses and exploits demonstrated live

David Rhoades, *Principal Consultant*, **Maven Security Inc.**

12.30 Lunch

13.15 Metrics For Good Management: What Is The Potential Cost Of Internal Security Breaches? **

CASE STUDY

- Quantifying the potential cost of network breaches to management
- Assessing accurately the likelihood of a malicious attack
- How can you assess whether the problem is escalating?
- Developing effective ways of analysing risk

Mark Stirland, *Chief Security Architect,* **Barclays Group**

13.15 Securing Voice-Over-IP (VoIP) Traffic – AKA: Click on the Monkey ***

- Using firewalls designed for VoIP traffic
- Eavesdropping on VoIP calls
- Encrypting voice traffic at the router or gateway if performance is a problem
- Separating off traffic
- Denying access to the voice gateway
- Using strong authentication for remote management and auditing
- Attack methodologies
- What the future holds

Richard Hollis, *CEO*, **Orthus Ltd.**

13.15 Using Your Intranet To Introduce A Fraud Awareness Strategy **

- How to make your staff aware of your company's fraud and ethics policies.
- Encourage your staff to identify their fraud risks
- Measure your staff's understanding of your policies and procedures
- Invite staff to record their perception of fraud in your company
- Use the intranet to explain how your company help-line / whistleblower policy works

Allan McDonagh, *Managing Director,* **Hibis Europe Ltd.**

14.15 Meeting The Business Need For Information Security In A Cost Effective Manner *

Although for a lot of security practitioners this is likely to be a step outside their comfort zone the rewards are significant and those that do manage information risk in a business-oriented, top-down, manner will be better equipped to drive it down and minimise the likelihood of damaging incidents.

- Selling security to the Board when the Board doesn't think there's a problem
- Deploying an enterprise-wide information risk analysis and management capability
- Changing mind-sets and awareness from being technology-centric to being business-centric

Andrew Wilson, *Project Manager*, **Information Security Forum (ISF)**

14.15 Values Of IDS & IPS: Understanding The Capabilities, Strengths, & Weaknesses **

PANEL

- Is IPS a replacement or a complement to IDS?
- Where do you position IDS and IPS in your overall network defence architecture?
- What is the best way to test the effectiveness of your IDS and IPS?
- Network intrusion detection devices
- Host-based intrusion detection devices
- Intrusion prevention products
- Honeypots and honeynets
- Costs of deploying the various technologies

Facilitator: **Ken Cutler**, *Vice-President, Information Security,* **MIS Training Institute**
Panellists: **Martin Hudson**, *Principal Advisor,* **KPMG LLP (UK), Richard Starnes**, *Director of Incident Response, Managed Security Operations Centre (MSOC),* **Cable & Wireless**

14.15 Mobile & Handheld Security **

CASE STUDY

New technologies and services impact on many areas of corporate security from policy and standards to technical implementation. This presentation focuses how Vodafone has been working on responses to the new fraud and security threats in the telecommunications sector and will include tips on how organisations can minimise fraud.

- New services, new threats, new opportunities
- Responses to the new threats from the convergence of mobile and internet
- Update on the latest phone and handheld attacks and mitigation
- Policy and standards issues you need to address
- How to minimise fraud and data theft opportunities
- The benefits of sharing information with suppliers, industry and government

Chris Cook, *Head of Product & Service Security,* **Vodafone UK**

15.15 Afternoon Tea Break

15.30 Outsourcing Your Information Security: Identifying Your Weakest Link *

- What to outsource, when, how much?
- Tracing and managing the whole vendor supply chain - 3rd party use
- Auditing software developers
- Buying process and evaluating your partners
- Ensuring web security policy compliance from your outsourcing partners
- Building a supportable infrastructure with the vendor
- What are the advantages and disadvantages of outsourcing security

Charles V. Pask, *Managing Director,* **ITSEC Associates Ltd.**

15.30 New Year, New Security Issues **

CASE STUDY

- Top skills to satisfy your security needs
- How to challenge new methods of attack
- New challenges of the extended perimeter of security
- Synergy between devices, and expectations (Blackberry, Smart Phones)
- Compliance: more than adherence to paper based policy
- Zero day threats: Have we seen them?

John Walker, *Head of Information Security and Specialist Security Services,* **Experian**

15.30 Securing Remote User Access With VPNs & Secure Sessions ***

- Differentiating between "trusted" and "secure" VPN services
- Defining the application, connection and security requirements for secure remote user connections
- Which VPN is better: IPsec, SSL or SSH?
- Defining security policies for the effective hardening and deployment of VPNs and secure sessions
- Applying VPNs to wireless applications
- Tools and techniques for detecting and auditing VPN application security

Ken Cutler, *Vice-President, Information Security,* **MIS Training**

16.30 Audit Tools For Top Security Vulnerabilities **

- Penetration testing versus vulnerability scanning versus audit
- Top tools and techniques for network discovery
- Top tools and techniques for vulnerability testing
- Top tools and techniques for penetration testing
- What every auditor should know about network security testing

Peter Wood, *Chief of Operations,* **First Base Technologies**

16.30 Auditor Security Collection: A Penetration Environment At Your Fingertips ***

- How to simplify the preparation of technical penetration tests
- What are the requirements and revenue of this collection?
- How to exhaust the wireless analysis specialities out of the CD-ROM
- How the usability enhancements make an auditor's life easier without losing flexibility
- How to place and use it in the real world
- Future plans

Max Moser, *Founder,* **Moser Informatik**

16.30 Building A Secure Infrastructure For Wireless LANs In Munich International Airport

CASE STUDY

- Wireless LAN implementation challenges
- Private Wireless LAN
- Public Wireless LAN
- Security measures for Wireless LAN
- VPN project in the Wireless LAN

Johann Gotz, *Project Director, WLANs*, **Munich International Airport**

17.30 Close of Day two

To register: email **mis@mistiemea.com** or fax **+44 (0) 20 7779 8293**

The programme may change due to unforseen circumstances. MIS Training reserves the right to alter the venue and/or speakers.

WEBSEC 2005 Conference Programme
Day Three: Thursday, 17th March 2005

08.30 Coffee and Registration

09.00 Integrated Security Management: Finding Interoperability Of Security Solutions To Enable Business

PANEL

How are organisations embedding security into every layer of the infrastructure, including physical to applications and networks to endpoints? Hear best and worst practice from practitioners and the experts, and how security is increasingly been used to enable competitive advantage.

- Don't rely on the vendors alone! How to maximize product capability
- Integrating information security architecture into the overall IT architecture
- Linking hardware and software options of your choice for maximum protection
- How can security enable business?
- Is vendor consolidation on the horizon? How will this impact your organisation's security strategy?
- Physical and IT security convergence: What is on the horizon? How can you approach this?
- What companies/industries are the most admirable with regards to security? Why?

Panellists: **Richard Starnes**, *Director of Incident Response, Managed Security Operations Centre (MSOC),* **Cable and Wireless**, **Vincent Bieri**, *Security Marketing Manager (EMEA),* **Cisco Systems, David Rhoades,** *Principal Consultant,* **Maven Security Inc.**

STREAM 1: Policies & Governance

Implementing Effective Information Security Policies

10.00 A Progress Report On The Adoption ISO 17799 *

CASE STUDY

- Selling the concept of information security in a company
- Adopting a framework
- How to leverage on existing standards and procedures
- Getting buy-in from technical staff
- How to measure progress and degree of success, or failure

David Allin, *Director in Information Services,* **European Patent Office**

11.30 Off-Shoring: Managing Security Risks Of Outsourced Code Development & Offshore Personnel *

- What to consider when selecting your outsourcing partner
- What to consider for relationship management
- Standards? What standards?
- Risk management – balancing system development control requirements against the perceived benefits

Martin Whitehead, *Director,* **ISMS Consulting Ltd.**, Formerly *Head of IT Security*, **Smile**

13.45 Business Continuity: Writing & Testing The Plan **

CASE STUDY

Advice for those starting a plan, some practical advice for those who have already done so.

- Why have a plan?
- What makes a disaster?
- How to handle security breaches while minimising the impacts
- What to include
- Who takes charge?
- Testing tips
- After the test what comes next?

Brian Shorten, *Systems Integrity Officer, International Security Group,* **MCI**

STREAM 2: IT Infrastructure Security

Anti-Hacking & Anti-Viral Tactics

10.00 Anatomy Of A Hack: How To Get Your Network Hacked In 10 Easy Steps ***

HACKING DEMO

In this session, learn about the 10 (actually 14) things that very successful hackers will do to compromise your network. Learn how hackers use these techniques, and how to prevent them. The techniques may surprise you, but your network health will improve greatly once you understand them.

- Do you think all hackers use the same techniques to break into your network?
- Do you think they all guess your passwords?
- Do you think that an unpatched vulnerability is the only way to compromise your domain controllers?
- SP2 and non-executable stacks: Is this really the end of buffer overflow vulnerabilities?

Stephen Lamb, *Lead Information Security Specialist,* **Microsoft**

11.30 Computers & Crime **

Hear the real facts behind the following statements and take away top tips on how you can protect your organisation.

- Virus writers have changed from hobbyists to criminals
- Spammers make millions by sending out their junk mail
- Real-world companies are launching DDoS attacks against each others
- Phishers are stealing banking information at an alarming rate
- Criminals are hosting fraud sites on innocents bystanders' home PCs
- What to do?

Mikko Hypponen, *Director, Antivirus Research*, **F-Secure Corp.**

13.45 Detecting Anomaly-Based Intrusion Detection Of Zero-Days Attacks **

- Why we desperately feel the need for anomaly detection today
- Intrusion detection as a system and a process, not a software
- Introduction to learning techniques for anomaly detection
- Detecting zero-days attacks: hope or hype?

Stefano Zanero, *Ph.D. Student, Politecnico di Milano University & Co-Founder,* **Secure Network Srl**

STREAM 3: Enterprise Application Security

Key Security Strategies for Internet Banking & Online Commerce

10.00 Latest Web Application & E-Banking Hacking Techniques & Defence Strategies **

CASE STUDY

Web applications themselves now form part of a Corporation's 'line of defence' and must robust enough to defeat or reduce the probability of an emerging plethora of http based hack attacks. The chosen defence strategy also must be based upon correct choice of application, application code design, implementation and integration with network security technologies (don't throw out your firewalls yet!!)

- 'Popular' vulnerabilities associated with web applications - especially those implemented within e-business and e-banking web portals
- Possible solutions that can be deployed to ensure secure web application deployment

Simon Pascoe, *Principle Internet Security Architect,* **BT Security Practice**

11.30 Hacking A Transactional Web Application ***

HACKING DEMO

This live demonstration of the latest application hacking techniques will show you how you can protect transactional web applications from emerging attacks.

- Why hackers target the application-layer
- Demonstration of application hacking techniques– Blended Phishing, XSS, SQL injection, etc.
- Analysis of the latest techniques and tools hackers used to attack Web applications
- How hackers automate application attacks
- Google hacking
- Holistic approach to developing secure web applications
- Proactive solutions to protect Web applications
- Hacking a transactional Web application:
- End point trust

Edward Barlow, *Technical Director*, **KaVaDo Europe**

13.45 XML-Based Application Security **

This presentation examines the range of highly secure applications architectures that can now be built using XML-based technologies.

- Concepts of 'application security' and the common security services API
- XML, Web Services architecture and XML security components
- SOAP messaging and its security extensions
- Derived security protocols: XKMS, S2ML, SAML, WS-Security, XACML
- XBRL and risk reporting

John Sherwood, *Operational Risk and Compliance Specialist,* **idRisk Limited**

11.15 Morning Coffee Break

12.30 Lunch

WEBSEC 2005 Conference Programme
Day Three: Thursday, 17th March 2005

14.45 Learning, Development And Communities Of Practice: Information Security's Secret Weapons *

CASE STUDY

What is the key role that the learning and development of individuals both within and outside the information security function can play? How can this be used to add further depth to an organisation's defences? You will learn how Communities of Practice can expand your Information Security Group's reach by hearing the lessons learnt from the development of Reuters' own Community of Practice.

- Stakeholder analysis: Identifying who else can help protect the organisation
- The importance of networking
- Developing a meaningful learning curriculum
- Adopting a "blended" learning approach
- Communities of Practice: theory and practice
- What are the important lessons learnt?

Andrew MacGovern, *Head of Learning - Operations & Technology,* **Reuters**

14.45 Modern Hacking Techniques: Theory & Realities Direct From The Ethical Hacker ***

HACKING DEMO

There is a huge lack of understanding when it comes to the real techniques and motivations of experienced hackers. This session will show you the context of a sophisticated, organised and financed attack: A group of experienced hackers, financed by an intelligence agency or an organised crime organisation attempting to remotely break into the operational network of a foreign bank. By describing all the possible steps of the scenario, you will learn:

- How is such a scenario possible today?
- If so, how? How much does it cost?
- How long does it take?
- What kind of skill is required?
- What can you do to prevent it?

Marco Ricca, *Founder, ILION Security SA and Researcher,* **EPFL/HP Labs**

14.45 Securing Active Directory Services ***

Active directory is rapidly becoming the most deployed directory service in the world. Microsoft's speciality of producing systems that provide core functionality out of the box has seen to this. There are unfortunate side effects to this policy, the understanding of which are essential. Although the good news is that, when designed and implemented creatively, it can offer functionality that you'd never have imagined, and becomes secure. You will gain insights into the most effective ways of using the Active Directory's own features and functions to shore up its own defences, while simultaneously increasing its ROI to your business.

- The concepts needed to create a secured architecture
- Tips, tricks and realities of group policies
- Laying down hierarchal authority
- Ensuring consistency and enforcing convention
- Creating cohesive architecture

Dominic Bland, *Principal Consultant,* **MindWalker Ltd.**

15.30 Afternoon Tea Break

15.45 Part One: Designing & Implementing Effective Security Policies *

CASE STUDY

- What was the need for ISMS?
- What was the approach/methodology
- Risk assessment
- Deliverables and specific key success factors
- Implementation plan
- Monitoring for compliance

George Chlomoudis, *Information Security Manager,* **TIM Hellas Telecommunications**

15.45 Peer to Peer Network Threats & Defences ***

- Peer-to-peer Internet-based services: Napster, Gnutella, Kazaa, eDonkey, public instant messaging
- Security and legal issues arising from use of peer-to-peer Internet-based services and peer-to-peer application sharing
- Methods for bypassing controls for peer-to-peer-applications
- Security countermeasures for detecting and controlling the use of peer-to-peer applications

Ken Cutler, *Vice-President, Information Security,* **MIS Training Institute**

15.45 Leveraging Today's Top Internet Forensics Tools **

- Responding to initial suspicions
- What are the early warning indicators of fraud or computer crime and misuse
- Investigative circumstances
- How best to commence and conduct the investigation
- 10 analytical methods common to all investigations
- Collecting computer evidence
- How to handle, collate and store admissible computer evidence
- Tools and techniques to recover and restore data

Ed Wilding, *Director*, **Data Genetics International Ltd**

16.45 Part Two: Implementing BS7799 & Achieving Certification: Challenges, Roadblocks & The Route-Map *

CASE STUDY

- Information security: challenges and roadblocks
- An introduction to BS7799 Standard
- Development and implementation of
- Policies and standards
- Achieving and monitoring compliance
- Ongoing awareness and training
- the certification process and the way forward

Gan Subramaniam, *Head of Information Security,* **Homeloan Management Limited**

16.45 The Windows XP Security Debate ***

Rarely these days do you hear contention on the stability of the system, but debate endlessly rages on its security. Fans of the system will tell you that point out that its security is constantly improving as lessons are learnt; its detractors will insist that patching should not be necessary, it should have been fully secured out of the box.

- What is XP good for? What is it not good for?
- The reality of patching
- Is there another browser war on the horizon?
- What was "wrong" with SP2 and will it happen again?

Dominic Bland, *Principal Consultant,* **MindWalker Ltd.**

16.45 Evaluating Your Patch Management Needs: Operational Risk & Cost Efficiency Approaches ***

CASE STUDY

95% of Wolverhampton Council PCs can now be patched within 24 hours of a software update being released. Learn how the challenges have been approached by WCC and the technical solutions.

- Setting the scene and business change requirements
- PM: Technical solutions deployed at WCC and the lessons learnt

Paul Dunlavey, *Major Projects Manager* and **Matthew Jeavons**, *LAN Manager,* **Wolverhampton City Council**

17.30 Close of Conference

Sponsored by:

F-SECURE®

F-Secure Corporation is a leading anti-virus and internet security vendor. It's award-winning solutions protect businesses and individuals from Internet security threats such as viruses, as well as providing parental control, desktop firewall with intrusion prevention, anti-spam and spy-ware technologies. Key strengths are the speed of response to new threats, together with ease-of-use and centralised management for businesses. Our core technologies include:

- **F-Secure Anti-Virus Client Security** - an integrated anti-virus and personal firewall solution that can be remotely installed to each workstation and managed centrally.
- **F-Secure Anti-Virus Total Suite** - provides the critical anti-virus components to protect laptops, desktops, file servers, email servers and gateways in a comprehensive, integrated solution.
- **F-Secure Anti-Virus Small Business Suite** - an easy-to-use, centrally managed solution designed specifically for Microsoft Small Business Server. It includes the key anti-virus components in a single, flexible solution.

F-Secure protection is also available through major Internet Service Providers including Deutsche Telekom and Wanadoo.

Contact Information: For more information, call F-Secure UK on 0845 890 3300 or email UK@F-Secure.com.

New Business Opportunities at WebSec 2005
Attendees at WebSec events are senior IT security professionals with purchasing power. If you are interested to find out how sponsorship or exhibiting at this event could complement your marketing strategy, please contact: Sara Hook on +44 (0)20 7779 7200, or email shook@mistiemea.com.

Media Sponsors:

ISSA — The Information Systems Security Association (ISSA)® is a not-for-profit international organization 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

CLUSIS — Established in 1989, CLUSIS (www.clusis.ch) is a non-profit-making Swiss association of thought leaders, specialists and technicians representing Swiss small and medium sized businesses and industries, banking, governmental organizations, IT suppliers, etc.. who share experience that is applied in current and future information security technology.

Information Security — Since it's debut in 1997, Information Security magazine has consistently remained the world-wide "number one" source of information for info security decision-makers. A resource for IT Security news, analysis, insight and commentary, it's recognized experts author each article, and the publication has won numerous awards for excellence in design and editorial content.

Information Systems Audit and Control Association — UK Chapters
The Information Systems Audit and Control Association, Inc. is a professional membership association comprised of individuals interested in Information Systems audit, control, and security. The Northern England Chapter covers the geographical area north of the Midlands and Northern Ireland (excluding Scotland). Meetings are usually held in Liverpool, Manchester and Leeds

INFOSECURITY MAGAZINE — Infosecurity Today is the new magazine for European IT managers. The magazine features articles focusing on the practical experiences of IT security professionals, provides in-depth analysis of current trends, independent reporting, and expert views and opinions on the latest developments in IT security. Infosecurity Today is distributed free of charge to over 10000 IT Security professionals in Europe 6 times a year. To apply for your subscription, visit: www.infosecurity-magazine.com/registration or email infosecurity@elsevier.com for further information

INFORMATION SECURITY BULLETIN — Information Security Bulletin is the leading international journal for infosec professionals. It is peer reviewed and count some of the leading experts in the field among its editorial team, e.g. John Sherwood, Eugene Schultz, Peter Wood, Phil Venables and Ken Lindup. The editor is Niels Bjergstrom, who in 2004 celebrates his 40th anniversary in IT, 17 of which were spent in information security. More information on isb-online.net.

INFORMATION SECURITY FORUM — The Information Security Forum (ISF) is widely recognised as being the dominant force in information security. ISF is an independent, not-for-profit association of leading organisations dedicated to clarifying and resolving key issues in information security and developing solutions that meet the business needs of its 260 corporate Members.

virus BULLETIN — Virus Bulletin has a formidable reputation as the leading specialist publication on computer viruses. Each issue contains news and opinions from the AV community, detailed analyses of the latest threats, comparative product reviews featuring the unique VB 100% award scheme and the VB Spam Supplement, covering anti-spam issues. www.virusbtn.com

MAG SECURS — MAG. SECUR, Le magazine Européen de la Sécurité - Informatique – Réseaux – Télécom – Internet, is a magazine diffuse to 5,000 decision makers, including Security Managers, Networks Managers, Engineering and Operation Managers. In all issues, you find news on Special investigation, Alertes: Analysis of the Attacks of the quarter, Experts analysis, Interviews of Security Managers: the best tools selected by Mag Securs. And Analysis of security solutions market

MIS TRAINING — About MIS Training: Founded in 1978, MIS Training Institute is the international leader in audit and information security training, with offices in U.S., UK, and Asia. MIS' expertise is drawn from the experience gained training more than 200,000 delegates across five continents. MIS offers conferences, on-site training, and more than 90 training courses in the areas of Internal and IT Audit, Information Security, Network Infrastructures, Operating Environments and Enterprise Applications. MIS is a Euromoney Training Group company.

To register: email **mis@mistiemea.com** or fax **+44 (0) 20 7779 8293**

The programme may change due to unforseen circumstances. MIS Training reserves the right to alter the venue and/or speakers.

WEBSEC 2005

REGISTRATION FORM

14th – 18th March 2005, London

EARLY BIRD DISCOUNT: Register by 16th January 2005 and save a possible £200

204KEN ISACA

REGISTRATION OPTIONS (PLEASE PHOTOCOPY FORM FOR ADDITIONAL DELEGATES)

No of dels	Conference Package:	Total	Discounted Price	Total
☐	3-Day Conference Only	£1,495	£1,395	£_____
☐	Conference & 2 Full-day Workshops	£2,395	£2,195	£_____
☐	Conference & 1 Full-day Workshop	£1,990	£1,835	£_____
☐	2 Full-day Workshops	£1,095	£1,045	£_____
☐	1 Full-day Workshop	£595	–	£_____
			Less discount	£_____
			Plus VAT @ 17.5%	£_____
			Grand Total	**£**_____

Discounts*

☐ Government: 10% off regular fee

☐ Group: Register 3 conference places and a 4th can attend for free

☐ Association: 10% off regular fee

ISACA No._____ ISSA No._____ CISSP Cert._____

**Discounts cannot be used in conjunction with each other*

After you have registered, you will be sent documentation asking you to select which conference sessions you plan to attend.

Workshop Selector
Please tick which of these workshops you will be attending:

Workshop 1: Practicalities of Information Security Management
Led by: **Charles V. Pask**, *Managing Director,* **ITSEC Associates Ltd** ☐

Workshop 2: Network Security for Today
Led by: **Vincent Bieri,** *Security Marketing Manager (EMEA),* **Cisco Systems** ☐

Workshop 3: Vulnerability Testing Tools & Techniques
Led by: **Ken Cutler**, *Vice President - Information Security,* **MIS Training Institute** ☐

Workshop 4: Security Governance, Maturity and Metrics
Led By: **George Thompson**, *Director IRM Security and Continuity &* **Nick Bleech**, *Principal,* **KPMG LLP (UK)** ☐

Workshop 5: Enforcing Internal IT / Web Surfing Policy's: How To Design And Implement A Clear Web Usage Policy
Led by: **Jeremy Barker,** *Technical Director,* **Orthus Ltd** ☐

Workshop 6: Hacking & Auditing Web-based Applications
Led by: **David Rhoades**, *Principal Consultant,* **Maven Security Inc.** ☐

4 EASY WAYS TO REGISTER

Fax +44 (0) 20 7779 8293
E-mail mis@mistiemea.com
Web www.mistieurope.com
Mail Guy Cooper
MIS Training, Nestor House
Playhouse Yard, London, EC4V 5EX, UK
Information tel +44 (0)20 7779 8153/8944

PLEASE SEND ME INFORMATION ON:

Conferences:
☐ IT Strategies for Managing Regulatory Compliance, 2-3 March 2005, London
☐ IT Audit Conference, 18-19 May 2005, London
☐ CISO Executive Summit, 16-17 June 2005, Geneva

Seminars:
☐ Information Security Boot-camp: Studying for Certification, 17-21 January 2005, London
☐ Sarbanes-Oxley for Information Security Professionals, 17-18 February 2005, London
☐ Network Firewall Security, 7-10 March 2005, London
☐ MIS Training Catalogue of Seminars 2005
☐ In-House Training

CUSTOMER INFORMATION (PLEASE PRINT OR ATTACH BUSINESS CARD)

Title	First name	Surname
Title/Position		
Organisation		
E-Mail Address (Required)		
Address		
Country		Postcode
Telephone		Fax

Please complete all fields in order for us to process your registration efficiently.

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 interest you. As an international group we may transfer your data on a global basis for the purpose indicated above. If you object to contact by telephone ☐, fax ☐, or email ☐ please tick the relevant box. If you do not want to share your information with other reputable companies please tick this box ☐

PAYMENT METHOD (FEES MUST BE PAID IN ADVANCE OF THE EVENT)

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

PLEASE DEBIT MY CREDIT CARD: ☐ AMEX ☐ VISA ☐ MasterCard

Card Number

Expiry___ ___ / ___ ___ Verification Code___ ___ ___

Cardholders name:

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 opposite

Signature: Date:

Approving Manager:

Position:

REGISTRATION INFORMATION

FEES MUST BE PAID IN ADVANCE OF THE EVENT

Accommodation: The event will be taking place at a 4 or 5 star hotel in central London. The venue will be confirmed upon registration. MIS Training has negotiated special accommodation rates. For further information please call IBR on +44 (0)1332 285521 or fax +44 (0)845 330 4982 from UK, or +44 (0) 1332 287613 if faxing internationally or go to www.ibr.co.uk/mis.

Cancellation Policy: Should a delegate be unable to attend, a substitute may attend in his or her place. A credit or refund, minus a 10% administration charge, is available if written notification is received by 13th February 2004. Thereafter, no refunds will be given. MIS reserves the right to change or cancel this programme due to unforeseen circumstances.

VAT: All delegates must pay VAT. After the conference organisations registered for VAT in the UK may reclaim the tax. Delegates from outside the UK but within the EU may also be able to reclaim the VAT. Organisations outside the UK should check with their excise authority as to which domestic fiscal regulations apply.

High Yield/No-Risk Guarantee: Attend this event and receive tools and techniques that will help you do your job better. If you do not, simply tell us why on your company letterhead and we will give you a full credit toward another programme.