

The 3rd annual

N.I.T.E.S

National IT & E-Security Summit

February 18 & 19, 2004 Croke Park Conference Centre, Dublin



supported by

Microsoft



invent

organised by

iQwest

THE SUNDAY BUSINESS POST

introduction

Now in its third 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 ideas are exchanged and relationships developed.

This year's event promises our most impressive line-up of national and international speakers. These experts 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 main sponsors personally for their support and contribution.

Microsoft®



invent



Computer Associates™

ENTERASYS
NETWORKS™

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

"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

"It was great to hear expert opinions 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

Sample list of companies who have attended previous N.I.T.E.S events:

- ESB
- Dept of An Taoiseach
 - Motorola
 - AccBank
 - Orix Ireland
 - Fianna Fail
 - Kingspan
- DNM Technology
- Performix Technologies
 - E.H.S.S
- 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
- EBS Building Society
 - Technomen
 - ROS Revenue
- Irish Software Assoc
 - Interpact USA
- Computer Associates
 - PwC
 - Sysnet
- Unitech Systems Ltd
 - Renaissance
- Microsoft BVBA / SPRL
 - RSA Security
- Systemhouse Technology
 - Sun Microsystems
 - Espion
 - Vordel
 - Ezitrust
 - Dept of Justice

Programme at a glance

- Meath County Council
 - CERT
- BDO Simpson Xavier
 - Eagle Star
- Public Prosecutions Dept
 - Penneys
 - BMC Software
 - Fyffes
- Dept of Agriculture
 - Zerflow
 - Celare
 - Newell & Budge
- Pfizer Drug Product Plant
 - Netfort ISS
 - TCM
 - De Royal Europe
 - CARA
 - Pearse Trust
- MGB & Associates
- Baltimore Technologies
- Landwell Solicitors
- Heineken Ireland
- Bank of Ireland
- Data Solutions
- FBD Insurance
 - Fexco
- Dept of Finance
 - Ernst & Young
 - Celestica
- Dublin City University
- Elan Pharmaceuticals
 - Kerry Group Plc
- Lan Communications
 - Accenture
 - Baker Consultants
- Fidelity Investments
 - EMC
 - Lecan Group
 - Asita
- Dept of Justice
 - Glanbia
 - Esat
 - Dairygold
 - Trinity
- Dept of Social Welfare
 - Friends First

DAY 1: February 18, 2004

Plenary

- Ministerial address
- Seeking the silver bullet against security attacks
- The economics of information security

Morning tea and exhibition viewing

Stream A	Stream B
<ul style="list-style-type: none"> ● Regulation & awareness ● The current firewall evolution ● Managing identity 	<p>Technical workshop 1</p> <p>Spam blocking</p>
LUNCH	LUNCH
<ul style="list-style-type: none"> ● Ensuring privacy, building trust ● Fraud and digital evidence ● Computer forensics 	<p>Technical workshop 2</p> <p>D.I.Y security testing</p>

Afternoon tea and exhibition viewing

Plenary

Update on Microsoft's trustworthy computing initiative

DAY 2: February 19, 2004

Plenary

- Navigating security while complying with mandates
- Dealing with Spam
- Defending the core: The need for monitoring

Morning tea and exhibition viewing

Stream A	Stream B
<ul style="list-style-type: none"> ● Network security management ● Wireless - the challenges ● The security profession 	<p>Technical workshop 3</p> <p>Defending your network</p>
LUNCH	LUNCH
<ul style="list-style-type: none"> ● Current business continuity realities ● Case Study 	<p>Technical workshop 4</p> <p>Target-based intrusion detection</p>

Afternoon tea and exhibition viewing

Plenary

Predictions on the future course of computer security

"Every single asset is a hope and a dream. IT better understand that."

"CIBC requires rock-solid reliability. Our customers trust us with billions in assets, which fuel both their business and personal ambitions. Our IT has to ensure their money is secure and always available.

"We're always looking for ways to push harder and get more out of IT. We have a mixed environment - from handhelds to mainframes - and we require a strategic partner to make it all work together, to make it invincible.

"HP Services came in, looked at our entire IT environment, and together, we designed the right outsourcing solution that cut costs, limited risk and has ultimately made us more flexible."

-Mike Woeller, CIO, Canadian Imperial Bank of Commerce

CIBC demands more from IT and HP makes sure they get it.



= everything is possible

www.hp.com/go/demandmore



keynote speakers



Ross Anderson

Ross Anderson leads the security group at the Computer Laboratory, **Cambridge University**, where he is Reader in Security Engineering. He is a Fellow of both the Institution of Electrical Engineers and the Institute of Mathematics and its Applications. **He has well known research publications on a number of security applications including medical privacy and banking systems**, as well as on the underlying technologies such as cryptography and tamper resistance. He is the author of the definitive book 'Security Engineering – A Guide to Building Dependable Distributed Systems'.

Most recently he has been one of the founders of the study of the economics of information security. Many security failures can be traced to inappropriate incentives rather than to simple technical errors, and the application of techniques from microeconomic theory has shed new light on a number of problems that were previously considered to be intractable.

Dr Anderson also chairs the Foundation for Information Policy Research, which is the main NGO in Britain for research into internet and technology policy issues.



David von Vistauxx

David von Vistauxx is the emeritus chairman of American Communications & Computation Incorporated and is a practitioner of the black art of computing. He is a former director and chairman of the audit committee of the publicly-traded Internet Growth Fund. **He has been practicing in the area of computer systems infrastructure and security since the late 1960s.** His clients include US government agencies as well as the

governments of Jamaica and the former Soviet Union. **He has presented at several international symposia including the American Society for Industrial Security, the Public Relations Society of America, the TransNational Crime and Corruption Conference and the International Association of Private Security Consultants.** He is a co-author of two books on Linux.

When not traveling internationally on business he spends his spare time working on the secure Linux kernel and writing device drivers for both Unix and Linux.



Marcus J Ranum

Marcus Ranum is a world-renowned expert on security system design and implementation. **He is recognised as the inventor of the proxy firewall, and the implementor of the first commercial firewall product.** Since the late 1980s, he has designed a number of groundbreaking security products including the DEC SEAL, the TIS firewall toolkit, the Gauntlet firewall, and NFR's Network Flight Recorder intrusion detection system. He has been involved at every level of operations of a security product business, from developer, to founder and Chief Executive of NFR. Marcus has served as a consultant to many FORTUNE 500 firms and national governments, as well as serving as a guest lecturer and instructor at numerous high-tech conferences. In 2001, he was awarded the TISC "Clue" award for service to the security community, and the ISSA Lifetime Achievement Award. Ranum is Senior Scientist at Trusecure Corporation, an international risk management firm. He serves as a technology adviser to a number of start-ups, established concerns, and venture capital groups.

secure

security

denied



DAY 1 FEBRUARY 18, 2004

7:45 Registration and breakfast

Delegates are invited to beat the traffic by arriving early and having a light breakfast with colleagues courtesy of iQuest and The Sunday Business Post



skilled security experts, what's the solution? Better automation is a good starting point. But technology alone isn't enough. Leading-edge companies are adopting a more comprehensive approach that combines policies, people and technology.
Tony Redmond, Chief Technology Officer, HP Services Worldwide

PLENARY

8:30 Opening remarks and introduction from the morning chair



Maurice Mortell, Chief Executive, Data Electronics Group

8:40 Ministerial address: Mary Hanafin, TD, Government Chief Whip and Minister of State



MANAGEMENT AND AWARENESS

9:00 OPENING ADDRESS: Seeking the silver bullet against security attacks

When companies learned how to harness the power of the web to enable e-business and online commerce, they found a powerful new tool to link customers, suppliers, partners and employees. But the striking success of online commerce has come at a hefty price: companies are now much more vulnerable to security attacks, which by some measures are doubling every year. Indeed, the threat level has forced some companies to reconsider how they conduct their online business.

With security incidents increasing steadily and companies facing a dearth of

9:40 INTERNATIONAL KEYNOTE ADDRESS: The economics of information security

Do we spend enough on keeping 'hackers' out of our computer systems? Do we not spend enough? Or do we spend too much? For that matter, do we spend too little on the police and the army, or too much? And do we spend our security budgets on the right things?

The economics of security is a hot and rapidly growing field of research. More and more people are coming to realise that security failures are often due to perverse incentives rather than to the lack of suitable technical protection mechanisms. (Indeed, the former often explain the latter.) While much recent research has been on 'cyberspace' security issues – from hacking through fraud to copyright policy – it is expanding to throw light on 'everyday' security issues at one end, and to provide new insights and new problems for theoretical computer scientists and 'normal' economists at the other. In the commercial world, as in the world of diplomacy, there can be complex linkages between security arguments and economic ends.



Dr Ross Anderson, Computer Laboratory, University of Cambridge, Britain

10:30 Morning tea and exhibition viewing

STREAM A

LEGAL AND REGULATORY

11:00 Regulatory requirements and awareness: Current needs and future programmes

- Complying with local and European data protection and software licensing laws
- Formation of contracts by e-mails: harassment laws; and safety at the workplace, which are also vital to corporate security strategies
- Asset classification and management
- Physical security and people security

Paul Lambert, Partner, Merrion Legal & Mathieu Gorge, Managing Director, Vigitrust

SECURING TECHNOLOGIES

11:30 New directions in firewalls and virtual private networks

- Most mid to small enterprise companies are using firewalls... are they really secure?
- The current firewall evolution – multi-layer security gateways
- Virtual Private Networks – Firewall to firewall

Niall Moynihan, Northern European Technical Director, Check Point Software Technologies, Inc

12:05 Mismanaging identity and access costs millions

- Managing identity is fundamental to managing security
- Multiple identities increase costs and operational risk as well as reducing effectiveness
- Smart technology can improve user experience while strengthening access controls and reducing costs
- This session describes practical approaches that can be used to improve identity and access management

Mike Small, C.Eng, FBCS, MIEE, Director of eTrust Strategy, Computer Associates



12:45 Lunch & exhibition viewing

STREAM A

2:05 Welcome back and introduction from the afternoon chair

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



2:10 PANEL DISCUSSION – Ensuring privacy... building trust

- Are EU directives making security more difficult to achieve in Europe?
- How do we ensure future privacy initiatives do not impact security practices?
- Should vendors become liable for insecure products?
- What are the emerging drivers of security investment?

Panellists will comprise leading industry figures including:

**Dr Ross Anderson, University of Cambridge, Britain
Conall Lavery, Managing Director, Entropy
Ahmed Patel, CNDSRGroup, Dept of Computer Science, University College Dublin**

INFORMATION INFRASTRUCTURE PROTECTION

2:55 Internet Investigations and digital evidence: The Garda Bureau of Fraud Investigation

- Policing your network (detection / prevention)
- Identifying and handling digital evidence
- Some examples
- New developments in digital theft, online scams and cybercrime in Ireland

Detective Superintendent Eugene Gallagher & Detective Sergeant John Finan, Garda Bureau of Fraud Investigation, Computer Crime Unit

3:30 Help, I have an incident!

**A short course in computer forensics
Colman Morrissey, Managing Director, Espion**

Your potential. Our Passion.™

Microsoft®

**Securing your network
requires a team of 10.**

The "team" is you.

**Introducing Microsoft® Windows
Server 2003. Do more with less.**

You're being asked to do more. You're being asked to do it with less. Microsoft® Windows Server™ 2003 is a server operating system that helps you do more with less. For example, solutions built on Windows Server 2003 can help you use the technology you have to increase efficiencies across your entire organisation, giving you the performance of big, high-priced systems, but with smaller management and financial commitments. For more information, go to www.microsoft.com/security. **Software for the Agile Business.**


Microsoft
Windows Server System

3:40 Afternoon tea & exhibition viewing

4:05 LOCKNOTE ADDRESS: Update on Microsoft's trustworthy computing initiative: all talk and action

Microsoft remains committed to Trustworthy Computing (TwC), a long-term vision that describes a time when people will be able to rely on their computing systems for dependable service. Microsoft has always maintained that this will take incredible investment and effort from themselves and the industry over many years. From a security perspective, TwC means reducing vulnerabilities in code and making software more resistant and resilient to attack. The security review of Windows Server 2003 was an important step along the path of TwC and you should expect there will be other evolutions as we make software more and more trustworthy.

- Reflections – the impact of the initiative to date
- Improving the patch management experience for customers – our response to customers
- Futures – raising the bar

Dr Detlef Eckert, Senior Director for Trustworthy Computing, Microsoft & Jonny Chambers, Platform Strategy Manager, Microsoft Ireland



4:50 – 6.00 Drinks 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

Technical workshop 1 SPAM BLOCKING



Marcus Ranum
11:00 – 12:50

If you're like most people, somewhere between 1/2 and 3/4 of the e-mails you get are junk e-mails ('spam'), but you don't have to tolerate it. There are new technical responses to the flood of spam that make it likely that the spammers will give up in the next four or five years. In this workshop, you will get a whirlwind overview of the state of the art in spam blocking.

Topics:

- What is spam and how bad is the problem?
- The death of spam?
- Eroding the spammers' vocabulary
- Eroding spammers' ability to make money
- A simple and effective antispam architecture built from open source tools

Technical workshop 2 D-I-Y SECURITY TESTING

Eoin Fleming, ISSA
(Information Systems Security Association)
2:00 – 3:45

Until recently, if you needed a security review you could bring in consultants or develop your own testing methodology – a significant commitment either way, whether in financial outlay or staff time. This workshop will introduce an alternative – a way to conduct your own security tests using a standard process.

The presenter will outline his experiences with the Open Source Security Testing

Methodology Manual (OSSTMM), which is a community initiative to develop standards and techniques for security testing. The OSSTMM process can be used either to perform in-house security testing or to maximise return on third-party testing.

This practical workshop will provide attendees with the basics of this exciting security testing methodology, as well as concrete ideas for applying it to their own organisation.

DAY 2 February 19, 2004

7:45 Registration and breakfast

Delegates are invited to beat the traffic by arriving early and having a light breakfast with colleagues courtesy of iQuest and The Sunday Business Post

8:30 Opening remarks and introduction from the morning chair

Conall Lavery, Managing Director, Entropy Ltd

8:40 INTERNATIONAL KEYNOTE ADDRESS: Navigating security while complying with mandates

The complexity of today's technological society is easily matched by the complexity of the mandates imposed by governments, customers and trading partners. Whether you are subject to HIPAA (a US Mandate), Basel II (an International Mandate), or Regulation (EC) No 45/2001 (a European Mandate), or you have litigious customers, your security decisions are drastically influenced by non-security related issues.

And yet, to define e-security by these parameters is to move against a constantly varying target. The motivations behind each of the players are contradictory and over time are subject to radical external influence. There is no technology-based 'silver bullet' that can provide security under these circumstances; There is no regulatory-based 'silver bullet' that can provide security under these circumstances; and there is no vendor – supplied 'silver bullet' that can provide security under

these circumstances.

We must set a definition of 'Security' within this context and provide a roadmap for the process of achieving 'Security' within this definition.

David von Vistauxx, Chairman (Emeritus) of American Communications & Computation, Inc.



SECURITY INFORMATION MANAGEMENT

9:30 Dealing with Spam

- Innovative measures for distinguishing spam from legitimate e-mail
- Learn how far we've advanced in the war against spam, the obstacles that remain and an anti-spam solution for your organisation
- Case Profile

Steve Munford, Global Vice President, Messaging, Sophos Plc



10:00 Defending the core: The need for security monitoring

It is an almost universal truism that wherever controls are important, monitoring is important as well. If locked doors and vaults kept burglars out of banks, there would be no need for security cameras and guards. If laws were universally abided by, would there be a need for police officers and courts? As long as people continue to violate speed limits and run red lights, there will always be a need for radar guns and point systems. Even in the world of accounting there is the need for both monitoring and control. If everyone followed budgets there would be no need for financial reporting or auditing. There will never be perfectly secure networks, so there will always be the need for security monitoring. Learn here about passive network discovery, vulnerability monitoring and management, as well as how to eliminate false positives/negatives and the benefits of intelligent traditional intrusion detection systems (IDS) response.

Dominic Storey, Technical Director, Sourcefire EMEA

10:30 Morning tea and exhibition viewing



STREAM A

ADVANCED SECURITY OPTIONS

10:55 It's not about network security, it's all about secure networks



A holistic solution that integrates security across the enterprise, delivering in-depth defence from the edge to the core...

Daniel Mothersdale, Marketing Director, NoE, EMEA, Enterasys Networks

11:30 Wireless LAN security – today and tomorrow

- Status on environment today
 - Challenges
 - Today's solutions
 - Case study
 - Tomorrow's solutions standards
 - Evolution of wireless security within the client
- Andrew Greenhalgh, Mobile Marketing Director EMEA, Intel**



12:10 The future of the security profession

- How our security profession has developed, in Ireland and internationally
- The drivers influencing the information security profession
- What does the future hold for us as professionals?
- What can we do to succeed – skills, education, professional development?

Paddy Roberts, Director of IT Security, Elan Corporation

12:45 Lunch & exhibition viewing

2:10 Welcome back and introduction from the afternoon chair

Greag Purcell, Director of Sales and Marketing, Hibernia College

STREAM A

2:15 Case study – Evolution of security within the lifecycle of an eBusiness system

This presentation will look at the implementation of an eBusiness System in a major Irish Institution:

- Detail of Risk assessment and countermeasures deployed
 - Account of the phases of security evolution which the solution has gone through
 - Looking to the future and the next phase of security evolution
- Kelvin Garrahan, IT Security Consultant, Hewlett-Packard**

RISK AND AUDIT

2:45 KEYNOTE ADDRESS: Enterprise business continuity: Current realities

- Current business continuity realities
- Business continuity and corporate governance
- Cornerstones to effective business continuity management
- Integrating business continuity into day to day business as usual

Karen McEntegart, Director, RMI Business Continuity Services

Karen McEntegart heads up RMI's Business Continuity Services. She has proven practical experience in creating and leading the innovation of business continuity plans, including the recent US blackout, hurricanes, transportation strikes, Year 2000 and 9/11. Karen was a prominent member of the Wall Street business continuity community, which includes liaising with the SEC and Federal Reserve on the joint Agencies white paper to strengthen the resilience of US financial markets, following 9/11.

3:40 Afternoon tea & exhibition viewing

THE FUTURE

4:05 INTERNATIONAL LOCKNOTE **ADDRESS: Predictions on the future course of computer security**

Computer security is a field that is evolving rapidly and is therefore subject to trends, hype, consolidation and introduction of destabilising technologies. Marcus Ranum, one of the 'old timers' of the security industry, and a designer of many key security technologies (firewalls, VPNs – virtual private network and IDS), will offer his projections about the state of the industry and the direction it is likely to follow in the next five years.

- Which technology drivers will be dominant in the next five years and why
- Which technologies are likely to succeed and which will fall by the wayside
- The death of general purpose computing and the art of system administration
- Microsoft monoculture and world domination: What to do

Marcus Ranum, Senior Scientist, Trusecure Corp, US

5:00 Conference closes

STREAM B

Technical workshop 3 **DEFENDING YOUR NETWORK – A WORM'S-EYE-VIEW**

Owen O'Connor ISSA (Information Systems Security Association) & Jonny Chambers, Platform Strategy Manager, Microsoft

10:50 – 12:50

Although network worms have been with us since the 80s, recent worms such as Blaster, Slammer and Nachi have shown their destructive potential. Many companies were surprised that they were affected, despite PC anti-virus and e-mail

filtering packages.

Network worms spread so quickly that only automated prevention, detection and removal methods stand a chance – a 'worm's-eye-view' is needed, assessing the network in a comprehensive and automated manner.

In this practical session, Owen O'Connor of the ISSA and Jonny Chambers of Microsoft will look at the threat of network worms, how they spread, and how you can protect against them. Real-world examples will show the exposures which worms exploit – and which you can easily address using the free tools and techniques you will pick up in this workshop.

Technical workshop 4 **TARGET – BASED INTRUSION DETECTION – THE FUTURE OF IDS TODAY!**



Dominic Storey, Technical Director, Sourcefire EMEA
2:00 – 3:45

One of the inherent issues with traditional intrusion detection systems (IDS) is that a fundamental lack of information leads to a great deal of ambiguity – sensors operate with virtually no knowledge of the composition of the network components that they are defending. Passive network profiling systems solve this problem by providing persistent information about all of the active components of a network that provide the contextual data required to disambiguate, or give the true perspective of the environment in which the IDS is operating, allowing the IDS to start protecting assets, not protocols or traffic

- The current state of IDS technologies
- The critical missing link
- Network awareness
- Introducing target-based intrusion detection

Microsoft®

Microsoft in Ireland has three operations: Microsoft European Operations (EOC), Microsoft European Product Development Centre (EPDC) and Microsoft Ireland. Across these three operations, Microsoft employs the largest number of employees in the Irish software sector. Microsoft technologies are designed to deliver optimum business value to customers through the integrated and innovative solutions that help businesses be more productive and secure.

Microsoft European Operations (EOC), which began operation in 1985, provides key support for the company's sales & customer support activities across some 85 different countries, and transacts in 18 currencies. Microsoft European Product Development Centre (EPDC) began in 1988 and is an intrinsic part of the development cycle of over 100 products in 27 different languages. Microsoft Ireland was established in 1991 and with a team of 60 people, based in offices in Dublin and Belfast, manages all sales, marketing and technical support for partners and customers of all sizes from enterprise customers, to small and medium sized businesses and home computer users.



HP Services can provide guidance for all aspects of information security, from strategy to implementation, with a team of experts dedicated to the field of information security. We help customers evaluate, architect and implement security and privacy programs necessary to earn the trust of their business partners and their customers.

HP takes a holistic view of the people, processes and technology to ensure enterprise-wide security. This means HP recognises the importance of the whole and the interdependence of its parts. HP's goal is to protect an organisation's privacy, intellectual property and the enterprise itself from intentional or unintentional harm or exposure.

With decades of experience in securing global business

assets, HP offers its clients a comprehensive portfolio of security services of the highest quality based on proven methodologies and best-in-class technologies that provide solutions for all of a company's security requirements.

HP is Ireland's largest IT organisation with over 4,000 employees nationwide. Security is one of four strategic initiatives for HP Services worldwide. In 2003 HP received the Secure Computing Magazine award for Best Security Service. This award recognises the quality and breadth of the offering, as well as the ability to meet the advice, management and solution delivery requirements of clients.



Computer Associates™

Computer Associates International, one of the world's largest software companies, delivers software and services that enable organisations to manage their IT environments. Focus areas include network and systems management, storage and security management, portal and business intelligence and application life-cycle management.

CA's eTrust security management solutions offer a holistic approach to business security management – whatever the business model or organisational structure – enabling an enterprise to quickly and effectively embrace new opportunities, improve operational efficiencies, reduce costs and proactively manage threats to its physical access and IT security. The three solution areas – eTrust Identity Management, eTrust Access Management and eTrust Threat Management are brought together with unified visualisation and management through eTrust Security Command Center.

Founded in 1976, CA is headquartered in Islandia, New York, and operates in more than 100 countries. For more information on CA, please visit <http://ca.com> or contact us at:

Computer Associates, Embassy House, Ballsbridge, Dublin 4

Phone: +353 1 607 7300

e-mail: ca.Ireland@ca.com



Confirmed sponsors include the following

Microsoft®



i n v e n t

ENTERASYS

NETWORKS™



Computer Associates™



www.ipoptions.com

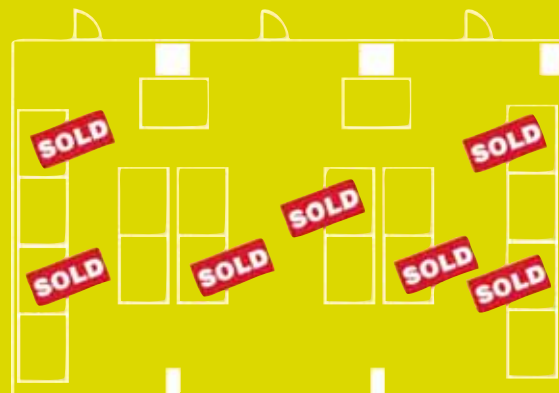
supported by



sponsorship

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.

For further information on promotional opportunities call Suzanne Brennan on 01-6026000



Who should attend?

N.I.T.E.S 2004 is specifically designed for enterprise, government and corporate managers responsible for identifying, evaluating, selecting and purchasing security technologies within your organisations, including:

- **Managing Directors/CEOs**
- **CTOs / CIOs**
- **Directors/Managers IT Security**
- **Security Consultants**
- **Systems Managers/Engineers**
- **Telecommunication Directors / Managers**
- **e-Business Managers / Directors**

BOOKING FORM

First name

Last name.....

Title

Company

Nature of Business.....

Address.....

.....

Telephone.....

Mobile.....

Fax.....

E-mail

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

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

.....

METHOD OF PAYMENT

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

Payments by credit card

Please tick appropriate box

Visa Mastercard

Please charge to my account number

□□□□/□□□□/

□□□□/□□□□

Expiry date □□/□□

Amount

Signed.....

Date

REGISTRATION FEES

please tick as appropriate

Early Bird - registration before January 29 2004

1 day € 400 plus Vat €84 = €484

2 days € 650 plus Vat €136.50 = €786.50

Please tick which days and streams you will be attending

Registration after January 29 2004

1 day € 450 plus Vat €94.50 = €544.50

2 days € 700 plus Vat €147 = €847

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.

5 EASY WAYS TO REGISTER



01-602 6000/602 6043



01-478 6198



conference@sbpost.ie

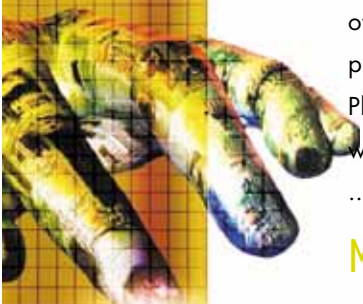


thepost.ie/events/



The Sunday Business Post,
80 Harcourt Street, Dublin 2

secure



denied



The 3rd annual **N.I.T.E.S**
National IT & E-Security Summit
February 18 & 19, 2004 **Croke Park Conference Centre, Dublin**



The Sunday Business Post, 80 Harcourt Street, Dublin 2

tel: 01-6026000 fax: 01-4786198 e-mail: conference@sbpost.ie web: www.thepost.ie/events/