MIS TRAINING presents:

## 4th Annual FinSec Conference

# Information Security for Financial Institutions

Gain 29 CPE Credits

## How to Prevent Cyber Attacks and Manage Risk in the context of Basel II

15th & 16th September 2004, Millennium Hotel London Knightsbridge
5 Optional Workshops: 14th & 17th September 2004

### Attend this timely event and leave with a greater understanding of how you can:

- **Prevent** 'phishing': educate on the dangers of online fraud and identity theft
- **Prepare** IS systems to meet new operational and compliance risk requirements
- **Protect** against viruses and worms: Critical responses to the latest wave of attacks
- **Budget** and measure IS spend for visible ROI on security actions
- **Integrate** mobile devices into your security strategy
- **Manage** a successful identity and access programme
- **Secure** back office and end-to-end transaction processing

### Learn from the experience of top financial institutions...

- BACS
- Bradford & Bingley plc.
- Dresdner Kleinwort Wasserstein
- Identrus
- Nomura International Plc.
- Nordea
- Norwich Union
- Saxo Bank
- Anti-Phishing Working Group

and more…

### New Agenda Format!

***Mornings:*** Hear Case Studies Directly from IS Departments
***Afternoons:*** Choose from Focused Business and Technical Round Table Discussions

Sponsor: Insight Consulting

Knowledge Partners: TUMBLEWEED COMMUNICATIONS, consult hyperion www.chyp.com

Media Partners: Information Systems Audit and Control Association UK Chapters, ISSA, FST, ZDNet UK www.zdnet.co.uk, silicon.com, BaselAlert.com, ISECOM, virus BULLETIN, BOBSGUIDE.com, BankersOnline.com, OperationalRisk

**Register NOW at www.mistieurope.com**

# Optional Pre-Conference Workshops: Tuesday 14th September

*Technical levels: Low * Medium ** High ****

08.30 **Coffee and Registration** • 09.00 **Commence of Workshop** • 12.30 **Lunch** • 17.00 **Close of Workshop**

## WORKSHOP 1*

## Preparing IT Security for Basel II Compliance

*Led by:* **Malcom Marshall,**
*Lead Partner, Security and Continuity Services,* **KPMG**
and **George Thompson,**
*Director, Information Risk Management,* **KPMG**

The application of Basel II in 2006 will have huge implications on IT/IS security departments due to the stringent requirements imposed on systems handling of sensitive data. Banks and investment companies need to plan, implement and maintain a comprehensive program of risk prevention, detection, analysis and management to achieve compliance to the new Accord. 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. You will leave this interactive workshop with the tools and tips to prepare your IT security systems to meet these new requirements.

### What will be covered:

- What are the new requirements?
- Identifying areas of operational risk: digital assets and information
- Novel approaches to preparing for Basel II projects, and integrating this into the overall IS infrastructure?
- Databases for both internal and external current and historical data
- Apparatus and processes for gathering loss data
- Methodologies to identify and estimate frequency of losses
- How can existing systems be leveraged to get more business value?
- Identify critical technology infrastructure that enables corporate operations
- Monitoring 3rd party relationships
- Assess threats and vulnerabilities in the existing IT environment: applications, networks, operational procedures and policies
- Compartmentalising and securing critical information
- Managing new risk-detection capabilities for ongoing monitoring
- Provisioning risk logging to meet new reporting requirements

### About your workshop leaders:

Malcolm Marshall has over seventeen years' experience in advising KPMG's leading global and national clients in managing technology and operational risks. He works for organisations in the financial, central government, technology, telecommunications, transport and manufacturing sectors. His experience ranges from large-scale security improvement programmes to product selection and security testing and assurance services.

George has extensive advisory experience in security management programmes, processes and architectures. George has 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. George has acted as security officer for clients. George specialises in defining security regimes that meet current and future business requirements while being practical and meeting clients' regulatory and statutory requirements.

## WORKSHOP 2***

## Securing and Monitoring Active Directory Services

*Led by:* **Dominic Bland, CISSP, MCSE,**
*Principal Consultant,* **MindWalker**

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. Firstly that, although Active Directory works out of the box, it offers only limited functionality unless shaped by skilled hands. Secondly that, although working "fine", it offers limited security unless suitably tethered.

The good news is that, when designed and implemented creatively, it can offer functionality that you'd never have imagined, and becomes secure. This workshop will offer you insight into the most effective ways of using the Active Directory's own features and functions to shore up its own defences, while simultaneously increasing it ROI to the business.

### What will be covered:

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

### About your workshop leader:

Dominic Bland is a national seminar leader and Active Directory architect for global corporations. A technical professional for the last 13 years, he has, for the last 6 focused on Windows infrastructure and security, authoring and delivering seminars, training Microsoft PSS, and building secured network service architecture for clients of all sizes in many industry sectors. He writes for the industry press on topics as diverse as the future of directory services, and technical risk assessment, while serving as the infrastructure specialist for a security incident response team.

## WORKSHOP 3**

## Preventing e-Fraud

*Led by:* **Martin Smith MBE,** *Managing Director,* **The Security Company (International) Limited**

Fraud has always been an underlying threat to any institution, but computers make the crimes bigger, easier and faster. Furthermore detection, apprehension and conviction are more difficult. e-Fraud seems the perfect way to get rich. This workshop will look at the nature of e-Fraud and then propose an action plan to reduce your organisation's exposure.

### What will be covered:

**The Control Environment**

- The importance of management policy
- Linking policy and operations
- Assignment of responsibilities
- Communication

**Risk Analysis**

- Fraud risk management
- Identifying vulnerability
- The risk of management function
- Risk management methodologies
- Risk management systems

**Deterrence Measures and Systems**

- IT security
- Internet and E-commerce security
- Classification of assets
- Personnel security
- Physical and environmental security
- Creating staff awareness at all levels

**Crisis Management and Contingency Planning**

- Crisis management action plans
- Crisis management team
- Insurance
- Notification and recovery
- Prevention of further losses
- An action plan

### About your workshop leader:

Martin Smith has had a fascinating and varied career in the world of espionage and terrorism. He is recognised in Europe as an authority on counter-terrorism, counter-fraud, anti-money laundering and computer security. Martin gained his degree in behavioural psychology before spending nearly 15 years as a commissioned officer in the Royal Air Force, firstly as a fast jet pilot and then assigned to counter-espionage and counter-terrorism duties. After being awarded Membership of the Most Excellent Order of the British Empire (MBE) for this work, he left the Service to carve out a second career in the commercial sector. He joined Touche Ross Management Consultants before becoming the UK Senior Director of Corporate Security for Kroll Associates. He then joined the Standard Chartered Bank as Head of Information Security. Mr. Smith formed The Security Company (International) Limited to exploit his unique and inventive approach to corporate and IT security. He has been working with major clients from the financial, commercial and business sectors, primarily reviewing and enhancing corporate security, fraud prevention, counter-terrorism and business continuity strategies and programmes. He is the Chairman of the Computer Weekly Infosecurity User Group, and is an internationally recognised author and speaker on his subject.

**To register:** email **misuk@misti.com** or visit our website at **www.mistieurope.com**

# Conference Day One - Wednesday, 15th September 2004

08.30 Coffee and Registration

08.50 **Chairman's Opening Remarks**

09.00 **The Synergy of Business and Security in a Dynamic Environment**

**Peter Kaye,** *Security Adviser,* **Bank of England**

09.30 **Identity and Access Management**

CASE STUDY & Q&A

A brief background to the established and successful DrKW Identity and Access Management environment will be followed by an introduction to the drivers behind their roadmap. An insight will be given into the types of work-flows and efficiencies deployed to enable delegation of access management back to the business units. This case study will also explore the drive towards single sign-on and credential management independence, and will be concluded by views on potential synergies with other topical security projects.

- Account automation, trusted work-flows and empowering the business
- Keeping costs down: high availability and visible ROI
- Maintaining momentum towards the final goal of Single Sign On
- Tactics to support client and server platform independence initiatives
- Synergies with network inventory and host-based monitoring

**Andrew Strong,** *Global IT Security Director,* **Dresdner Kleinwort Wasserstein**

10.15 **Outsourcing IT Banking Operations Securely**

CASE STUDY & Q&A

This session will look at the process of outsourcing significant security responsibilities from the standpoint of a regulated business. How to identify and engage potential partners, perform due diligence and transition services to outsourced delivery. This will include approaches to managing business change in an outsourced structure, gaining buy-in from the internal business and a look at the implications of placing services offshore.

- Identifying potential outsourcing partners
- Contracting for new security services and contract re-negotiation
- Assessing your potential outsourcers: keys to successful due diligence
- Specifying, monitoring and managing performance of your vendor - key performance measures
- Managing an outsourced service - essential skills to retain
- Comparing 'boutique' vs full service outsourcing partners
- Managing the process internally - ensuring buy-in across the enterprise
- Implications of offshore outsourcing

**Peter Taylor,** *Information Security Manager,* **Bradford & Bingley Plc.**

11.00 Morning Coffee and Networking Break

11.20 **Securing Electronic Banking**

CASE STUDY & Q&A

- Assessing application security risks
- Delivering accurate, effective and automated detection and fraud prevention
- The impact on business of European signature laws
- PKI versus non-PKI authentication
- How should you respond to a compromise?

**Kari Oksanen,** *Head of Risk Management-Electronic Banking,* **Nordea**

12.05 **Operational Risks: Managing Information Security in support of Regulatory Compliance**

Basel II is forcing heads of IT Security to reduce their risk exposure as a matter of urgency. A new European directive is being proposed that will be 'Sarbanes-Oxley' in all but name, whilst FSA regulation is imminent for the Mortgages and Insurance industries in the UK. For the financial services sector it is now crucial to assess all operational risks including IT related risks.

- Developing an IT security infrastructure that provides the basic foundation to address risk
- How regulation-driven projects can fit into the overall Information Security infrastructure
- Mechanisms for measuring risk - leveraging existing processes
- Effective compliance auditing and risk reporting
- Will increased regulation really affect levels of exposure?
- Best practice, standards and assurance levels

**Steve O'Reilly,** *Senior Consultant,* **Insight Consulting**

12.50 Lunch

## Please select from these concurrent breakout sessions:

14.00 **Business Strategy Round Table: Information Security for Financial Services Institutions: The Legal Issues**

- Regulatory framework in the UK and U.S.
- IT security standards and regulatory duties to customers
- Specific issues with outsourcing of financial services/accounting functions
- Practical issues in information security outsourcing deals

**Rory Graham,** *Partner,* **Baker & McKenzie**

14.00 **Technical Round Table: Securing Transaction Processing: End-to-End Transaction Security**

- Securing inter-bank payment transactions
- Advanced authentication strategies
- Transaction security to prevent fraud
- Managing the risk of new channels
- Identity theft/fraud

**Mark Stanhope,** *Information Security Architect,* **BACS**

15.30 Afternoon Tea and Networking Break

## Please select from these concurrent breakout sessions:

16.00 **Business Strategy Round Table: Authentication Strategies to Prevent Online 'Phishing' Fraud**

Many major financial institutions have recently been hit by 'phishing scams'. 'Phishing' attacks use 'spoofed' e-mails and fraudulent web-sites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers. The concern for information security professionals is, what happens when it is discovered that the trusted financial institution could have stopped this but failed to do so? This session will discuss:

- Where are the inherent system weaknesses?
- What e-mail authentication standards that have been proposed for solving the problem?
- How can banks protect reputation following an incident?
- Critical immediate responses to a 'phishing' scam
- Authentication for securing complex banking operations.
- How can banks educate users against an attack?

**Dave Brunswick,** *Technical Director,* **Tumbleweed EMEA** *and EMEA Spokesperson,* **Anti-Phishing Working Group**

16.00 **Technical Round Table: Newest and Most Critical Cyber Threats and Attacks: Worms, Viruses and System Intrusions**

As the time between disclosure and exploitation of vulnerabilities continues to shrink, threats that target vulnerabilities before they are known are imminent. Patch management continues to be critical, and this session will show how financial organisations can manage these risks effectively.

- Denial of Service probes and scans
- Viruses and other forms of malicious code
- Social engineering
- SQL injection, session hi-jacking and other current hacking methods
- Exploiting vulnerabilities in customer-facing web applications
- What threats should we prepare for in the short-term?
- Trojan horses: ensuring nothing inside can hurt you
- Incident correlation
- Open Signatures: a must have?
- Mission critical applications aggregation and correlation
- Patch management

*Senior Representative,* **F-Secure**

17.30 Close of Day One and Networking Drinks Reception

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

# Conference Day Two - Thursday, 16th September 2004

08.30 Coffee and Registration

08.55 **Chairman's Re-opening Remarks**

09.00 **Practical Risk Management: Choosing the Right Tools to Capture Day-to-Day and Strategic Input**

CASE STUDY & Q&A

Handling IT and physical security incidents on a daily basis, in addition to keeping an eye on strategic risks, such as legal liabilities, regulatory requirements, and general trends, is a challenge. How can you best capture all data, apply risk management and end up with the risks adequately managed? Saxo Bank has attempted to tackle this challenge. On the one hand, it has applied quantitative risk management tools to reiterate the risk data and bring forward the current key risks. On the other, it uses qualitative risk management to ensure that critical issues make it onto the agenda.

- The risk management objectives
- The tools created in Saxo Bank
- The organisational issues
- Procuring the data to make risk decisions
- Reiteration of the risk assessments

**David Boye,** *Chief Security Officer,* **Saxo Bank**

09.45 **Securing and Integrating Mobile and Wireless Environments: People, Policy and Process**

CASE STUDY & Q&A

Wireless connectivity for remote working is available across the globe. These days almost every airport, train station and coffee shop offers wireless hotspots with the promise of increased productivity whilst away from the office environment. Links via mobile phones are getting faster and the process of connecting your laptop or PDA seems ever easier. This presentation will look at the hard realities of providing a seamless, connected, service to your Executives and other staff. Is it really as simple (and secure) as the adverts claim?

- User expectations vs. operational reality
- Security policies, procedures and guidelines
- Lockdown vs. ease of use
- Support and maintenance

**David Ward,** *Security & Business Continuity Manager (Services),* **Norwich Union Central Services**

10.30 Morning Coffee and Networking Break

10.50 **Reducing Operational Costs and Demonstrating the Ongoing Effectiveness of Security Spending**

CASE STUDY & Q&A

- Importance of security information management: An investor's perspective
- Discovering and managing vulnerabilities
- Prioritising threats and enabling mitigation (shielding and patch management)
- Monitoring effectiveness and providing baseline planning data
- Security Information Management (SIM) as an essential monitoring function

**Andy Hardy,** *Principal, Technology, Private Equity,* **Nomura International Plc.**

11.35 **How can Information Security Bundle Finance Risk, Compliance Risk and Operational Risk? What is the Real Impact of Basel II**

PANEL DISCUSSION

Regulations like the Basel II Accord on capital adequacy have placed IT security into a corporate limelight. This panel discussion will examine how financial institutions have approached IT security in preparation to meet Basel II requirements from 2006, the expectations and the costs involved.

- What does operational risk look like for information security?
- Exploiting the overlap between Basel II, best practice credit risk management and International Accounting Standards (IAS) to improve ROI on security spend
- IT security software to improve capital allocation, financial transparency and profitability
- Are regulators finally satisfied that settlement and operational risk have been sufficiently reduced? What developments are on the horizon?
- Does regulation really improve risk management processes, or simply add cost? Are the costs of preparing for Basel II justified? What other risk management processes are needed for IT?

**Panellists: Malcolm Marshall,** *Lead Partner, Security and Continuity Services,* **KPMG, John Bullard,** *VP Global Ambassador,* **Identrus, Steve O'Reilly,** *Senior Consultant,* **Insight Consulting, Martin Smith MBE,** *Managing Director,* **The Security Company (International) Limited**
**Richard Feist,** *Board Director,* **ISECOM**
**Ray Stanton,** *Director, European Security Centre of Excellence,* **Unisys**

12.45 Lunch

## Please select from these concurrent breakout sessions:

14.00 **Business Strategy Roundtable: How to Respond to an Information Security Compromise**

- Damage discovery/file integrity assessment
- Establishing a plan and policy
- Disaster recovery back-up site issues
- Instant restore and automated backup capabilities
- Are physical and information security part of the same issue?
- Collecting electronic evidence traces/data retention/privacy issues/network forensics/investigation
- Predicting and protecting from the next generation of unanticipated threats and network hazards
- After the security breach: who are you going to call?

**Richard Hollis,** *Managing Director,* **Orthus Ltd.**

14.00 **Technical Round Table: Smart Cards and Biometrics: The Security Dream Team?**

- What are the security problems that the financial sector wants to address?
- An update on the smart card sector and some trends from around the world
- Using biometrics in practical environments
- The pluses and minuses of biometric identification and authentication
- The strategic link between biometrics and smart cards
- Practical experiences and case studies: what have we learnt so far?

**Dave Birch,** *Director,* **Consult Hyperion**

15.30 Afternoon Tea and Networking Break

## Please select from these concurrent breakout sessions:

15.50 **Business Strategy Round Table: Information Security Policies for Compliance Risk**

- Centralised or federated IT security system?
- Compliance risk identification, assessment and mitigation - how can the IT security team participate?
- Risk reporting: architectures for feeding the executive management dash-boards
- Gramm-Leach-Bliley and IAS Compliance
- Cyber Security and Sarbanes-Oxley: What is the IT Security department's responsibility?
- Understanding how the Sarbanes-Oxley Act is being implemented in your company to determine if you can leverage this approach to other risk management areas
- Compliance for security: keys to implementing customer verification, government watch lists, individual and group transaction monitoring and money flows

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

15.50 **Technical Round Table: Protecting Your Network Perimeter and Maximising Value**

This session will look at how firewalls operate and where to position them in an enterprise network. What are the security benefits and operational trade-offs of different firewall architectures? How can you evaluate the benefits and positioning options for different types of IDS components? Includes tips for selecting firewall and intrusion detection products and services.

- IDS vs. IPS Systems
- Design and visuals of IDS more user friendly
- How do you test IDS? Stealth testing
- What's the latest in firewalls?
- What is the future of this technology?
- Assessing Intrusion Detection solutions
- Identifying acceptable/unacceptable behaviour
- Outsourcing IDS: a good idea?

17.20 Close of Conference

# Optional Post-Conference Workshops: Friday 17th September

*Technical levels: Low * Medium ** High ****

08.30 **Coffee and Registration** • 09.00 **Commence of Workshop** • 12.30 **Lunch** • 17.00 **Close of Workshop**

## WORKSHOP 4*

### What do Security Specialists in the Financial Sector need to know about Privacy Law?

*Led by:*
**Dr. Chris Pounder,** *Consultant, Information and Technology Group,* **Masons**

Financial companies must have a thorough understanding of legal privacy issues and risks should a breach of privacy occur. Staff who work in information security are often well placed to play a crucial role in preparing their organisation to meet any challenge on the privacy front.

This interactive workshop will explore some of the major legal issues relating to technology privacy and IT governance. You will leave with a better understanding of the role of your organisation's data protection obligations and practical tips on how new technologies can affect your consumer's privacy.

**What will be covered:**

Part I:
- How the Data Protection Act relates to the security of information systems
- The scope of the Act
- How the case of Financial Services Authority v Durant impacts on the definitions
- How the Data Protection Principles relate to security and integrity of personal data
- How security issues can become data protection complaints
- How the offences in the Data Protection Act work
- How the Data Protection offences relate to other offences (e.g. Computer Misuse Act)

Part II:
- How the privacy scene is changing in the post 9/11 era
- Privacy and audit trails - tracking the citizen
- An emerging trend in relation to a statutory obligation towards security

**About the workshop leader:**

Dr. Chris Pounder has worked in the field of data protection, privacy, FOI and IT security since 1983. He provides consultancy services in relation to the field of data protection. He also develops and delivers courses in data protection (some of which lead to a formal qualification) and several other courses related to IT security, freedom of information and human rights. It is expected that he will launch a set of courses in relation to a forthcoming qualification in FOI. Chris is the editor of Data Protection & Privacy Practice, which is published by Masons. Chris regularly contributes to specialist security magazines and trade press.

## WORKSHOP 5***

### WiFi Security 102: Hacking Methodologies, Design and Configuration Counter-measures

*Led by:*
**Richard Hollis,** *Managing Director*, **Orthus Ltd**
*and* **Guvan Bayram, Orthus Ltd**

In this all-day hands-on workshop, Richard Hollis will cover the latest issues in WiFi security. Richard will discuss current WiFi hacker goals and methodologies as well as effective, little-no cost countermeasures. In addition to a live WLAN hacking demonstration, the topics covered will include:

**What will be covered:**
- WiFi architectures: 802.11a– z, WISPs, WLANs & Hotspots
- Typical WiFi architecture security vulnerabilities
- A profile of the WiFi Hacker
- Hacking tools & methodologies
- Live hacking demonstration
- Risk assessment practices
- Design & configuration countermeasures
- Integration issues and solutions
- WPA, AES and next generation standards

**About your workshop leader:**

**Richard Hollis,** *Managing Director,* **Orthus Ltd**

A Certified Information Security Manager, Richard is a seasoned security professional with over 20 years of industry management experience. He has extensive "hands on" skills and experience in designing comprehensive information security programs and architectures and has consulted to dozens of high-tech blue-chip companies across Europe. Orthus Ltd. is a European "product agnostic" information security consulting firm headquartered in London specialising in wireless security solutions. Richard's career also includes serving as the Director of Security for Philips Communications, Deputy Project Security Director to the U.S. Embassy Moscow Reconstruction Project and numerous sensitive security positions within the U.S. Government. Richard has published numerous articles and white papers and has appeared on BBC 4, Channel 4 and CNN and cited in Time, SC, InfoSec, Computing and Computer Weekly.

*Sponsor:*

Insight Consulting is a leading provider of information security, business continuity and risk management solutions. From the development of policy, strategy and awareness through to delivery of complete, end-to-end projects comprising testing, training, recruitment and managed security, Insight helps organisations identify and manage the risk in their IT and business operations. Our solutions include:
- Risk management guidance for strategic and operational projects
- Design and management of information security management systems
- Cost-effective business continuity and disaster recovery solutions
- Design, implementation and management of e-security infrastructures
- Compliance programmes for BS 7799, FoI and Data Protection Act

*Media Partners:*

Information Systems Audit and Control Association UK Chapters · ISSA Information Systems Security Association · FST · ZDNet UK www.zdnet.co.uk · ISECOM · virus BULLETIN · BOBSGUIDE.com · silicon.com · BankersOnline.com · OperationalRisk · BaselAlert.com

*Knowledge Partners:*

TUMBLEWEED COMMUNICATIONS · consult hyperion www.chyp.com

**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 in training more than 200,000 delegates across five continents. MIS offers conferences, on-site training, and more than 90 seminars 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 **misuk@misti.com** or visit our website at **www.mistieurope.com**

**REGISTRATION FORM**

# Information Security for Financial Institutions

15th & 16th September 2004, Millennium Hotel, London Knightsbridge

EMT 728

## 4 EASY WAYS TO REGISTER


**Fax** +44 (0) 20 7779 8293

**E-mail** misuk@misti.com

**Web** www.mistieurope.com

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

Information tel: +44 (0)20 7779 8153/7229


**PLEASE SEND ME INFORMATION ON:**

- ❑ The ISI Network Infrastructure Security Academy, 2nd - 13th August 2004, London
- ❑ Infosec Week, 16th - 20th August 2004, London
- ❑ Preventing and Detecting Fraud Conference, 26th - 27th October 2004, London
- ❑ MIS Training 2004 Catalogue of Seminars

I would like to receive e-news updates from:

❑ ZD Net UK ❑ Silicon.com

**Early Bird Discount: Register by 23rd July 2004 and save £100**

## REGISTRATION OPTIONS (PLEASE PHOTOCOPY FORM FOR ADDITIONAL DELEGATES)

| | Regular price | Early-bird price | |
|---|---|---|---|
| 2-Day Conference only | £1,095 | £995 | £ ..... |
| Conference and 2 Workshops | £2,095 | £1,995 | £ ..... |
| Conference and 1 Workshop | £1,595 | £1,495 | £ ..... |
| 2 Workshops only | £990 | £890 | £ ..... |
| 1 Workshop only | £500 | - | £ ..... |
| | *PLUS VAT† (17.5%)* | | £ ..... |
| Grand Total | | | £ ..... |

**Workshop Options**

Please Tick Box

- ❑ Workshop 1: Preparing IT Security for Basel II Compliance
- ❑ Workshop 2: Securing and Monitoring Active Directory Services
- ❑ Workshop 3: Preventing e-Fraud
- ❑ Workshop 4: Privacy Law
- ❑ Workshop 5: WiFi Security 102: Hacking Methodologies, Design

*Discounts:

- ❑ Government: 10% off regular fees
- ❑ Please call to enquire about group discounts

Discounts can not be used in conjunction with each other

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

❑ 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:*

.....

.....

❑ Cheque enclosed (payable to MIS Training)

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

Signature: ..... Date: .....

Approving Manager: .....

Position: .....

## 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 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 e-mail ❑ please tick the relevant box. If you do not want to share your information with other reputable companies please tick this box ❑

## REGISTRATION INFORMATION

FEES MUST BE PAID IN ADVANCE OF THE EVENT

**Accommodation:** The event is taking place at the Millennium Hotel London Knightsbridge, 17-25 Sloane Street, Knightsbridge, London, UK, SW1X 9NU. Tel: +44 (0) 20 7235 4377 Fax: +44 (0) 20 7235 3705. MIS Training has negotiated special accommodation rates. For further information please call IBR on +44 (0) 1332 285521 or fax +44 (0) 1332 374904 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 26th August 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 these workshops 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.