

THE SUNDAY BUSINESS POST

iQuest

NITES 4

March 1 & 2, 2005

National IT and E-Security Summit

Croke Park Conference Centre, Dublin



sponsored by

Rits



Introduction

Information security is now, more than ever before, recognised as being at the core of industry strategy. With the ever changing threat landscape, it is imperative that organisations respond effectively - the N.I.T.E.S e-Security conference will show you how.

Now in its fourth year, N.I.T.E.S has emerged as Ireland's leading IT and e-Security Summit. The conference is a top-level strategic forum where tactics and strategies are examined, ideas exchanged and relationships developed.

This year's event promises our most impressive line-up of national and international speakers. Visionary leaders, international experts and real-life customers will share their experiences and knowledge with you through thought-provoking presentations and interactive workshops.

The organisers, The Sunday Business Post and iQuest, would like to thank our sponsors and endorsers personally for their support and contribution.

Who should attend?

N.I.T.E.S 2005 is specifically designed for enterprise, government and corporate managers responsible for identifying, evaluating, selecting and purchasing security technologies within organisations, including:

- Managing Directors/Chief Executives
- Chief Technology Officers/Chief Information Officers
- Directors/Managers IT Security
- Security Consultants
- Systems Managers/Engineers
- Telecommunication Directors/Managers
- e-Business Managers/Directors

Comments from previous N.I.T.E.S conferences

"It was great to hear expert opinion on how technology works, what doesn't work and issues that make it work or not. This well-organised event also afforded me further opportunities to meet with other security professionals"

Gill Leo - Group IT Security Manager, Glanbia

"Attendance at this type of high-quality conference is crucial for tracking down security skills and strategies for tomorrow's challenges"

Enda Gallagher - Network Manager, Penneys

"I find this annual event provides an on-going opportunity to keep abreast of emerging threats and trends, in addition to learning from recent experiences encountered by speakers and delegates well connected with the IT Security business"

Colin McKeeman, IT Security Officer, Eagle Star Insurance Co Ltd

"N.I.T.E.S provides one of the best learning conferences for what is happening in the security industry that I have experienced"

Ian Kelly, Business Analyst and Information Security Officer, Pfizer Ireland

Sample list of companies and organisations which have attended previous N.I.T.E.S events:

- ROS Revenue
- Irish Software Association
- CityJet
- Systems Ltd
- Microsoft
- RSA Security
- Sun Microsystems, USA
- Checkpoint Software
- Dept of Justice
- Dublin Co Council
- CERT
- Orix Ireland
- Dept of the Taoiseach
- Motorola
- ACCBank
- ESB
- Fianna Fail
- Kingspan
- Performix Technologies
- EHSS
- Dr Steevens Hospital
- Royal Sun Alliance
- Canada Life House
- NEHB
- Hewlett-Packard
- AIB
- AIB Capital Markets
- Rotunda Hospital
- Ericsson Services Ireland
- Irish Life & Permanent HQ
- McKeever Rowan Solicitors
- RTE
- EBS Building Society
- Technomen
- BDO Simpson Xavier
- Pearse Trust

- Eagle Star
- Public Prosecutions Dept
- LGCSB
- Dept of Agriculture
- CIE
- Penneys
- Pfizer Healthcare Ireland
- Netfort ISS Ltd
- TCM
- De Royal Europe
- Fyffes
- MGB & Associates Ltd
- Forfas
- Landwell Solicitors
- Heineken Ireland
- Bank of Ireland
- GE Capital
- FBD Insurance
- Oracle
- Fexco
- Ernst & Young
- Celestica
- Dublin City University
- Elan Pharmaceuticals
- Kerry Group Plc
- LAN Communications
- Accenture
- Baker Consultants
- Fidelity Investments
- EMC
- Lecan Group
- Asita
- Dept of Finance
- European Central Bank
- Dept of Social & Family Affairs
- Glanbia
- Esat
- Dairygold
- Musgrave Group
- Dept of Social Welfare
- Friends First

PROGRAMME AT A GLANCE

DAY 1: March 1

Plenary

- Ministerial address
- International response to international challenge
- The Information Security Ostrich

Morning tea and exhibition viewing

Stream A	Stream B
<ul style="list-style-type: none"> ● Tone at the top: role of the board and of directors ● The role of modelling and attack simulation in risk management automation ● Analysing mergers & acquisitions within the security industry 	<p>Technical Workshop 1 Computer forensics as an IT management problem</p>

LUNCH

LUNCH

Stream A	Stream B
<ul style="list-style-type: none"> ● PANEL: Minimal acceptable business practices in enterprise information security management ● The changing landscape of security 	<p>Technical Workshop 2 My dad's computer, and the future of internet security</p>

Afternoon tea and exhibition viewing

Plenary

- Will SSL VPNs kill off IPSEC-based VPNs?
- Windows security: Is it getting any better?

DAY 2: March 2

Plenary

- Mapping and visualising the internet and intranets
- Biometric identity management for governments and enterprises in the 21st century
- Identity theft in Ireland

Morning tea and exhibition viewing

Stream A	Stream B
<ul style="list-style-type: none"> ● The challenge of "engineering" secure software products ● Incident responses essentials ● The dangers of Instant Messaging 	<p>Technical Workshop 3 Wireless security fundamentals</p>

LUNCH

LUNCH

Stream A	Stream B
<ul style="list-style-type: none"> ● Information security: What price must we pay? ● Best practices in e-mail security ● Key projects for 2005 	<p>Technical Workshop 4 Insider security threats</p>

Afternoon tea and exhibition viewing

Plenary

- Build your own security culture
- Will we ever stop internet hacking?



Bill Cheswick, Chief Scientist, Lumeta Corp, US

Cheswick has worked on (and against) operating system security for over 35 years. He was under contract for several years at Lehigh University, US, and the Naval Air Development Centre, working on systems programming and communications. In 1978, he worked at the American Newspaper Publishers Association/Research Institute, where he shared a patent for a hardware-based spelling checker, a device clearly after its time.

In 1987 he joined Bell Laboratories, and worked there for over 12 years. He did early work on firewall design and implementation, including the first circuit-level gateway, for which he coined the term "proxy". Cheswick also worked on PC viruses, mailers, internet munitions, and the Plan 9 operating system. He co-authored the first full book on firewalls, and has since toured the world giving media interviews and entertaining post-lunch security talks. Cliff Stoll, who is given to overstatement, has called Cheswick "one of the seven avatars of the internet".

In 1998, Cheswick started the **Internet Mapping Project**. This work became the core technology of a Bell Labs spin-off, Lumeta Corporation, which **explores the extent of corporate and government intranets and checks for host leaks that violate perimeter policies.**

Cheswick has a wide interest in science. In his spare time he flies high-power model rockets, RC aeroplanes and automates his home. He eats very plain food – boring even by American standards – and peppermint oil is his favourite insecticide.



Eugene Schultz PhD, CISSP, CISM, Principal Engineer, Lawrence Berkeley National Laboratory, US

Eugene Schultz is a Principal Engineer at Lawrence Berkeley National Laboratory of the University of California. He is the author/co-author of five books, one on Unix security, another on internet security, a third on Windows NT/2000 security, a fourth on incident response and the latest on intrusion detection and prevention. He has also written over 100 published papers. Dr Schultz is the Editor-in-Chief of Computers and Security and is an associate editor of Network Security and Information Security Bulletin.

He is also a member of the editorial board for the SANS NewsBites, a weekly information security-related news update and is on the technical advisory board of three companies. He has been an adjunct professor of computer science at Purdue University, where he taught courses and participated in research in the CERIAS (Centre for Education and Research in Information Assurance and Security) programme. **Schultz has received the NASA Technical Excellence Award, the Department of Energy Excellence Award, the Information Systems Security Association (ISSA) Professional Achievement and Honor Roll Awards, the ISACA John Kuyers Best Speaker/Best Conference Contributor Award, the National Information Systems Security Conference Best Paper Award. He has also been elected to the ISSA Hall of Fame.**

While at Lawrence Livermore National Laboratory he founded and managed the US Department of Energy's Computer Incident Advisory Capability (CIAC). He is also a co-founder of **FIRST**, the Forum of Incident Response and Security Teams. **Schultz has provided expert testimony before committees within the US Senate and House of Representatives** on various security-related issues, and has served as an expert witness in legal cases.



Richard Hackworth, Group Head of IT Security for HSBC Holdings, UK

Richard Hackworth is Group Head of IT Security for HSBC Holdings and has global responsibility for IT security policy and standards. Richard has also been a consultant with Coopers & Lybrand. **His consulting experience includes IT strategy development and implementation, marketing and IT security and control. His clients included UK central and local government, police forces, financial services, manufacturing and the European Commission.**

He has also held IT management positions in the manufacturing industry, physical distribution and commodity trading. He worked with the DTI to develop **BS7799**, and sat on an OECD expert committee that prepared the **OECD IT Security Guidelines** published in 1993. Hackworth has been a member of the British Computer Society Security Committee and of the Council of the Royal Statistical Society. He is a chartered engineer and a chartered statistician.



Professor Fred Piper, Director of Information Security Group, Royal Holloway, University of London

Fred Piper has been Professor of Mathematics at the University of London since 1975 and has worked in security since 1979. He is currently **Director of the Information Security Group (ISG) at Royal Holloway.**

Royal Holloway ISG offers MScs in Information Security and Secure Electronic Commerce and has a PhD programme that has produced over 100 doctorates.

In 1985, Piper formed a consultancy company, Codes & Ciphers Ltd, and since then he has acted as a consultant to over 100 companies in Britain, Europe, Africa, Asia, Australia, Canada and the US.

The consultancy work has been varied and has included algorithm design and analysis, key management and security audits of large networks. **Fred has lectured worldwide on Information Security, both academically and commercially, with recent emphasis on the use of digital signatures and the role for public key infrastructures.** He has published more than 100 research papers and is joint author of Cipher Systems (1982), one of the first books to be published on the subject of protection of communications, Secure Speech Communications (1985), Cryptography: A Very Short Introduction (2002), and an ISACA research monograph on Digital Signatures (1999).

In 2002, he was awarded an IMA Gold Medal for "services to mathematics". In 2002 he was awarded the first honorary CISSP for a European. This was for **"leadership in information security"**. In 2003, Professor Piper received an **honorary CISM for "globally recognised leadership" and "contribution to the Information Security Profession"**.

Programme Agenda

DAY 1

8:00 Registration and breakfast

Delegates are invited to beat the traffic by arriving early and having tea/coffee and pastries with colleagues courtesy of iQuest and The Sunday Business Post

PLENARY

8:40 Opening remarks and introduction from the morning chair

Jim Friars, Chief Executive, Irish Computer Society Chairman, ECDL Foundation Ltd

8:45 MINISTERIAL ADDRESS

Noel Dempsey, TD, Minister for Communications, Marine and Natural Resources

THE BUSINESS OF SECURITY

9:00 INTERNATIONAL KEYNOTE ADDRESS

International response to international challenge

Economic and social developments are becoming linked to the success of the internet and depend upon reliable and safe information technology.

- What should be the priorities for the private and public sector to protect this critical resource over the next ten years, and what does this mean to the senior management of individual enterprises?

In this session, Richard Hackworth will explore and give his personal views on these questions from the perspective of a major global financial services business.

Richard Hackworth, Group Head of IT Security for HSBC Holdings, UK

9:40 KEYNOTE ADDRESS

The Information Security Ostrich

- The IT policeman
 - E-mail informality
 - Application insecurity
 - Covert channels and customer education
- Sean Reynolds, Managing Director, Rits Information Security**

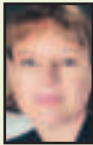
10:20 Morning tea and exhibition viewing

STREAM A **MANAGEMENT & GOVERNANCE**

10:45 Tone at the top: role of the board and of directors

● What can directors and boards do to influence high standards of corporate governance and corporate compliance in their organisations?

Niamh Brennan, Professor of Management, University College Dublin



11:15 The role of modelling and attack simulation in risk management automation

Organisations are under tremendous pressure to protect digital assets in compliance with new regulations. With tens of thousands of vulnerabilities, ten new vulnerability types published daily and constant network changes, it takes months for enterprises to prioritise the top 1 to 3 per cent of critical vulnerabilities that are accessible, exploitable and that matter - an unmanageable window of exposure. Products that help identify and mitigate vulnerabilities through automation have fallen short of delivering on their promises because they ignore the IT environment and business context. Through customer case studies, this session will introduce the role of attack simulation in the four steps to automation.

- Prioritising the top 1 to 2 per cent critical business exposures
 - Remediation sequencing and resource prioritisation
 - Communicating the state of security to business executives
 - Security risk management compliance
- Avi Corfas, Vice President and Managing Director, Europe, Middle East & Africa, Skybox**



12:15 Analysing mergers & acquisitions within the security industry

- Understand the technical, regulatory and social issues driving change in the information security industry
- Review market consolidation to date and information security convergence with other industries
- Inside look at future M&A trends
- Leveraging M&A trends to protect your organisation and preserve IS investments

Jim Reavis, President, Reavis Consulting Group, US



12:45 Lunch and exhibition viewing

STREAM A

2:00 Welcome back and introductions from the afternoon chair

Paddy Roberts, President, ISSA Ireland (Information Systems Security Association)

2:05 Panel Discussion
Minimal acceptable business practices in Enterprise Information Security Management

- Why is the US so far ahead of the EU in terms of legislation?
- The impact US regulations are having here
- Managing effectively your electronic communication strategy
- Security breaches: Who is liable?
- e-Voting: US systems versus EU
- "Phishing": its effect on financial services

Panellists will include leading industry figures including:
Jim Reavis, President, Reavis Consulting Group & International
Kevin Thiele, Managing Director, SonicWALL
Joe McCarthy, Network Consultant

MOVING BEYOND THE PERIMETER WITH INTELLIGENT SECURITY

2:55 The changing landscape of security

- Internet security drivers in 2005: security must be intelligent
 - Security: Raising the bar
 - Perimeter, internal and web security
- Niall Moynihan, EU Technical Director, Checkpoint Corp**



3:25 Afternoon tea and exhibition viewing

PLENARY

3:50 Will SSL VPNs kill off IPSEC-based VPNs?

Organisations are increasingly facing the challenge of how to enable employees, customers and suppliers secure easy access to resources in the internal network.

SSL-based VPN solutions have been positioned by vendors as the ultimate easy-to-implement, zero footprint, remote access solution.

- How do SSL VPNs work?
 - What are the economics?
 - SSL v IPSEC - the pros and cons
 - Questions to ask vendors
 - A real world case study
- Walter Jekat, European Director of Research and Development, Unit 4 Agresso, Germany**



WINDOWS SECURITY

4:20 LOCKNOTE ADDRESS

Windows security: is it getting any better?

Windows security issues are perpetually in the spotlight. Vulnerabilities in Windows systems have abounded, and hotfixes and service packs have almost as a rule initially been faulty. Windows-targeting viruses and worms have infected millions of systems over the last few years, and hacking methods that assault Windows systems are widely



used. In response to growing criticism (and also possibly diminished sales of its products), three years ago Microsoft initiated its Trusted Computing Initiative (TCI) in an attempt to produce more reliable and bug-free software. Sceptics labelled the TCI as a publicity stunt; others have applauded Microsoft for launching this bold initiative. Who is right? Is Windows security getting any better, and if so, what evidence is there? This presentation addresses these and other questions.



Eugene Schultz PhD, CISSP, CISM, Principal Engineer, Lawrence Berkeley National Laboratory, US

4:50 Conference close

5:00 Wine reception

iQuest and The Sunday Business Post would like to invite delegates and speakers to meet for a drink to discuss the day's proceedings and network in a relaxed atmosphere

STREAM B

10:45am - 12:45pm

TECHNICAL WORKSHOP 1

Computer forensics as an IT management problem

In recent years many organisations have used computer forensics to pursue internal investigations, respond to external threats, pursue or defend litigation and deal with security breaches. From originally being a "black art", forensics is fast becoming a mainstream discipline and an essential part of the information security function.

As computer forensics develops, it is increasingly becoming an IT problem that can be advanced through effective systems management. This session will look at how forensic processes can leverage technologies such as system virtualisation, SAN and NAS storage, network booting, remote control software, etc. Participants will see concrete examples of how forensic techniques can scale to enterprise environments using common technologies.

Owen O'Connor, Vice President, ISSA Ireland

2:00pm - 3:25pm

TECHNICAL WORKSHOP 2

My Dad's computer and the future of internet security

The computer world is mostly populated with naive computer users who just want to get their work done. They are easy prey for the writers of malware, and have not received much help from Microsoft in the past. The new Microsoft push for increased security was announced in February 2002. How well is it doing, and what does the future look like for various aspects of internet and computer security?

This talk is aimed at a technical audience, both in predicting some future successes and failures in internet security, and dealing with the current problems of widespread insecurity in Microsoft's operating system.

Bill Cheswick, Chief Scientist, Lumeta Corp, US



DAY 2

8:00 Registration and breakfast

Delegates are invited to beat the traffic by arriving early and having tea/coffee and pastries with colleagues courtesy of iQuest and The Sunday Business Post

PLENARY

8:45 Opening remarks and introductions from the morning chair

8:50 INTERNATIONAL KEYNOTE ADDRESS Mapping and visualising the internet and intranets

The Internet Mapping Project started at Bell Labs in 1998. It has revealed some interesting insights into the internet, and some really smashing posters! The techniques can be used to monitor disturbances in internet connectivity, such as fibre cuts or acts of war. These same techniques have been used to explore the extent and connectivity of large corporate and government intranets, which are generally hard to survey and manage.

A related technique has been used to identify

hosts that pierce perimeter network defences, bypassing firewalls and corporate policies. This presentation takes an in-depth look at this project, and its lessons for the big world.

Bill Cheswick, Chief Scientist, Lumeta Corp, US

IDENTITY AND ACCESS MANAGEMENT

9:30 Biometric identity management for governments and enterprises in the 21st century

- What is biometric identity management?
- How are governments and enterprises using it to protect their borders, citizens and assets?
- How can it enable legitimate travel and trade?

Clive Bourke, Vice President, Europe, Daon



10:00 Identity theft in Ireland

This session will include various experiences the gardai have had in investigating and dealing with cases of identity theft in Ireland and address some of the key issues arising from it.

- Chip & Pin
- Case Study

David Dowling, Detective Inspector, Garda Bureau of Fraud Investigation; Eugene Gallagher, Detective Superintendent, Garda Bureau of Fraud Investigation

10:30 Morning tea and exhibition viewing

HACKERS & THREATS STREAM A

10:50 The challenge of 'engineering' secure software products

Oracle has had a focus on building secure products from its inception in the late 1970s. Its products have undergone 19

external evaluations. Additionally, an internal hacking group actively tries to penetrate products. Secure programming practices and experience are employed to minimise security flaws. Nevertheless, Oracle also released critical security patches. This presentation discusses these experiences and outlines implications of secure product development for the wider software industry.

Patrick McLaughlin, Director of Security Solutions, Oracle, EMEA

11:20 Incident responses essentials: the react, respond and recover paradigm

- The current threat environment: Who are the perpetrators?
- **React:** policy and procedures review, triage, personnel management, information collection and appropriate action
- **Respond:** information gathering and assessment, stopping the attack, securing the crime scene, preservation of evidence, forensic examination, law enforcement involvement and root cause analysis
- **Recover:** raising security expectations, evaluation of the current security posture, creation of an implementation plan, oversight and validation of the implementation and after action review

Delegates should come away from this session with a greater understanding of the complex nature of information security, incident response and investigation management

Richard Starnes, Director of Incident Response, Cable & Wireless, UK



11:55 The dangers of Instant Messaging (IM): how to tackle emerging IM threats which bypass traditional security solutions - case study

- Opportunities of IM – commercial perspective



- Legal and operational aspects of IM
- VistaTec business and technical challenges: How does IM affect Irish businesses?

- IM security solution strategy at VistaTec: technology, deployment, value add

Jerry Lane, IT Manager, VistaTec & Mathieu Gorge, MD, Vigitrust

12:30 Lunch & exhibition viewing

STREAM A

1:45 Welcome back and introductions from the afternoon chair

Neil Wisdom, Sales Director, LAN Communications



1:50 INTERNATIONAL KEYNOTE ADDRESS

Information Security – What price must we pay?

This session will look at some of the technical security mechanisms, mainly cryptographic, used for protecting information and some of the political and social 'overheads' associated with them.

The use of technical security mechanisms (plus the fact that the same technology is used by both law enforcers and law breakers, by businesses and by individuals), leads to a number of social and political problems. Furthermore these technologies require a second infrastructure to establish trust and facilitate their secure implementation. Any defect in this second infrastructure could have profound consequences, as evidenced when trust is abused in political or accounting processes. The concept of abuse leads naturally to a discussion of privacy and human rights, together with the need to balance the 'rights' of individuals with the 'needs' of society.

Professor Fred Piper, Director of Information Security Group, Royal Holloway, University of London



2:25 Spam, viruses, phishing, fraud ... best practices in e-mail security - How to handle the rising threat to e-mail

- Analysis of the current threats facing corporate e-mail users – virus, spam, phishing, compliance, archiving, content, liability etc
- Future Problems – what the market is likely to face with the growth of associated protocols – IM, VoIP etc
- How to use e-mail effectively – simple steps to help corporates handle growing e-mail volumes and procedures to put in place to protect their users
- Solutions in the marketplace – pluses and minuses of the current approaches to handling e-mail



**Jeff Brainard, Senior Manager,
Product Marketing, Mirapoint**

AWARENESS, EDUCATION & TRAINING

2:50 Key Projects for 2005 - ISSA Member Survey Results

- What's top for budget requests?
- What are the top priorities for today's security professionals?
- How has legislation/regulation impacted 2005's project schedule?
- Survey results



**Paddy Roberts, President, ISSA
Ireland**

3:20 Afternoon tea and exhibition viewing

PLENARY

3:40 Build your own security culture

- Design a cost-effective awareness programme
- Engage your audience through creative activities
- Use metrics to grow the security culture



**Dr Gary Hinson, (CISSP, CISA, MBA)
Chief Executive, IsecT Ltd, UK**

INFORMATION SECURITY: THE FUTURE

4:10 LOCKNOTE ADDRESS

Will we ever stop internet hacking?

Internet hacking has been around now for over 20 years and shows no signs of diminishing; especially as what was once primarily the sport of technical geeks is now very firmly criminally organised, determined and clinical in its nature. Will organisations alone ever be able to keep apace with each new generation of hacker or will it eventually require greater intervention and control from the state and internet itself?



**Nigel Beighton, Director of Enterprise
Strategy, EMEA, Symantec Corp**

4:50 CONFERENCE ENDS

STREAM B TECHNICAL WORKSHOP 3

10:50am - 12:35pm

Wireless security fundamentals

With wireless technology becoming ubiquitous, many companies do not as yet have a clear idea of its potential impact on corporate security. In this session the policy aspect of wireless technology will be discussed along with options for securing data in a perimeterless network.

**Eoin Fleming, Chief Security
Specialist, HP Services Ireland**

TECHNICAL WORKSHOP 4

1:50pm - 3:25pm

Insider security threats

The presentation will cover a myriad of insider threats and how to combat them.

The main threats covered are:

- Rogue devices placed in your network
 - Port authentication or the lack of it in your network
 - Key stroke loggers placed on systems
 - LAN structure design and associated threats
 - Patching and the risk of not patching
 - USB and bootable CD-Roms – define the risk associated with having these devices enabled in your network
 - Information monitoring – where e-mail, for example, can be monitored in your network and outside of your network
 - Lack of logging – why you should log and correlate log information generated by your systems and security devices
 - Clear text protocols – why these protocols should not be used and what they can be replaced with
 - Social engineering – the risks and the education of staff requirements
 - Code review – the things developers don't do when they build software, which leave it open to exploitation
 - Remote control software – the risks of such software and how to deploy and use it securely
- With each threat a threat scenario will be provided. The presenter will then tell you how to combat against the threat in various ways taking into account the audience will be from small to large companies.*

**Myles Gallagher, Senior Technical
Security Specialist, IT Security
Operations, Allied Irish Bank**

Information Security **Looking For Direction?**

Information **Security** Specialists

Policy & Strategy

Penetration Testing

Computer Forensics

PBX Review

Systems Hardening

Application Security

IS 17799

Training

Rits Information Security Centre **2052 Citywest Business Campus** Co Dublin
Tel: +353 (0) 1 6420500 **E-mail: info@ritsgroup.com** www.rits.ie

Rits

Rits

Rits - Information Security Specialists

Rits is the premier independent provider of Information Security consulting and professional services in Ireland. Our vendor independence, superior levels of technical excellence and our 'security only' focus differentiate us from other providers.

Rits is a wholly-owned Irish company that was established in 1990. We count Ireland's leading companies and government departments among our clients. Internationally, Rits works with many leading financial institutions and technology companies.

Assurance Services

- Penetration Testing
- Application Security Testing
- Vulnerability Assessment
- SafetyNet
- Systems Hardening
- PBX Reviews
- War Dialling
- Wireless Assessments
- Network Security Reviews
- Database Security Reviews
- Anti Virus Health Checks
- Firewall Rules Review

Consulting

- Computer Forensics
- Policy Formulation/Review
- Outsourced Information Security Functions
- Strategic Planning
- Executive Briefings
- IS 17799
- Corporate Compliance

Design & Procurement

- System Design
- Managed RFP/RFT
- Vendor selection
- Implementation Management

Additional Services

- Training
- Staff Awareness Solutions
- Data Recovery

**Rits, Information Security Centre, 2052 Citywest
Business Campus, Co. Dublin**
Tel: +353 (0) 1 6420500
E-mail: info@rits.ie www.rits.ie

supported by



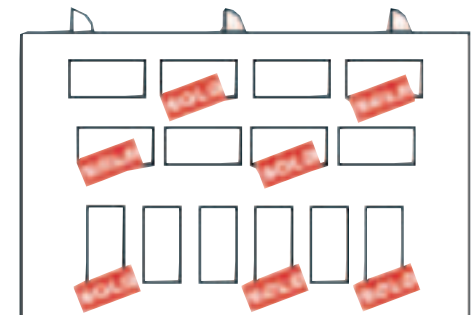
Confirmed sponsors include



Promotional Opportunities

A range of promotional opportunities exists allowing you to promote your business to IT decision makers attending this event. The opportunity is there for you to increase your brand profile, network and generate new business leads by:

- ◆ Hosting a lunch or drinks reception
- ◆ Booking an exhibition space at the conference
- ◆ Advertising in the delegate documentation pack



**Please contact Suzanne
Brennan on 087 9191292**

Booking form

First name

Last name.....

Title.....

Company

Nature of Business.....

Address.....

Tel.....

Mobile.....

Fax.....

E-mail

Please fill in the delegate name below as you would like it to appear on the delegate badge

If you do not want to receive information on other Sunday Business Post and iQuest events, please tick here

Registration fees

please tick as appropriate

Early Bird – registration and payment before February 9, 2005

 1 Day €440 plus Vat €92.40 = €532.40

 2 Day €680 plus Vat €142.80 = €822.80

Registration and payment after February 9, 2005

 1 Day €480 plus Vat €100.80 = €580.80

 2 Day €750 plus Vat €157.50 = €907.50

Which day?

Please tick which days and streams you will be attending

 Day 1 Morning Stream A or Stream B
 Day 1 Afternoon Stream A or Stream B
 Day 2 Morning Stream A or Stream B
 Day 2 Afternoon Stream A or Stream B

Special discounts

 Send three or more delegates from the same organisation and save 10 per cent (before Vat) off the total registration fee

 Members of the ISSA (Information Systems Security Association) are entitled to 10 per cent discount

Cancellations

Refunds are not available, but places are transferable once notice is given.

Payment must be received before the event

Method of payment

Payments by cheque made payable to The Sunday Business Post (Envelopes marked N.I.T.E.S)

Payments by credit card

Please tick appropriate box Visa Mastercard

Please charge to my account number

Expiry date

Amount Date..... Signed.....

THE SUNDAY BUSINESS POST

iQuest

NITES 4

National IT and E-Security Summit

Croke Park Conference Centre, Dublin

March 1 & 2, 2005



01-6026015 / 01-6026000



01-4786198



conference@sbpost.ie



thepost.ie/events/



The Sunday Business Post,
80 Harcourt Street, Dublin 2