ISACA®

Two Conferences in One Location!

Information Security Management Conference

Providing Strategic Vision for
Information Security Managers
Visit ***www.isaca.org/infosecurity*** for details.

Network Security Conference

Providing the Essentials to
Secure Your Network
Visit ***www.isaca.org/nsc*** for details.

10-12 November 2008
NH Grand Hotel Krasnapolsky
Amsterdam, The Netherlands

Register Now and Save!

Earn up to **32** CPE credits for the event of your choice.

10-12 November 2008

Information Security Management Conference:
Providing Strategic Vision for Information Security Managers

ISACA® is pleased to offer its 4th annual European Information Security Management Conference, designed for experienced information security managers and those who have information security management responsibilities. The combination of management focus and highly detailed content will provide you with an opportunity to customise your conference experience to meet your specific interests and professional needs. Experienced professionals as well as new or aspiring Certified Information Security Manager® (CISM®) holders will find great value in the conference.

Network Security Conference:
Providing the Essentials to Secure Your Network

ISACA's 8th annual European Network Security Conference is uniquely designed to meet the education and training needs of the seasoned information security professional as well as the newcomer. Whether you are an experienced information security professional keeping pace with complex network environments, an information systems (IS) audit professional in search of detailed knowledge and competencies on specific topics, or an IS control professional seeking information on guarding one of your organisation's most important assets, this year's Network Security Conference will benefit you.

Keynote Address

Kim Aarenstrup
Chief Information Security Officer
A.P. Moller-Maersk

Information Security Wall-to-Wall

Kim Aarenstrup, chair of the Information Security Forum and chief information security officer of the global shipping, oil and retail conglomerate A.P. Moller-Maersk, will address information security through his knowledgeable and varied perspective. In Aarenstrup's 10 years of heading the information security programme in his company, he has achieved what could be called wall-to-wall information security coverage, allowing the enterprise to function without any business disturbance from security incidents for the past six years. The company mantra is that information security must happen below the business radar. Only what cannot happen that way needs to be brought to the attention of the business.

Aarenstrup also has a law enforcement background, being the prime mover in establishing the first high-tech crime unit in Denmark under Copenhagen Police in the mid-1990s.

Conference Streams

Information Security Management Conference—Stream I

CISO Panel Discussion—Security by Compliance

Moderator: Hugh Penri-Williams, CISM, CISA
Former CISO, Alcatel Group

Panelists: Kim Aarenstrup, John Kirkwood

A panel of distinguished information security managers will engage in a lively discussion and debate on hot topics and the future of information security. At various times in the discussion, the panel will take questions from the floor. Join us for 90 minutes of insights and predictions from leaders in the information security profession.

Topics include:
- An update on the impact of new regulations
- Trends in the security manager's role as it relates to corporate governance
- Compliance: What works and what does not
- Leveraging security standards and *Control Objectives for Information and related Technology* (COBIT®) to achieve governance
- Ensuring security is funded at the right level—expectations for increase or decrease in IT and security spending
- New threats of greatest concern and how to deal with them
- Likely evolution of the security manager's role over the next two years

Prerequisites:
The participant should have information security management experience and an understanding of information security technology, concepts, terminology, policies, procedures and techniques.

111
Privacy and Security Awareness ▲

Todd Fitzgerald, CISM, CISA
Systems Security Officer
National Government Services

Participants will learn more about:
- Techniques for making security awareness fun
- Seven steps for a successful awareness programme
- Creating innovative, interactive security awareness programmes
- Assessing awareness effectiveness
- Tailoring the message

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

121
Threat and Vulnerability Analysis ▲

John Pironti, CISM, CISA, CGEIT
Chief Information Risk Strategist
Getronics

Participants will learn more about:
- Threat and vulnerability management programmes
- Threat analysis—who, what, when, where and how
- Open Systems Interconnection (OSI) and OSI methodology
- Vulnerability analysis
- Risk mitigation strategies
- Technological options to assist in the operations of the programme

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

211
Skills Necessary to be an Effective Security Leader ▲

Todd Fitzgerald, CISM, CISA
Systems Security Officer
National Government Services

Participants will learn more about:
- The skills necessary to communicate with business leaders
- Making the transition from technical to business
- Communicating with senior management
- Understanding different reporting models
- The future of the chief information security officer (CISO)

Prerequisites:
The participant should have information security management experience and an understanding of information security technology, concepts, terminology, policies, procedures and techniques.

221
Designing and Implementing Vendor Security Compliance Programmes ▲

Peter Taylor
Information Security Manager
Bradford & Bingley Plc

Participants will learn more about:
- Key elements of an effective vendor security management programme
- Identifying business and regulatory drivers and their impact on programme design
- Overcoming challenges inherent in implementing and maintaining a global programme with multiple and diverse vendor relationships
- Developing metrics and measures that drive successful programme compliance
- Programme maintenance strategies that meet the needs of diverse organisations

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

B Basic ▲ Intermediate A Advanced
Note: One person's intermediate level may be another person's advanced. Please review session descriptions and prerequisites to determine if the session is appropriate for you.

231
Information Security Offshore: What to Expect and How to Cope ▲

Michael Bacon
Information Security Compliance Director
Williams Lea

Participants will learn more about:
- The different security issues that exist
- Practical approaches to meeting security needs
- How to satisfy privacy and data protection requirements
- Managing information security remotely

Prerequisites:
The participant should have at least three years of IT information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

241
Metrics, Measures and Myths ▲

Ramsés Gallego, CISM
General Manager
Entel Security & Risk Management

Participants will learn more about:
- Meaningful metrics for security management
- Technical measures to effective tactical and strategic security metrics
- The design and development of metrics to guide the security programme in the organisation

Prerequisites:
The participant should have at least five years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

311
Competitive Intelligence and IP Protection ▲

Meenu Gupta, CISM, CISA
President
Mittal Technologies

Participants will learn more about:
- Intellectual property (IP)-related issues and global laws of its governance
- The World Intellectual Property Organization and international copyrights treaties
- The latest European/American joint initiatives towards patent applications
- Threat of industrial espionage and competitive intelligence
- Examination of industries most subjected to IP protection issues—European and global statistics on thefts/piracy
- Available tools and technologies and digital rights management
- The basic laws of IP protection—due diligence and due care

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

B Basic ▲ Intermediate A Advanced

Note: One person's intermediate level may be another person's advanced. Please review session descriptions and prerequisites to determine if the session is appropriate for you.

321
Web 2.0—How Secure Are Your Applications? ▲

John Burroughs
Senior Security Architect
Watchfire, an IBM Company

Participants will learn more about:
- Why Web 2.0 is a sleeping-giant security risk
- Common Web 2.0 vulnerabilities
- How vulnerabilities occur and what can be done to prevent them
- Protecting against existing threats and general best practices to combat emerging attacks
- Building effective application security testing into the systems development life cycle

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

Information Security Management Conference—Stream 2

112
Security Knowledge Management ▲

John Kirkwood
Chief Security Officer
Royal Ahold N.V.

Participants will learn more about:
- Implementing a knowledge management process and capability
- The knowledge management process as a reasonable balance between the due diligence security practices and the demonstration of due diligence for multiple stakeholders
- Two financial service firms that have implemented this process
- The knowledge management framework as a combination of core processes, work flows and a repository of artifacts

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

122
Using CobiT, ITIL and the ISO 27000 Series for Business Benefit ▲

Yves LeRoux, CISM
Technology Strategist
CA Inc.

Participants will learn more about:
- IT good practices as a critical component to the success of the enterprise strategy
- Why a management framework is needed
- The three specific practices and standards that are becoming widely adopted around the world—CobiT, Information Technology Infrastructure Library (ITIL) and ISO/IEC 27000 Series

Prerequisites:
The participant should have at least five years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

212
Transforming Information Security to Information Risk Management ⚠

John Pironti, CISM, CISA, CGEIT
Chief Information Risk Strategist
Getronics

Participants will learn more about:
- The evolution of electronic business and the introduction of disruptive technologies to enhance business capabilities
- The transformation of a proactive and risk-based approach to information assurance
- The introduction of the risk office and the position of the chief risk officer, threat and vulnerability management, compliance management, and business risk management

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

222
The Value of Certification and Professional Development in the Security Profession ⚠

Vernon Poole, CISM, CGEIT
Head of Business Consultancy
Sapphire

Participants will learn more about:
- Ongoing survey results that discuss why certification in the security profession is gaining global appeal
- What the Certified in the Governance of Enterprise IT™ (CGEIT™) certification means for senior management working towards continuous monitoring for constant vigilance
- Developing a career path road map for professional development using certification programmes in the security profession
- Mentoring and coaching programmes for implementing the road map

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with terminology, approaches, methodologies and techniques.

232
Convergence of Security and ERM ⚠

A Panel Discussion

Participants will learn more about:
- The current concept of security and enterprise risk management (ERM)
- Security as a component of ERM and how the organisation benefits from an expanded view of ERM
- Approaches security managers can take in integrating risk concepts with ERM
- Research compiled by The Alliance for Enterprise Security Risk Management™ (AESRM™)

Prerequisites:
The participant should have information security management experience and an understanding of information security technology, concepts, terminology, policies, procedures and techniques.

242
Business Continuity Management ⚠

Hugh Penri-Williams, CISM, CISA
Senior Security Advisor
Accenture, Paris

Participants will learn more about:
- Why business continuity management (BCM) is a duty rather than merely an option
- How BCM fits into information security governance and enterprise risk management
- What range of activities are covered by BCM
- Which elements constitute good BCM
- How BCM is put into practice and maintained
- Characteristics of successful BCM

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

312
Continuous Controls Monitoring ⚠

Vernon Poole, CISM, CGEIT
Head of Business Consultancy
Sapphire

Participants will learn more about:
- The roles of internal security and management in continuous monitoring
- Implementing continuous monitoring and the challenges of doing so
- Identifying control points
- The tools and techniques to utilise in the continuous monitoring process

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

322
IT Control Objectives for Basel II ⚠

Robert White, CISA
Operational Risk Manager
ING Bank

Participants will learn more about:
- A framework for managing operational and information risk in the context of Basel II
- The evolving regulatory landscape
- The need to manage operational risk
- IT control objectives for Basel II
- The use of key IT risk indicators

Prerequisites:
The participant should have at least three years of information security management experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques to manage the IT environment. Managerial experience will be helpful for this session.

Network Security Conference—Stream 3

113
Networked-based Services ▲

Rene Pluis
System Engineer
Cisco Systems

Participants will learn more about:
- Network services such as load balancing and firewalling
- Extensible Markup Language gateways and message stream manipulation and checking
- The relevance to application developers
- What this could mean to business processes and security/auditing

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

123
Revealing the Secrets of the E-crime Underworld ▲

Maksym Schipka
Senior Architect
MessageLabs Inc.

Participants will learn more about:
- The parallels between the legitimate commercial world and the shadow economy
- Gaining an insight into the mechanics of the shadow economy
- The buying chain and how profit is made
- Identifying the key players in the shadow economy and where they reside

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

133
Anatomy of Evolving Threats ▲

Roel Schouwenberg
Senior Anti-Virus Researcher
Kaspersky Lab

Participants will learn more about:
- The evolution of the malware ecosystem
- The anatomy of a malware attack, including a live demonstration
- Threat analysis: who, what, when, where and how
- Risk mitigation strategies from a technical perspective

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

213
Next Generation Network Security Tools ▲

Gene Schultz, CISM (Honorary)
Chief Technology Officer
High Tower Software

Participants will learn more about:
- What differentiates next-generation network tools from current types of network tools
- Types of next-generation tools and how they work
- The likely implications that next-generation network tools will have on the practice of information security and auditing

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

223
PCI Compliance: A Realistic Approach ▲

Simon Langley
Principal
KPMG

Participants will learn more about:
- Payment Card Industry (PCI) Data Security Standards (DSS) compliance—what is it all about
- How not to reinvent the wheel and how to capitalise on efforts made for other compliance programmes
- General gaps and how to effectively remediate them
- How to sustain your PCI DSS compliance status

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

233
Penetration Testing ▲

Peter Wood
Chief of Operations
First Base Technologies

Participants will learn more about:
- The strengths and weaknesses of penetration testing and vulnerability assessment techniques
- The steps involved in both external and internal penetration tests
- Popular vulnerability and penetration testing tools and how to interpret their results
- Finding out-of-date services and software and why it matters
- Checking the results of automated tools manually

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

B Basic ▲ Intermediate A Advanced

Note: One person's intermediate level may be another person's advanced. Please review session descriptions and prerequisites to determine if the session is appropriate for you.

313
Developing, Designing and Auditing an Integrated Incident Response Programme

Marc Vael, CISM, CISA
Executive Director
Protiviti Belgium

Participants will learn more about:
- Designing and auditing an integrated incident response programme
- Coordinating the activities of the enterprise teams in the event an incident occurs
- Implementing an integrated response plan
- How to respond to an incident when regulations and laws conflict
- Understanding what to include in an incident response plan

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

323
Devise a Strategy to Mitigate Malware

Yuval Ben-Itzhak
Chief Technology Officer
Finjan Inc.

Participants will learn more about:
- New techniques behind the latest web threats, such as code obfuscation, antiforensic, evasive and crimeware tool kits
- The mounting challenges in crimeware prevention
- Recent, real-world examples of crimeware found on compromised legitimate web sites and their impact on businesses and individuals
- The commercialisation of stolen data and malware
- New technologies that can prevent crimeware attacks before impacting business organisations and members of the community

Prerequisites:
The participant should have at least five years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

Network Security Conference—Stream 4

114
Networks and Their Fuzzy Boundaries

Wendy Goucher
Security Empowerment Consultant
Idrach Ltd.

Participants will learn more about:
- Security indiscretion and careless behaviour that allows information to be gained by a casual observer
- Organisational requirements including mobile staff and the ability to contact flexible and mobile staff
- Data leakage from mobile devices
- The study of mobile usage using cognitive psychology to gain insight as to why people are so indiscrete when working and speaking in public
- The risks created when moving information outside to the care of partners or customers

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

124
Lifestyle Device Security

Andrew Yoemans
Vice President Global Information Security
Dresdner Kleinwort

Participants will learn more about:
- Current devices and the security they require
- Establishing a security policy to accommodate various devices and usage while ensuring operations continue
- Communicating the policy to staff

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

134
Data Loss Prevention: Concepts and Solutions

Ramsés Gallego, CISM
General Manager
Entel Security & Risk Management

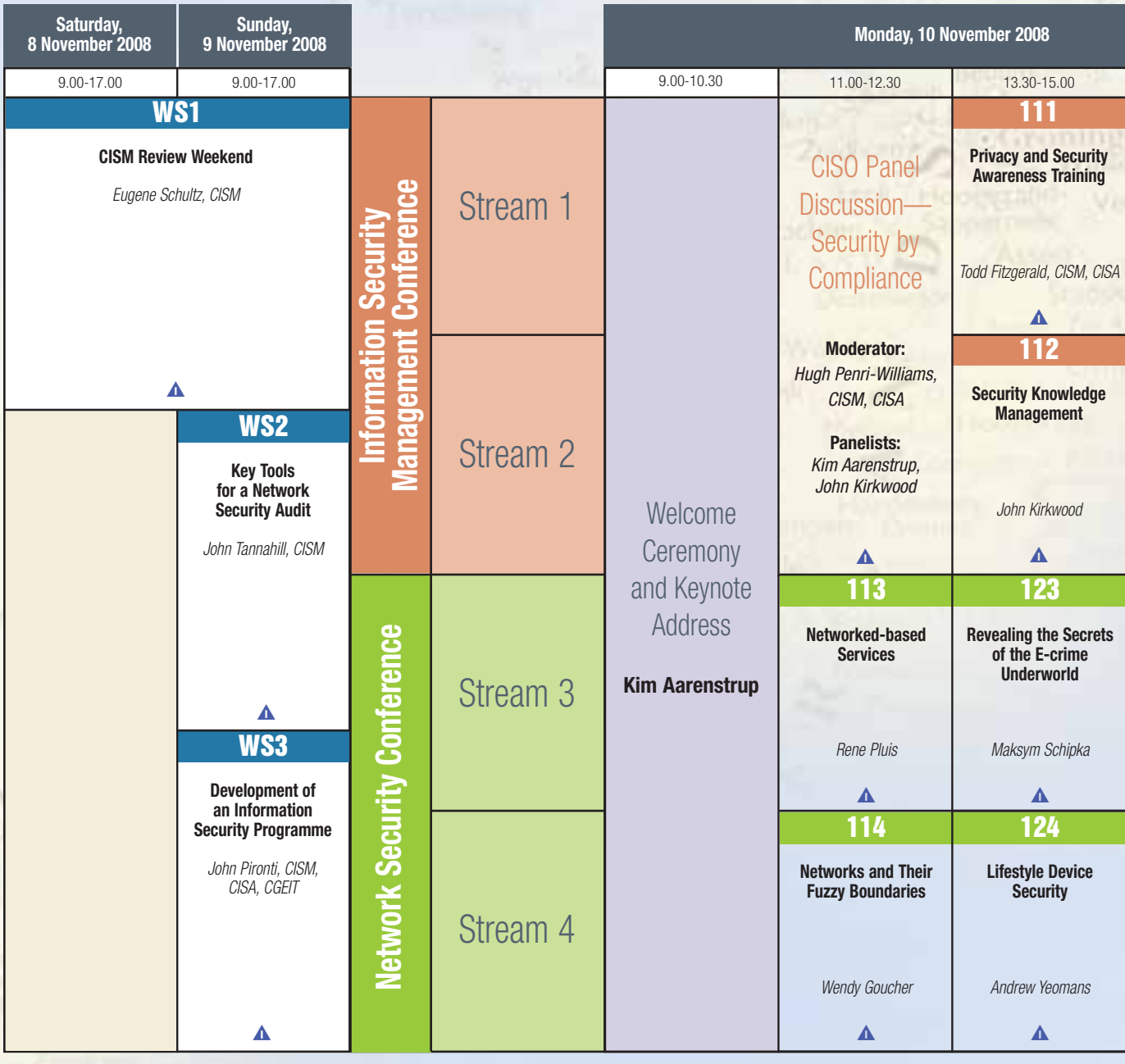
Participants will learn more about:
- Technologies associated with digital leak prevention—what they are and how they function
- Architectural and design considerations when designing and implementing a digital leak-prevention solution
- Key considerations when auditing a digital leak-prevention solution
- Realistic expectations of what digital leak-prevention solutions can assist you with and what they cannot
- Case studies of successful and not so successful implementations of digital leak-prevention technologies

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge, completed some basic training and be familiar with information technology terminology.

214
Establishing a Computer Forensics Practice

Participants will learn more about:
- The critical factors for deciding to establish an internal forensics practice
- Limitations of an internal forensics practice
- What resources are available
- Available standards
- What considerations to plan for during the process of establishing a practice

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.


Saturday, 8 November 2008
Sunday, 9 November 2008
Monday, 10 November 2008
9.00-17.00
9.00-17.00
9.00-10.30
11.00-12.30
13.30-15.00
WS1
CISM Review Weekend
Eugene Schultz, CISM
WS2
Key Tools for a Network Security Audit
John Tannahill, CISM
WS3
Development of an Information Security Programme
John Pironti, CISM, CISA, CGEIT
Information Security Management Conference
Network Security Conference
Stream 1
Stream 2
Stream 3
Stream 4
Welcome Ceremony and Keynote Address
Kim Aarenstrup
CISO Panel Discussion—Security by Compliance
Moderator:
Hugh Penri-Williams, CISM, CISA
Panelists:
Kim Aarenstrup, John Kirkwood
111
Privacy and Security Awareness Training
Todd Fitzgerald, CISM, CISA
112
Security Knowledge Management
John Kirkwood
113
Networked-based Services
Rene Pluis
123
Revealing the Secrets of the E-crime Underworld
Maksym Schipka
114
Networks and Their Fuzzy Boundaries
Wendy Goucher
124
Lifestyle Device Security
Andrew Yeomans

	Tuesday, 11 November 2008				Wednesday, 12 November 2008	
15.30-17.00	9.00-10.30	11.00-12.30	13.30-15.00	15.30-17.00	9.00-10.30	11.00-12.30
121	**211**	**221**	**231**	**241**	**311**	**321**
Threat and Vulnerability Analysis *John Pironti, CISM, CISA, CGEIT* I	**Skills Necessary to be an Effective Security Leader** *Todd Fitzgerald, CISM, CISA* I	**Designing and Implementing Vendor Security Compliance Programmes** *Peter Taylor* I	**Information Security Offshore: What to Expect and How to Cope** *Michael Bacon* I	**Metrics, Measures and Myths** *Ramsés Gallego, CISM* A	**Competitive Intelligence and IP Protection** *Meenu Gupta, CISM, CISA* I	**Web 2.0— How Secure Are Your Applications?** *John Burroughs* I
122	**212**	**222**	**232**	**242**	**312**	**322**
Using CobiT, ITIL and the ISO 27000 Series for Business Benefit *Yves LeRoux, CISM* A	**Transforming Information Security to Information Risk Management** *John Pironti, CISM, CISA, CGEIT* I	**The Value of Certification and Professional Development in the Security Profession** *Vernon Poole, CISM, CGEIT* I	**Convergence of Security and ERM** *A Panel Discussion* I	**Business Continuity Management** *Hugh Penri-Williams, CISM, CISA* I	**Continuous Controls Monitoring** *Vernon Poole, CISM, CGEIT* I	**IT Control Objectives for Basel II** *Robert White, CISA* I
133	**213**	**223**	**233**		**313**	**323**
Anatomy of Evolving Threats *Roel Schouwenberg* I	**Next Generation Network Security Tools** *Eugene Schultz, CISM (Honorary)* I	**PCI Compliance: A Realistic Apprroach** *Simon Langley* I	**Penetration Testing** *Peter Wood* I		**Developing, Designing and Auditing an Integrated Incident Response Programme** *Marc Vael, CISM, CISA* I	**Devise a Strategy to Mitigate Malware** *Yuval Ben-Itzhak* A
134	**214**	**224**	**234**	**244**	**314**	**324**
Data Loss Prevention: Concepts and Solutions *Ramsés Gallego, CISM* I	**Establishing a Computer Forensics Practice** I	**From Virtualisation vs. Security to Virtualisation-based Security** *Steve Orrin* I	**Addressing the Insider Threat to Database Security** *Steve Moyle* I	**The Evolution of Security Monitoring Powered by SIEM Systems** *Christos Dimitriadis* I	**Securing Wireless Technologies** *John Tannahill, CISM* I	**Encryption in the Enterprise** *Sathvik Krishnamurthy* I

B **Basic** I **Intermediate** A **Advanced**

Note: One person's intermediate level may be another person's advanced. Please review session descriptions and prerequisites to determine if the session is appropriate for you.

224
From Virtualisation vs. Security to Virtualisation-based Security ▲

Steve Orrin
Director of Security Solutions
Intel Corporation

Participants will learn more about:
- Platform virtualisation mechanisms
- Advances in virtualisation technologies that improve your security posture
- Strategies for effective compliance and enforcement in virtualised environments
- New ways to secure platforms using virtualisation including application isolation, sandboxing and policy-based execution environments

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

234
Addressing the Insider Threat to Database Security ▲

Steve Moyle
Founder and Chief Technology Officer
Secerno Ltd.

Participants will learn more about:
- Recognising and identifying insider threat risks that exist within an enterprise
- Strengthening existing IT infrastructure against insider threat risks
- Monitoring threats in real time
- Identifying the most common insider threat scenarios and database vulnerabilities
- Understanding database access controls and policies that will prevent unauthorised access
- Developing tamper-evident monitoring systems and audit trails

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

B Basic ▲ Intermediate A Advanced

Note: One person's intermediate level may be another person's advanced. Please review session descriptions and prerequisites to determine if the session is appropriate for you.

244
The Evolution of Security Monitoring Powered by SIEM Systems ▲

Christos Dimitriadis
Technical Manager
Expernet SA

Participants will learn more about:
- Integrating identity management, physical and logical convergence, Security Information and Event Management (SIEM), and application and database monitoring
- How government agencies and enterprises have taken advantage of the evolution of the SIEM market to protect their organisations
- What technologies should be implemented
- The pitfalls to avoid in implementing solutions

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

314
Securing Wireless Technologies ▲

John Tannahill, CISM
Partner
J. Tannahill & Associates

Participants will learn more about:
- Understanding current wireless technologies
- Wireless threats and risks
- Securing wireless technologies and wireless risk assessment
- Secure wireless architecture, design and deployment
- Wireless security assessment

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge and be familiar with information security terminology, approaches, methodologies and techniques.

324
Encryption in the Enterprise ▲

Sathvik Krishnamurthy
President and CEO
Voltage Security Inc.

Participants will learn more about:
- How to evaluate the use of specific encryption applications
- Which business drivers are most important for the increasing use of encryption
- Classifying how your organisation's overall IT security strategy and performance compares to its peers
- Positioning your own IT organisation amongst its peers' progress in adopting an enterprise encryption strategy

Prerequisites:
The participant should have at least three years of IT experience or equivalent knowledge and be familiar with terminology, approaches, methodologies and techniques to audit the IT environment.

Pre-conference Workshops

WS1

CISM Review Weekend ▲

8-9 November 2008

Gene Schultz, CISM (Honorary)
Chief Technology Officer
High Tower Software

This workshop is a review course designed to assist and enhance the study process of CISM candidates in preparation for the December 2008 CISM exam. The workshop will highlight key information security management practices, issues and concepts and will emphasize the topics likely to receive coverage on the CISM exam. Participants will receive handout material, including the *CISM® Review Manual 2008*, published by ISACA.

Prerequisites:
The participant should have three years of information security management experience or equivalent knowledge and be familiar with terminology, approaches, methodologies and techniques appropriate to an IT environment.

WS2

Key Tools for a Network Security Audit ▲

9 November 2008

John Tannahill, CISM
Partner
J. Tannahill & Associates

This popular workshop has been updated for 2008 with new network security tools and updates to existing tools. It will discuss the key tools and techniques that can be used to perform a comprehensive network security assessment and will feature demonstrations of and practical tips on using them. The workshop will use a live TCP/IP network with Windows 2000/2003 and UNIX operating systems to display network mapping and discovery, TCP/IP port scanning, network vulnerability assessment tools, and network packet capture and analysis tools. A structured approach to network security assessment will be discussed and applied to provide the framework for the practical use of tools and techniques.

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge, completed some basic training, and be familiar with IT terminology.

WS3

Development of an Information Security Programme ▲

9 November 2008

John Pironti, CISM, CISA, CGEIT
Chief Information Risk Strategist
Getronics

Information security has become a critical issue within organisations and a key success factor for businesses. To effectively maintain the integrity and security of an organisation's information infrastructure, an organised information security strategy must be developed and implemented. The concepts of an information security programme, threat and vulnerability management, and enterprise security monitoring are introduced in this workshop. This workshop highlights the key functional areas, processes, methodologies and organisational concepts that should be included to implement and maintain an effective information strategy. Key functional areas are discussed in depth and highlighted for their importance to the strategy activities that they will perform and their associated key performance indicators. Interactive discussions and case studies will be utilised to highlight operationally capable models and solutions.

Prerequisites:
The participant should have at least three years of information security experience or equivalent knowledge, completed some basic training, and be familiar with IT terminology.

General Information

Programme Benefits

Your registration fee includes:

- Attendance to the conference sessions of your choice from both the Network Security Conference and the Information Security Management Conference
- Complete set of electronic proceedings that includes all session handouts received by the production deadline
- Unlimited entry to the InfoExchange on Monday, 10 November 2008 and Tuesday, 11 November 2008
- Complimentary lunches on Monday, 10 November 2008 and Tuesday, 11 November 2008
- Complimentary morning and afternoon refreshment breaks throughout the two and a half days of the conference
- Invitation to the Exhibitors' Reception on Monday, 10 November 2008
- An opportunity to earn up to 32 continuing professional education (CPE) credit hours

Conference and Workshop Dates

Pre-conference Workshops

8-9 November 2008

Conference

10-12 November 2008

Registration Dates and Hours

Pre-conference Workshop Registration

Saturday, 8 November 2008, 7.30-12.00
Sunday, 9 November 2008, 7.30-12.00

Conference Registration

Sunday, 9 November 2008, 15.00-17.00
Monday, 10 November 2008, 7.00-17.00
Tuesday, 11 November 2008, 8.00-17.00
Wednesday, 12 November 2008, 8.00-12.00

Pricing (in US dollars):

Conference:

Member early-bird discount (payment received on or before 17 September 2008) $1,450
Member (payment received after 17 September 2008) $1,600
Non-member $1,800

Pre-conference Workshop:

One-day Workshop

Member $550
Non-member $750

Two-day Workshop

Member $750
Non-member $950

* VAT: The delegate fees indicated above qualify for VAT exemption; therefore, the registration fees do not include VAT. The full registration fee indicated must be received by ISACA to consider your registration paid in full.

Cancellation Policy

If a cancellation is received by phone, e-mail or fax by 10 October 2008, your conference registration fee will be refunded less a US $100 cancellation charge, workshop registration less a US $50 cancellation charge and (if applicable) less the amount of membership dues applied as a result of ticking the box marked: "I wish to apply the difference between member and non-member conference fees towards a membership in ISACA." After 10 October, no refunds can be given. Substitutions may be made at any time up until the conference. Substitution of a non-member for a member will result in additional non-member conference fees being charged.

Note: Registration is contingent upon full payment of the registration fee. To guarantee your registration, conference or workshop fees must be received no later than the published deadline. Wire transfers and mailed cheques may take 10 or more business days to reach ISACA, so please plan accordingly. If ISACA must cancel a course or event for any reason, liability is limited to the registration fees paid only. ISACA is not responsible for other expenses incurred, including travel and accommodation fees. Those who register onsite or whose registration remains unpaid as of the beginning of the event are not guaranteed conference materials. For more information regarding administrative policies, such as complaints and/or refunds, please contact the ISACA conference department:
Phone: +1.847.660.5585
Fax: +1.847.253.1443
E-mail: *conference@isaca.org*

Invitation to Join

Not yet a member? You can apply the difference between member and non-member conference fees towards membership in ISACA. This could potentially enable you to become a member at both the international and chapter level at no additional charge, and enjoy all the benefits of membership. Non-members pay the non-member conference rates when registering; the difference between the member and non-member rate is applied toward membership. Tick the box on the registration form to accept this invitation. This offer expires 30 days after completion of the event. For more information about ISACA membership, contact the membership department by e-mail at *membership@isaca.org* or visit the web site at *www.isaca.org/membership*.

Special Events

Exhibitors' Reception and Opening of the InfoExchange

Monday, 10 November 2008, 17.00-19.00

The Exhibitors' Reception marks the official opening of the InfoExchange. Join us for refreshments and stay to examine the latest products and services available to IS professionals. Exhibitors will be available to demonstrate products and answer questions.

InfoExchange Exhibits

Monday, 10 November 2008, 17.00-19.00
Tuesday, 11 November 2008, 10.30-11.00, 12.30-13.30, 15.00-15.30

A vendor exhibition featuring the latest products and services from leading suppliers will take place during the ISACA security conferences. The exhibition is designed to help IS professionals be more efficient and effective.

Dress

Business casual is appropriate for the conference and all conference events.

Venue and Accommodations

This year's conferences will be held at the NH Grand Hotel Krasnapolsky. The hotel is located in the heart of Amsterdam at Dam Square, opposite the Royal Palace. The hotel is surrounded by department stores, boutiques and museums, all in the historic city centre. NH Grand Hotel Krasnapolsky is known as the Grand Dame of the Amsterdam five-star hotels.

NH Grand Hotel Krasnapolsky
Dam 9
NL 1012 JS Amsterdam
The Netherlands
Telephone: +31.20.554.91.11
Fax: +31.20.622.86.07
Web site: *www.nh-hotels.com*
Guest room rate: €239 (exclusive of breakfast)
Room block cut-off date: 22 October 2008

Please contact the hotel directly to make your reservations. Staying at the host hotel helps keep the cost of the conference and membership dues down by helping to fulfil the negotiated guest room commitments to the hotel. You will also enjoy the benefits of being onsite for conference activities at a discounted price.

Continuing Professional Education Credits

To maintain Certified Information Security Manager® (CISM®), Certified Information Systems Auditor™ (CISA®) and Certified in the Governance of Enterprise IT™ (CGEIT™) certifications, ISACA's continuing professional education (CPE) policy requires CISMs, CISAs and CGEITs to earn 120 CPE credit hours over a three-year period. Attendees can earn up to 32 CPE credits by attending the ISACA security conferences (18 CPE hours) and an additional seven CPE credits for attending each day of an optional pre-conference workshops. For more information or to register for the conference online, please visit *www.isaca.org/nsc* or *www.isaca.org/infosecurity*.

About This Brochure

The speakers, topics and events are correct at the time of printing. If unforeseen circumstances occur, ISACA reserves the right to alter or delete items from the ISACA security conferences' programme. The presenters have prepared their material for the professional development of ISACA members and others in the IS audit, control, security and governance community. Although they trust that it will be useful for this purpose, neither the presenters nor ISACA can warrant that the use of this material will be adequate to discharge the legal or professional liability of the members in the conduct of their practices.

INFORMATION SECURITY CONFERENCE

2009 and Beyond…

You told us what you wanted and we listened. Join us in 2009 when the Information Security Management Conference and the Network Security Conference combine to become the ISACA Information Security Conference.

ISACA will host one conference that will build on and include the key elements of information security management practices and network security practices. The conference will cover related business, programme and technical issues and the impact of risk management. This expanded event will feature five separate streams, allowing attendees to go to sessions from any of the streams and earn CPE credits.

Plan to join us in 2009 at the ISACA Information Security Conference!

Registration Form

ISM08 NS2008

1. Fill in the information below in block letters.

Name (Mr., Mrs., Ms., Miss) _____
(First/Given Name) (Middle Name) (Last/Family Name)

Title _____ Company Phone _____

Company _____ Company Fax _____

Badge Name (first name or nickname) _____ E-mail Address _____

☐ Company or ☐ Home Address (please indicate) ☐ This is a change of address.

Address _____

City _____ State/Province _____ Zip/Postal Code _____ Country _____

☐ Please do NOT include my full address on the roster given to delegates, speakers and exhibitors.

ISACA member? ☐ Yes. Member Number _____ ☐ No

2. Please select your conference and circle your session choices.

(No more than one session per time period, please.) You may attend sessions at either conference, but you must select one conference for registration.

☐ **Information Security Management Conference** ☐ **Network Security Conference**

Saturday, 8 November 2008	Sunday, 9 November 2008		Monday, 10 November 2008				Tuesday, 11 November 2008				Wednesday, 12 November 2008	
9.00-17.00	9.00-17.00		9.00-10.30	11.00-12.30	13.30-15.00	15.30-17.00	9.00-10.30	11.00-12.30	13.30-15.00	15.30-17.00	9.00-10.30	11.00-12.30
WS1		Stream 1	Welcome Ceremony and Keynote Address	CISO Panel Discussion—Security by Compliance	111	121	211	221	231	241	311	321
	WS2	Stream 2			112	122	212	222	232	242	312	322
		Stream 3		113	123	133	213	223	233		313	323
	WS3	Stream 4		114	124	134	214	224	234	244	314	324

SAVE NOW!

Not yet a member? You can apply the difference between member and non-member course fees towards membership in ISACA. This could potentially enable you to become a member at both the international and chapter level at no additional charge and enjoy all the benefits of membership. Simply tick this box to accept the offer.

☐ **I wish to apply the difference between member and non-member course fees towards membership in ISACA. I have read and agree to the following membership disclaimer:**

By applying for membership in ISACA, members agree to hold the association and the IT Governance Institute, their officers, directors, agents, trustees, members and employees harmless for all acts or failures to act while carrying out the purposes of the association and institute as set forth in their respective bylaws, and certify that they will abide by the association's Code of Professional Ethics (*www.isaca.org/ethics*).

Attendee name_____

3. Registration Fees (Please circle your choice.)

Conference Registration* (all fees are quoted in US dollars)
Member early-bird discount (payment received on or before 17 September 2008)..$1,450
Member (payment received after 17 September 2008) $1,600
Non-member. $1,800

Pre-conference Workshops
One-day Workshop
Member $550
Non-member $750
Two-day Workshop
Member $750
Non-member $950

*** VAT: The delegate fees indicated above qualify for VAT exemption; therefore the registration fees do not include VAT. The full registration fee indicated must be received by ISACA to consider your registration paid in full.**

TOTAL (Add all circled above plus any additional item fees.) US $_____

4. Indicate Method of Payment

☐ Payment enclosed. Make cheque **payable in US dollars, drawn on a US bank**, to ISACA.

☐ Wire Transfer in US $_____ Date Transferred _____
Wire transfers and mailed cheques may take 10 or more business days to reach ISACA, so please plan accordingly.

Charge my ☐ Visa ☐ MasterCard ☐ American Express ☐ Diners Club
(NOTE: All payments by credit card will be processed in US dollars.)

Number Expiration Date

Name of Cardholder

Signature of Cardholder

Complete Billing Address of Cardholder (if different from above)

5. Registration Methods

A. **REGISTER ONLINE** at *www.isaca.org/nsc or www.isaca.org/infosecurity.*

B. **FAX** your completed registration form to +1.847.253.1443.

C. **MAIL** your completed registration form to:
ISACA
1055 Paysphere Circle
Chicago, IL 60674 USA

D. **BANK WIRES:** Send electronic payments in US dollars to:
Bank of America, ABA #071000505,
ISACA Account #22-71578, S.W.I.F.T. code LASLUS44

[Please include **attendee's name** and **Network Security Conference—Amsterdam** or **Information Security Management Conference—Amsterdam** on the Advice of Transfer.]

6. Cancellation Policy

If a cancellation is received by phone, e-mail or fax by 10 October 2008, your conference registration fee will be refunded less a US $100 cancellation charge, workshop registration less a US $50 cancellation charge and (if applicable) less the amount of membership dues applied as a result of ticking the box marked: "I wish to apply the difference between member and non-member conference fees towards a membership in ISACA." After 10 October, no refunds can be given. Substitutions may be made at any time up until the conference. Substitution of a non-member for a member will result in additional non-member conference fees being charged.

Note: Registration is contingent upon full payment of the registration fee. To guarantee your registration, conference or workshop fees must be received no later than the published deadline. Wire transfers and mailed cheques may take 10 or more business days to reach ISACA, so please plan accordingly. If ISACA must cancel a course or event for any reason, liability is limited to the registration fees paid only. ISACA is not responsible for other expenses incurred, including travel and accommodation fees. Those who register onsite or whose registration remains unpaid as of the beginning of the event are not guaranteed conference materials. For more information regarding administrative policies, such as complaints and/or refunds, please contact the ISACA conference department:
Phone: +1.847.660.5585
Fax: +1.847.253.1443
E-mail: *conference@isaca.org*

7. Special Arrangements

☐ Special Dietary Requirements_____

☐ I will require assistance. Please contact me to make the necessary arrangements.

Responsibility for obtaining VISAs is entirely that of the registrant. Please contact the local government of the hosting country for details. Once a paid registration is received, a letter of invitation will be provided by ISACA, upon request.

ISACA®
Serving IT Governance Professionals

3701 Algonquin Road, Suite 1010
Rolling Meadows, IL 60008-3105, USA

Please share this brochure with

_____ Security director/manager
_____ Security staff
_____ Audit director/manager
_____ IS/IT director
_____ CISO/CSO/security executive
_____ CIO/CTO

Programme Committee

John Pironti, CISM, CISA, CGEIT
Chair
Chief Information Risk Strategist
Getronics

Meenu Gupta, CISM, CISA
President
Mittal Technology

Yves LeRoux, CISM
Technology Strategist
CA Inc.

Vernon Poole, CISM, CGEIT
Head of Business Consultancy
Sapphire Technologies Ltd.

Dr. Eugene Schultz, CISM
(Honorary)
Chief Technology Officer
High Tower Software

R. Kinney Williams, CISM
President
Yennik Inc.

Peter Wood
Chief of Operations
First Base Technologies

Staff Liaison: Madeline Parisi
Manager of Education
Development
ISACA