

Gartner IT Security Summit 2007

17-19 SEPTEMBER 2007, ROYAL LANCASTER HOTEL, LONDON
europe.gartner.com/security



AGILE SECURITY. PROACTIVE RISK MANAGEMENT.

SUMMIT CO-CHAIRS

KEYNOTE SPEAKERS



Ant Allan
Research VP, UK



Jay Heiser
Research VP, UK



John Pescatore
VP & Distinguished
Analyst, US



Joanna Rutkowska
CEO/Founder, Invisible Things Lab,
and acclaimed security researcher

Gartner

IT Security
Summit 2007

17-19 September 2007
Royal Lancaster Hotel, London

Register before 20 July 2007 and save €300
off the standard delegate rate

Agile Security. Proactive Risk Management.

INTRODUCTION FROM THE SUMMIT CO-CHAIRS



Traditional IT security over-protects the wrong assets, over-reacts to the unexpected and over-spends on almost everything.

Welcome to Security 3.0, a clear-eyed approach to risk management that applies security resources appropriately while maximizing business agility. Instead of bolting security on as an afterthought, Security 3.0 integrates compliance, risk assessment and business continuity dynamics into every process and application.

It's the only way to contain security spending while managing the risks of doing business in a connected world. And it's the main thrust of the Gartner IT Security Summit 2007.



Due to demand for even more content on best practice, we've added a third day packed with implementation strategies, methodologies and other best practices content. We've also created four tracks to cover the security landscape, including emerging threats, the demands of compliance, planning for the unexpected and the new security infrastructures & processes to rise to these challenges.

We are pleased to present among our many guest speakers a guru keynote from distinguished security researcher Joanna Rutkowska, popularly known for her research on stealth malware, virtualization technology and defeating Vista security mechanisms. She will discuss the attacker's goals after getting into the system, defense approaches and the conundrum of preventing or detecting attacks such as targeted stealth malware.

With over 70 sessions and the active participation of 19 senior Gartner analysts, this is going to be a great Summit.

We hope you can join us!

A handwritten signature in black ink that reads "Ant Allan".

Ant Allan
Research VP, Gartner

A handwritten signature in black ink that reads "Jay Heiser".

Jay Heiser
Research VP, Gartner



BENEFITS OF ATTENDING

- **Understand emerging threats** and your best defenses
- **Sharpen your security strategy** and tighten your tactics
- **Sharpen the way you communicate** security to the business
- **Integrate security** in all processes and applications
- **Drive down the cost of compliance** while harvesting the benefits
- **Better manage** all kinds of risk
- **Learn from your peers** in a series of in-depth practical case studies
- **Get the latest Gartner research** on key security issues
- **Share your experiences** with your peers from across Europe
- **Hear the visionary keynotes** from the industry's top thinkers
- **Attack your toughest challenges** in Analyst One-on-One meetings
- **Take away the complete event CD** for sharing the knowledge back at the office

WHO SHOULD ATTEND

CIOs, CTOs, CISOs, IT security officers, Enterprise Security Architects, Network Managers, Risk Managers, Internet Security Managers, Business Continuity Managers, Security Analysts and Consultants, and all other professionals with an interest in security decisions.

KEY TOPICS

- Creating and managing the right security program for a changing threat landscape
- The IT Security Competency Center: roles, structures and organization
- Information security architectures: the right content and structure
- Risk management for information security practitioners
- The process-oriented activity cycle for security and risk management
- Effective processes and technologies for
 - a) identity and access management,
 - b) vulnerability and threat management,
 - c) risk and control assessment and
 - d) communications and relationship management
- Regulatory compliance and corporate governance
- Achieving maturity in business continuity management and disaster recovery
- The art of meaningful security metrics
- Trends in emerging cyberthreats and information security technologies
- Latest analyses of information security markets and vendors

Four Tracks to Proactive Security!

The Gartner IT Security Summit, for the first time with an expanded 3-day agenda, focuses on architectures, methodologies, best practices and the latest technologies designed for proactive strategies that can be used for reducing your IT security risks and meeting your security challenges.

1

Infrastructure Protection

The technology infrastructure is fundamental to Security 3.0 and it must be fundamentally secure. Enterprises must prevent and limit damage to their business operations by deploying policies, processes and technologies to detect and block attacks — both internal and external — and minimize the vulnerabilities that enable attacks. The enterprise threat environment is changing rapidly, as are the approaches, applications and technologies enterprises use to engage customers and partners — and your strategies must change with them. This track focuses on the processes, technologies and services needed to protect data, applications, systems and the network, as well as on ways to discover and solve security weaknesses.

2

Secure Business Enablement

Once you build it, it must be secure. Security 3.0 is about knowing how to trust users, consumers, contractors, and partners. Past approaches no longer fully address organizational demand for a well-managed and automated identity and access management function. Legacy access control technologies, fragmented user administration processes and directories, spoofable e-mail, and single-platform security administration products are all typical examples of business 'disabling' approaches that are no longer sufficient. New techniques and tools are needed to manage the identities and entitlements of end users inside and outside the organization, and provide assurance against fraud, deception, and identity theft. This track focuses on processes and technologies that integrate security into electronic business processes and transactions.

3

Risk Management and Compliance

Compliance and risk management are not about technology. However, the fact is this: IT systems support the way an organization lives and breathes. So how can you help business units within your organization understand and manage IT-related risks and achieve compliance confidently? By systematically addressing IT risks across the enterprise and improving critical business and security management processes. Such a proactive approach enables top-line growth while still maintaining necessary levels of control in the complex areas of governance, regulations, risks, performance, sourcing, security, access control and vendor selection. This track focuses on the tools, strategies and tactics characteristic of a coordinated program for addressing regulatory, commercial and organizational risk effectively.

4

Information Security Tomorrow

Information security must continually evolve, reflecting and responding to ongoing changes in technology, business activities, and shifting patterns of technology misuse. This track takes a strategic view of emerging cyberthreats and emerging trust technologies, architectures, and programs. It is intended for IT risk managers who want to better understand how their career and discipline will evolve over the next 10 years.

An Expanded Agenda

Due to strong demand, we have expanded the agenda from two to **three days**. Get ready for more **hands-on, implementation material** from Gartner analysts and real-life case studies.

We're also increasing our focus on **security strategy** and **long-term trends** and boosted the number of sessions on **risk management, compliance and governance**.

Day 3: BEST PRACTICES AND IMPLEMENTATION DAY

- Focus on best practices, implementation strategies and methodologies
- Benefit from additional networking opportunities
- Take away day 3 presentations for your reference, including the Magic Quadrant Power Session

Meet the Gartner Community

For over 25 years, Gartner analysts have been the trusted advisors to many of the world's largest and most demanding organizations. No one sees the implications of technology so clearly, so consistently.

Gartner analysts draw constantly from the real-life challenges and solutions experienced by more than 45,000 clients worldwide. The value of this resource, combined with our deep analysis of technology vendors, is unrivaled.

The Gartner IT Security Summit brings a level of experience and expertise that you simply cannot get anywhere else.

Worldwide Expertise at Your Fingertips – Your Questions on IT Security Issues Answered!



Ant Allan
Research VP, UK

"You need something better than passwords in all but low-risk scenarios. But be clear why, when and how before you decide what and whose."

Focus Areas: User authentication; other IAM (password management, ESSO, user provisioning, etc.)



Monica Basso
Research VP, Italy

"For most organizations, the added risk of a NOC-based wireless email architecture is minor when the content has been encrypted at each end and is transferred over an encrypted transport."

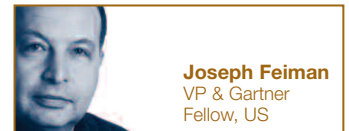
Focus Areas: Enterprise mobility, secure mobile e-mail, location-based services, mobile applications



Christian Byrnes
Managing VP, US

"The time nears when over 50% of IT security organizations will meet maturity level three standards. Our world will be populated by leaders and laggards."

Focus Areas: Security program governance, structure and management



Joseph Feiman
VP & Gartner Fellow, US

"Network Security technologies protect enterprises' perimeter against external attacks. This is important but insufficient. A new discipline – Application Security – should enable building security into applications."

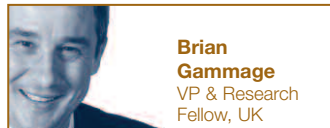
Focus Areas: Application Security; technologies and methodologies that enable developing secure applications



Peter Firstbrook
Research Director, Canada

"Organizations are under a continuous barrage of malware from the web and email. Multiple products and procedures across multiple IT disciplines are necessary to effectively defend the enterprise."

Focus Areas: Antivirus, Antispyware, Antispam, Email security



Brian Gammage
VP & Research Fellow, UK

"Being wise after the event is not good enough for the security of client computing. We need devices and software with security 'baked in', not added as an after-thought."

Focus areas: Client computing, consumerization of IT, virtualization technology, client application delivery models



John Girard
VP & Distinguished Analyst, US

"It's not a lack of security solutions causing companies to land in the headlines. It's the complexity of managing so many company and personal devices."

Focus Areas: Wireless, Mobile and Remote User Security & Privacy



Arabella Hallawell
Research VP, US

"Most companies today operate at extremes when it comes to security and global sourcing. But under- or overestimating the role and costs of security is bad for business."

Focus areas: Privacy, international issues, email security and anti-spam, acceptable use policies, web filtering



Jay Heiser
Research VP, UK

"The new IT risk challenge is in controlling the use of your information, even when it is being used on someone else's computer."

Focus areas: Trust Communities, Risk Management, Compliance, Forensics & investigation



Richard Hunter
GVP & Research Fellow, Gartner Executive Programs, US

"IT risk is business risk with business consequences. Period."

Focus Areas: CIO, risk governance, risk management, BCM



Gregg Kreizman
Research Director, US

"Personal identity frameworks (PIFs) are evolutionary extensions to today's identity and access management architectures. Microsoft and OpenID are starting the battle for mindshare."

Focus Areas: Password Management, Enterprise Single Sign-On, e-signature, PIFs



Mark Nicolett
VP & Distinguished Analyst, US

"With the rise in targeted attacks, IT organizations need to get better at finding and fixing security weaknesses before they are exploited, and need to more quickly discover patterns of inappropriate resource access."

Focus Areas: Security Information and Event Management; Vulnerability Management, IT GRC Management



Eric Ouellet
Research VP, Canada

"Security is the environmental suit protecting organizations from hazardous elements. When used properly, businesses can operate and thrive in hostile environments that would otherwise be off-limit."

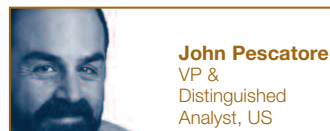
Focus Areas: Risk Management, Security Program Measurement, Secure E-Mail, Data Encryption, Rights Management, Certification



Earl Perkins
Research VP, US

"Organizations are beginning to understand the role and value of identity in their enterprise, but know they have to secure and leverage it if they want to be effective or competitive."

Focus Areas: Identity Management (e.g. user provisioning), Privacy, SOA Security



John Pescatore
VP & Distinguished Analyst, US

"Both threats and business models keep changing. Successful businesses will have security programs that move rapidly to neutralize new threats and to support new business initiatives."

Focus Areas: Internet Security, Intrusion Prevention, Wireless Security, Network Access Control, Metrics



Steve Prentice
Distinguished Analyst, Chief of Research, Security and Risk Management

"The consumerization of technology is already having a significant impact on people, processes and technology in the enterprise, and the greatest changes are yet to come."

Focus Areas: Strategic direction of technology; The impact of consumerization



Tom Scholtz
Research VP, UK

"Many security teams have unrealistic expectations about standardizing on a single risk assessment tool. This is impractical for most organizations because of the variety of scenarios which the tool has to support."

Focus Areas: Security strategy/architecture; Security organization; Investment justification; Secure outsourcing; BCP/DRP



Les Stevens
Research Director, South Africa

"Despite receiving high attention from senior executives and internal and external auditors, infosec departments still seem to struggle to establish relevant and enforceable policies."

Focus Areas: Policies, risk management and assessment, security strategy, security organization; BCP/DRP



Jeffrey Wheatman
Research Director, US

"The key to a successful program is business alignment; many organizations focus on answers before they identify the questions that need to be asked."

Focus Areas: Security organization, metrics, program maturity measurement, risk assessment

Speakers

"A window into the thought leadership currently in place in the information security industry."

Andrew Rose, Global Technology Risk Manager, Clifford Chance

KEYNOTE SPEAKERS

Joanna Rutkowska
CEO/Founder, Invisible Things Lab, and acclaimed security researcher



Joanna Rutkowska is a recognized researcher in the field of stealth malware and system compromises. Over the past several years she has introduced several breakthrough concepts and techniques on both the offensive and defensive side in this field. Her work has

been quoted by the international press and she is a frequent speaker at security conferences around the world. In April 2007 she founded Invisible Things Lab, a consulting company dedicated to cutting-edge research into operating systems security.

John Pescatore
VP, Gartner Fellow



John Pescatore is a Vice President and Gartner Fellow in Gartner Research with 24 years experience in computer, network and information security.

Mr Pescatore is Gartner's lead analyst on all Internet-facing security issues, covering a broad range of enterprise-critical areas. He also provides thought leadership in wireless security, ways to develop software without vulnerabilities, and trustable computing platforms.

He is frequently quoted in such publications as BusinessWeek Online, InformationWeek, ZDNet, Computerworld, VNUnet Newswire, Business Wire, and InfoWorld Daily News.

Exclusive BOOK LAUNCH ONSITE!

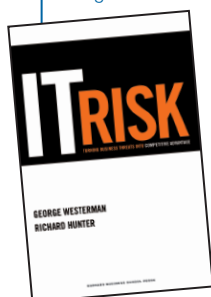
IT RISK

Turning Business Threats into Competitive Advantage

George Westerman and Richard Hunter

IT risk matters more than ever. In this timely and authoritative book, the authors define four types of IT risk: *availability, access, accuracy, and agility.* Citing numerous company examples, they introduce disciplines enterprises must master to manage IT risk effectively:

This book, co authored by Gartner Fellow Richard Hunter, offers powerful diagnostic tools to measure your company's strengths in each core discipline-and help you continuously improve competency and competitive advantage.



GARTNER ANALYST/USER ROUNDTABLES

These 45 minute discussions are moderated by a Gartner analyst and limited to 8 end-users per session, this is an additional opportunity to tackle key issues with experts and peers alike.

- 1 Organizing the IT Security Competence Center**
Jay Heiser
- 2 Surviving Identity & Access Management Deployments**
Earl Perkins
- 3 Security Architecture: Challenges and Best Practices**
Tom Scholtz
- 4 The CISO's View of Risk Management (*invitation only*)**
Eric Ouellet
- 5 Mobile Device Management Challenges**
John Girard
- 6 Towards More Secure Client Computing**
Brian Gammage
- 7 Best Practices for IT Governance, Control and Compliance**
Christian Byrnes
- 8 The Metrics of Our Success**
Jeff Wheatman
- 9 Security Trends**
Steve Prentice
- 10 Handling Privacy and Data Retention (*for privacy and data protection officers*)**
Arabella Hallawell
- 11 How To Manage (Without) Passwords**
Ant Allan

END-USER CASE STUDIES AND PANELISTS

Adrian Seccombe
CISO & Senior Enterprise Architect
Eli Lilly & Company

Iain Sutherland
Managing Director
Information Security Solutions

Des Ward
Director, Security Awareness
Information Systems Security Association (ISSA)

Andreas Wuchner
CISO
Novartis Pharma

Robert Carolina
Principal
Origin Solicitors

Rolf Winz
Group Information Security Officer
Schindler Informatik

Randi Røisli
CISO
Statoil

Toni Bekker
Head of Corporate IT Risk,
TeliaSonera

David Lodge
Global Head IT Risk Control
UBS

Neil Dudleston
Group Information Security Officer
United Utilities

"Three ways to update your security strategies information:

- 1) Google, but good luck.*
- 2) Read the latest books and white papers.*
- 3) Some strategic seminars like Gartner."*

Gohari Pejman, CISO and IT RM, Société Générale

Conference Program

Experience a unique mix of Gartner analyst presentations, guest keynotes, real-life case studies, interactive panels and selected solution provider sessions adding up to a cutting edge program agenda.

At a glance schedule

DAY 1

08.00 – 08.45	Pre-Summit Tutorials*
09.00 – 09.15	Conference Opening
09.15 – 12.00	Plenary Sessions
12.00 – 13.15	Lunch & Solution Showcase
13.15 – 18.00	Track Breakout Sessions
18.00 – 20.00	Networking Drinks Reception

DAY 2

07.30 – 08.30	Analyst Networking Breakfast
08.30 – 12.00	Track Breakout Sessions
12.00 – 13.10	Lunch & Solution Showcase
13.10 – 16.15	Track Breakout Sessions
16.40 – 17.25	CISO Panel
17.25 – 18.00	Executive Keynote Session
18.00 – 20.00	Networking Drinks Reception

DAY 3

08.30 – 12.15	Track Breakout Sessions
12.15 – 13.15	Lunch & Roundtables for Country and Industry Peer Groups
13.15 – 14.10	Track Breakout Sessions
14.25 – 15.20	Market Players: Magic Quadrant Power Session
15.20 – 16.00	Keynote Session
16.00	Conference Close

*See p7 for full details.

One-on-One Analyst Meeting Program: Discuss your issues with our experts

Gartner analysts participating in the IT Security Summit will be available to registered delegates for 30 minute One-on-One appointments to ask questions about the presentations, or address specific issues within the analysts area of expertise (pre-event booking via the conference website).

PRE-SUMMIT TUTORIALS

Tutorial A: Corporate Encryption – A Guide to Sleeping Comfortably at Night

Organizations are being challenged more than ever to protect sensitive data from both targeted attacks and accidental disclosure. Encryption can be the right answer, if applied correctly and judiciously.

- What are the best practices when developing a corporate encryption strategy?
- What can be done to minimize the impact of encryption deployments on applications and budgets?
- What are the leading deployment technologies and vendors providing encryption?

Eric Ouellet, Gartner

Tutorial B: Identity and Access Management

Deploying a successful identity and access management (IAM) solution demands an understanding of not only the strengths and weaknesses of individual tools but also their interrelationships and how they contribute to the greater whole. It also requires awareness of the IAM program context.

- IAM architecture, processes, and controls
- The Gartner taxonomy for identity and access management tools
- The roles, strengths and weaknesses of, opportunities for and threats to these tools.

Ant Allan, Gartner

Tutorial C: Selecting Information Security Risk Assessment Methods and Tools: A Use-Case Approach

Leading organizations understand that effective risk assessment depends on the ability to manage a toolbox of assessment techniques, and to apply the most appropriate technique on a case by case basis.

- How should enterprises characterize the use cases for information security risk assessment?
- How should enterprises select appropriate risk assessment methods and tools?
- How can enterprises formalize risk assessment experience and learning?

Tom Scholtz, Gartner



“Gartner knows how to run conferences! The IT Security Summit gave me a good insight into the IT security domain and was fun.”

Joseph Lee, Enterprise Information Architect,
National Australia Group Europe

PLENARY SESSIONS

Gartner Keynote: Security 3.0: Skating Ahead of the Puck

Security has traditionally been reactive, lagging new business trends and new technologies. Security 3.0 demands fundamentally changing our approach, focusing on processes, controls and architectures that support agile and responsive security. Security 3.0 is a tectonic shift in security program evolution to meet boardroom concerns of protecting customer data, minimizing risks to the business bottom line, and reducing the cost of demonstrating compliance to an increasing number of regulations.

John Pescatore, VP Distinguished Analyst, Gartner

Guru Keynote: Human Factor vs. Technology

This lecture will present current challenges in operating systems security – from both a human as well as a technical perspective – and views on possible ways of addressing those issues. The main message will be that the so-called “human factor” is not, in contrast to common belief, the weakest link in IT security, as eliminating the incompetence of users and administrators does not solve many of the serious problems we’re facing today.

Joanna Rutkowska, CEO/Founder, Invisible Things Lab, and acclaimed security researcher

Premier Panel

Meet top-executives from leading technology providers in the IT security arena, including Cisco and Internet Security Systems, an IBM Company, moderated by a Gartner analyst.

CISO Panel: Creating a Secure Organization

Security officers have been forced to change with the evolving needs of their organizations.

- What are the different models of security organization?
- How do you reach agreement on what is “good enough” security?
- How can information security be a business enabler?
- What are the likely challenges and opportunities for CISOs in the future?

A panel of four Chief Information Security Officers of leading end-user organizations, moderated by a Gartner analyst.

Market Players: Magic Quadrant Power Session

Meet the Gartner analysts at their best: ad hoc on stage. Ask questions about vendors or tools. Hear the Gartner position on the technology providers in Security Information and Event Management, User Provisioning, Content Monitoring and Filtering and Data Loss Protection, Personal Firewalls and Mobile Data Protection – unscripted, unfiltered, unbiased.

- Who is hot and who is not?
- Which vendors will survive the consolidation?
- Which providers understand where the market is going?

John Girard, VP Distinguished Analyst
Mark Nicolett, VP Distinguished Analyst
Eric Ouellet, VP Research
Earl Perkins, VP Research, Gartner

Gartner Debate:

To Perimeter or not to Perimeter, the Firewall Is the Question

Today’s security is firmly based on the perimeter principle, with a hardened control boundary between the enterprise and the outside. A growing school of thought rejects this idea, arguing that boundaries are already porous, perimeters are becoming irrelevant, and security must be baked into IT components. Join a group of top Gartner analysts as they face off – two against two – to decide whether deperimeterization is just a buzzword, or the only way forward.

Joseph Feiman and Brian Gammage vs.
John Pescatore and John Girard

TRACK 1: INFRASTRUCTURE PROTECTION

Vulnerability Management, Security Information and Event Management

Vulnerability management requires multiple technologies and vendor products as well as processes to fill technology gaps. SIEM technology can speed reaction times to solving external and internal threats and be helpful in regulatory compliance.

- What new technologies should organizations employ to manage vulnerabilities and improve regulatory compliance?
- What are the essential components of an effective vulnerability management program?
- What are the functional characteristics of an effective SIEM product?

Mark Nicolett

Integrating Security into the Application Lifecycle

Application developers often focus on functionality, not security. Applications get built with exploitable security vulnerabilities, and losses continue. This session addresses the application lifecycle: from requirements analysis through development and operations, and review how it can be made more secure.

- Who should be responsible for application security?
- What are security lifecycle methodologies?
- How to apply security along the entire application lifecycle?
- What vendors provide security solutions for application development?

Joe Feiman

Endpoint Security: Moving Beyond Signature Antivirus

Today’s attackers have your data in their crosshairs. Although the malware threat continuously evolves, the \$4billion+ anti-virus industry is offering the same old product. Security planners need a broader range of end-node security solutions. This presentation addresses three major key issues:

- What are the trends in malware?
- What is the process for proactively securing end-nodes?
- How can end-node security be automated?

Peter Firstbrook

Security Testing Trends, Tools, and Practices

Vulnerability testing must be part of the application lifecycle, but can testing technology be relied upon? Should you buy a testing tool or subscribe to a testing service? This presentation addresses technology and service selection, planning, and operations.

- How mature are application security testing technologies?
- How do you combine security code testing and security application runtime testing?
- Will the security testing market remain a standalone market?

Joe Feiman

Securing the Internet Gateways

The Internet is both a productivity enabler and a fire-hose of malware and spam. Prudent organizations recognize the increasing legal and regulatory risks as

well as the potential for data loss. This presentation presents effective solutions for filtering email and web traffic:

- What are the threat trends from Internet and email traffic?
- Is unified threat management practical and does convergence make sense?
- How are solutions adapting?

Peter Firstbrook

Mobile Device Management and Device Security Convergence

Mobile device utilization is rapidly climbing within enterprises. The vendors who can support device lock-down, session encryption and other key functions present an overlapping and confusing set of choices.

- What are the drivers for security and management of mobile devices?
- How will the security configuration and mobile management markets for laptops and small devices evolve?
- What are best practices for implementing a secure mobile system management strategy?

John Girard and Monica Basso

Implementing Controls for IT Security Processes and Technologies

Proof of integrity of the IT infrastructure is stronger and less costly when security best practices are implemented and mapped to control frameworks that are the basis for many audits. Enterprises are evaluating emerging automation for IT security controls through vulnerability management, security configuration policy compliance, security policy management and security information management. The goal is to map these security operations capabilities to a compliance program.

Mark Nicolett

Getting to Next Generation Network Security

As new network threats emerge, defenses and safeguards will to more proactive approaches. New security function “mash-ups” improve security postures without creating resource burdens. This presentation surveys network security Magic Quadrants, describes the solutions, and looks forward to implementing the Security 3.0 philosophy.

- How are network security threats evolving?
- How should enterprises get ahead of them?
- What new security products are emerging, and how will existing ones change?

John Pescatore

How to Secure Wireless Email and Other Vulnerable Applications

Mobile email and applications are now a priority for user organizations, but security represents a major limitation for wide deployments. We discuss real and perceived security threats, and identify solutions to manage them.

- Which are the main wireless email security threats?
- What is the best strategy to secure your wireless email deployments?
- Which products and vendors will help to implement wireless email security?

Monica Basso

“Advance with Gartner from IT security to risk management.”

Guy Bejerano, CISO, Ness

Conference Program



TRACK 2: SECURE BUSINESS ENABLEMENT

The Role of Directories in Authentication and Authorization

The dream of a single, central authentication and authorization repository for all platforms and applications will never be realized. How, then, do organizations cope with the diverse needs of authentication and authorization?

- Why is a central authentication repository not achievable?
- How do authentication and authorization repositories differ?
- What solutions can be used to lessen the pain points of multiple authentication stores?

Earl Perkins

The Future of Secure Messaging

Spam volumes are escalating and existing solutions are struggling to keep up, particularly with the growth in image spam. Requirements for monitoring of outbound email are increasing. Sender reputation is becoming an important issue. IM, consumer web mail and web 2.0 are redefining the scope of messaging, and what it takes to secure it.

- How are threats and business requirements changing messaging security?
- How is the market evolving?
- What are best practices?

Arabella Hallawell

Authentication Marketplace: I Want That One

The authentication marketplace is rapidly evolving, with "new! best!" products appearing almost monthly. Confronted with a bewildering choice of methods, organizations may struggle to identify what meets their needs for robust, convenient and affordable authentication.

- Is there a useful classification of authentication methods?
- Which methods are organizations using now, and what will they be using in 2010?
- How can organizations best identify suitable methods?

Ant Allan

Your Information, Someone Else's Device

The move by some organizations toward employee-owned mobile devices is appealing for balance sheets and cost of ownership reasons, but could potentially offset any perceived economies by creating an adverse situation with new security and management challenges.

- Are employee-owned PCs and notebooks appropriate for your company?
- How will technology facilitate working with non-company-owned computing devices?
- How must enterprise policies change to ensure risk containment?

John Girard and Brian Gammage

Password Management and Enterprise Single Sign-On

We seemingly cannot avoid passwords, so how can they be managed to reduce support requirements and improve convenience? The session will also highlight market analysis of password reset, synchronization, and single sign-on vendors.

- What are the options for management passwords in complex environments?
- Which vendors offer competitive password management and single sign-on solutions?
- What are the best practices for implementing password management and single sign-on tools?

Gregg Kreizmann

Officer, Someone's Stolen My Identity Management!

Identity management has become an overused and misunderstood term, expanded to mean more than the traditional enterprise view of user provisioning and workflow. This has implications for both enterprises and consumers unless the taxonomy is understood, particularly when dealing with vendors.

- What identity management is and isn't
- Tools and techniques for 'identifying' and communicating IAM in your security programs
- Applying real identity management solutions for consumers and employees

Earl Perkins

Federated Identity Management and Personal Identity Frameworks

Federated identity management offers lower costs for B2B federations and user SSO. Digital identity evangelists tout new frameworks and technologies offering privacy, convenience and trust as the necessary for online services and commerce.

- What are the business drivers for federated identity management?
- What are personal identity frameworks (PIFs)?
- Can enterprises find competitive advantage by supporting PIFs?

Gregg Kreizmann

The Un-death of Public-Key Infrastructures

There may be truth in the rumours that the death of PKI may be only slightly exaggerated. With new deployments within government and corporate settings, a review of the un-death of PKI is warranted.

- What is fueling the PKI life support?
- What are the lessons learned in actual successful and in-use PKI deployments?
- Will PKI/PKO adoption grow and continue to breathe life or are there challengers looking at finally pulling the plug?

Eric Ouellet

IAM Audit and Compliance

Regulatory compliance is driving most of the increased identity management implementations being done today. This session will highlight the regulatory compliance issues for IAM, the contribution of different IAM products to compliance, and management of the IAM compliance process.

- What are the regulatory compliance issues for IAM?
- How does each IAM product component contribute to overall compliance efforts?
- How should managers manage the IAM/compliance process?

Earl Perkins

TRACK 3: RISK MANAGEMENT AND COMPLIANCE

IT Risk: Turning Business Threats into Competitive Advantage

Business executives, including CIOs, must now manage IT risk as business risk with business consequences. This presentation, based on the recently published Harvard Business School Press book, outlines a new model for integrated risk management based on three key disciplines.

- How will IT risk drive business decision-making?
- What approaches to IT risk management will be most effective for businesses and CIOs?
- What mechanisms should businesses adopt to manage IT risk effectively?

Richard Hunter

Global Security and Privacy Strategies

Almost every company has international operations or suppliers and service providers in emerging markets. This presentation details country-specific security and privacy indicators, service provider security, and privacy ratings. In addition, it examines:

- Practices for dealing with issues such as how and whether to maintain different security standards for international operations
- Sourcing, data transfers, employee monitoring and marketing privacy
- Security risks in a global world

Arabella Hallawell

Security Architecture Best Practices

Dynamic business models make the virtual perimeter hard to define. Security architectures are rapidly maturing along with enterprise architecture (EA).

- What are the information security architecture (ISA) best practices?
- What are the best techniques for assessing the maturity of ISA practices?
- What are the main obstacles to closer integration of the ISA into the EA, and practical strategies for overcoming these obstacles?

Tom Scholtz

The Metric System: Your Executive Communications Plan

Management wants to know that the security function is providing value. So they ask for metrics. This presentation describes the current state of the quest for security metrics and provides guidelines for using them.

- How do you determine which security metrics are relevant and collectible?
- In what form are security metrics digestible by senior executives?
- How is the Formal Security Communication Plan for executives structured and completed?

Christian Byrnes

The Art of Policy Management

To be truly effective, policies need to address specific security risks, be aligned to the organizational culture and be kept current. This session will propose a framework for policy management, including:

- Which policies are most appropriate to address security threats and organizational requirements?
- How should security organizations structure and phrase policies?
- What processes should be in place to ensure that policies remain relevant and current?

Les Stevens

How to Conduct a Risk Assessment – A Play in Three Acts

The days of strictly technical RAs are over management doesn't understand them, and often doesn't want to. This session goes through a set of mock interviews with various stakeholders as part of the RA process.

- Why are risk assessments still being done from a technical perspective?
- How can we communicate risks to the business more effectively?
- How can security be better aligned with business objectives?

Jeffrey Wheatman

Business Continuity Management: The Key to Business Survival

The best laid plans can be shattered by unforeseen events. Business continuity management processes are required to ensure that operations can continue during significant disruption.

- What are the processes required to respond to an emergency, continue operating, and to re-establish 'business as usual'?
- What are the key resources, tasks and responsibilities required for a business continuity program?
- What standards, frameworks, methods and tools are there to guide a business continuity program?

Les Stevens

Information Security Lifecycle: Aligning with the Business

Organizations with successful security programs are successful because they implement cyclical process-based programmatic approaches. This presentation details the security management lifecycle with a focus on how to gauge current process maturity and how to improve each domain.

- What are the components of a successful information security program?
- How can we align the components with business goals?
- How can we measure the maturity of these processes to facilitate improvement?

Jeffrey Wheatman

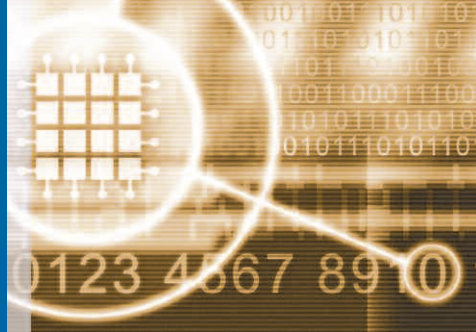
Panel Discussion: Chief Privacy Officers: Reconciling Data Privacy And Monitoring And Retention Requirements

This panel brings together leading privacy practitioners in the EU to discuss the evolving privacy landscape and best practices for managing compliance and business interests. Topics will include complying with national implementations of the EU Privacy Directive, cross border transfers and employee monitoring.

Arabella Hallawell

“Excellent overview of strategic and tactical approaches to security challenges. Good blend between Gartner insight and customer practices.”

Frits Andersen, IT Manager, Jyske Bank



New
FOR 2007

TRACK 4: INFORMATION SECURITY TOMORROW

Research Live: Gartner Analysts Debate the Future of Security Threats and Defenses

Join a team of Gartner analysts in a real-time debate of future security scenarios about technology and practice, as they offer their insight and predictions into how security practices will evolve to overcome new internal and external threats. Audience members will be encouraged to contribute their own thoughts, collaborating with the analysts to jump start a new series of Gartner research findings.

John Girard moderates other Gartner analysts

World Without Secrets

In the world without secrets, everything is recorded, and available to anyone who wants it badly enough. In an information ocean, which information can cause the most harm? Businesses that are prepared to navigate this world can create high value for themselves and their customers.

- How will the world without secrets evolve?
- What social and business roles will emerge?
- How will you position your business to thrive?

Richard Hunter

Reputation: The Next Internet Revolution

The Internet is no longer a place where everyone knows your name, so how do you know who to trust? Evaluate their reputation. Amazon and eBay demonstrated the power of reputation management, but now we are seeing the first instances of reputational war. Will your organization thrive or wither?

- Who is responsible for reputation?
- How do you gain competitive advantage through reputation management?
- Can your users evaluate reputations?

Jay Heiser

EDRM: The Future of Enterprise Security

Enterprise Digital Rights Management technology is a leading-edge technology. Engineering, manufacturing, finance, media and other industries are interested and are often getting the wrong ideas about what EDRM is about and what benefits it may bring to their organizations.

- What value does EDRM propose to the enterprise?
- What critical elements need to be in place before considering EDRM adoption?
- What does the present and future hold for EDRM deployments?

Eric Ouellet

Bubbles and Footprints: The Future Shape of Client Computing

Diverse device “footprints” must be managed, but you no longer own all the platforms. Technology offers new hope. Virtualization liberates these, turning them into bubbles of control. Gain flexibility by removing endpoints from the equation and by pursuing new ways to secure remote computing.

- How are the demands on client computing changing?
- How will client computing technology evolve through 2012?
- How do you support all categories of client computing usage and devices?

Brian Gammage and Monica Basso

Building a Community of Trust

Businesses demand more collaboration with external partners and more outsourcing, but auditors, regulators and customers expect higher privacy and control. Supply chain coordination, board communications, and outsourcing require trusted working environments that include computers belonging to other organizations.

- How can you create secure, multi-enterprise environments?
- How can flexible trust services be implemented within the application or data layers?
- What technologies can effectively support a community of trust?

Jay Heiser

DAY 3: BEST PRACTICES AND IMPLEMENTATION DAY

These sessions running across the four tracks continues the focus on best practices, implementation strategies and methodologies.

Implementing Controls for IT Security Processes and Technologies

Mark Nicolett

Federated Identity Management and Personal Identity Frameworks

Gregg Kreizmann

Business Continuity Management: The Key to Business Survival

Les Stevens

Getting to Next Generation Network Security

John Pescatore

Authentication Marketplace: I Want That One

Ant Allan

Information Security Lifecycle: Aligning with the Business

Jeffrey Wheatman

How to Secure Wireless Email and Other Vulnerable Applications

Monica Basso

IAM Audit and Compliance

Earl Perkins

Panel Discussion: Chief Privacy Officers: Reconciling Data Privacy And Monitoring And Retention Requirements

Arabella Hallawell

Market Players: Magic Quadrant Power Session

**John Girard
Mark Nicolett
Eric Ouellet
Earl Perkins**

Gartner Keynote II: To Perimeter or not to Perimeter, the Firewall Is the Question

Joseph Feiman and Brian Gammage vs. John Pescatore and John Girard

These Gartner presentations on Day 3 will be complemented by 6 end-user case studies.



Sponsors

Meet innovative technology and service providers at the forefront of IT security. At the Summit we'll help you develop a "short list" of technology providers who can meet your particular needs. We offer you exclusive access to some of the world's leading technology and service solution providers in a variety of settings. Visit the demonstration forum, attend the sponsor presentations and join in the networking drinks reception for informal relationship-building.

PREMIER SPONSORS



Cisco Systems

Cisco's Self-Defending Network (SDN) provides an integrated security approach to ensure business continuity and protect against threats. With security threats increasing in number and sophistication, businesses want to gain protection, control, and visibility over their systems, proactively preventing incidents and threats that disrupt productivity, impact customer relationships, and erode profits. The SDN approach to security provides the flexibility organizations need in order to protect their business whilst staying ahead of the rapidly evolving threat landscape.

www.cisco.com/go/security

Internet Security Systems, an IBM Company

Internet Security Systems, an IBM Company

Internet Security Systems, an IBM Company, is the trusted security advisor to thousands of the world's leading businesses and governments, providing pre-emptive protection for networks, desktops and servers. An established leader in security since 1994, the IBM Proventia® integrated security platform is designed to automatically protect against both known and unknown threats, helping to keep networks up and running and shielding customers from online attacks before they impact business assets.

www.iss.net

SPONSORSHIP OPPORTUNITIES

If your organization is interested in sponsoring this event, please contact James Berg for further details.

Tel: +44 (0)1784 267898

Email: james.berg@gartner.com

PLATINUM SPONSORS

Aladdin Knowledge Systems



Aladdins' Software Rights Management products are the #1 choice of software developers and publishers to protect intellectual property, increase revenues, and reduce losses from software piracy. Aladdin eToken is the #1 USB-based authentication solution. The Aladdin eSafe secure Web gateway provides the most advanced protection against the latest Web-based threats and attacks.

www.aladdin.com

Cybertrust



Cybertrust is the global information security specialist, delivering services that secure critical data, protect identities and help customers demonstrate ongoing compliance. Headquartered in Herndon, Virginia, USA with more than 30 offices around the globe, Cybertrust is one of the world's largest providers of information security and is recognized as the global market leader in managed security services.

www.cybertrust.com

Gemalto



Gemalto, a leader in digital security (€1.7 billion revenues in 100 countries), provides end-to-end solutions: development of software applications, production of secure personal devices, and management of deployment services. More than a billion people use our solutions for telecommunications, financial services, e-government, identity management, IT security and many other applications.

www.gemalto.com

NetIQ



NetIQ is a leading provider of integrated systems and security management solutions. With powerful features such as real-time security monitoring and protection, mapping threat indicators, policy violation alerts and expedited incident forensics & resolution, NetIQ Security Management solutions deploy quickly and easily to assure effective protection from, and response to, security-related threats.

www.netiq.com

SafeBoot



The SafeBoot suite of mobile data security solutions protects data, devices and networks against the risks associated with loss, theft, and unauthorized access. SafeBoot is the vendor-of-choice for leading global organizations and provides them with powerful encryption and strong access control technologies that seamlessly integrate with existing enterprise systems.

www.safeboot.com

"The IT Security Summit has given me fresh insight into today's and tomorrow's security issues. I can now validate our strategy with confidence."

Paul Herbert, Senior Technical Specialist, States of Jersey

SILVER SPONSORS

Citrix Systems

Citrix Systems, Inc. is the global leader and the most trusted name in application delivery infrastructure. More than 180,000 organisations worldwide rely on Citrix to deliver any application to users anywhere with the best performance, highest security and lowest cost.
www.citrix.co.uk



ArcSight

ArcSight, a leader in Security and Network Information Management, delivers mission-critical solutions for security, network and IT operations that enable enterprises to turn operational data into action.
www.arcsight.com



Fortify Software

Fortify Software's application security solutions are used by government and Fortune 1000 companies, including 7 of the 8 world's largest banks, to hack-proof their software.
www.fortifysoftware.com



Finjan

Finjan is a leading provider of web security solutions for businesses and organizations.

Finjan's award-winning Vital Security™ Web Appliances utilize patented real-time code inspection technology, enabling enterprises to block malicious web attacks (e.g. spyware, phishing, Trojans, and other malicious code) on the fly, without requiring signatures or patches.

www.finjan.com



GuardianEdge

GuardianEdge, the leader in endpoint data protection for the enterprise, serves more than two million users at leading commercial and government organizations worldwide.
www.guardianedge.com



Imprivata

Imprivata develops an enterprise single sign-on solution that dramatically simplifies password administration and enhances IT security. Imprivata's OneSign product is packaged as an affordable, easy-to-implement appliance.
www.imprivata.com



Pointsec

With the most users, certifications, and the broadest platform support – including Vista – Pointsec, a Check Point company, is the undisputed global leader in data security.
www.pointsec.com



Qualys

Qualys, the leader in on-demand vulnerability management, allows security managers to effectively strengthen the security of their networks, conduct automated security audits and ensure compliance.
www.qualys.com



LANDesk

LANDesk delivers cost-effective and intelligent systems, security and process management solutions. LANDesk® solutions simplify IT management of desktops, servers, mobile devices and processes. LANDesk has focused on developing systems and security management solutions for more than 19 years and is now leading the convergence of the systems and security and process management markets.
www.landesk.com



RSA Security

RSA, The Security Division of EMC, offers industry-leading solutions in identity assurance & access control, encryption & key management, compliance & security information management and fraud protection.
www.rsasecurity.com



Sourcefire

Sourcefire (Nasdaq: FIRE), SNORT® creator, is the leader in Enterprise Threat Management (ETM) – unifying IPS, NBA, NAC, and Vulnerability Assessment technologies under one management console.
www.sourcefire.com



Postini

With over 36,000 businesses using our services, Postini is the global leader in on-demand communications security, compliance, and productivity solutions for email, instant messaging, and the web. Postini protects users from spam, viruses, phishing, fraud and other attacks; ensures messages are secure; and archives content for e-discovery and regulatory compliance.
www.postini.com



TippingPoint

TippingPoint, the leader in intrusion prevention systems (IPS), provides the IPS-Secured Network, which delivers attack control, access control and application control.
www.tippingpoint.com



Tumbleweed

Tumbleweed is the industry's leading pure play messaging security vendor. We provide the most comprehensive solution for both inbound/outbound email and file transfer needs.
www.tumbleweed.com



VeriSign

VeriSign's digital infrastructure enables and protects billions of interactions daily across the world's voice and data networks. We enable delivery of integrated marketing campaigns and content across PC's, mobile phones and TV; mobile banking, VoIP, video over broadband and layered security solutions that protect consumers, brands, websites and networks.
www.verisign.com



Vontu

Vontu is the leading provider of Data Loss Prevention solutions that protect data anywhere-at rest, in motion or at the endpoint.
www.vontu.com



How to Register

On-line: europe.gartner.com/security
Telephone: +44 (0)1252 771 060
Email: gg@delegate.com

Registration Rates

Summit Only

- Standard Rate: €2,695 + 17.5% VAT
- Early Bird: €2,395 + 17.5% VAT
(offer ends 20 July 2007)

Why register early?

- Save €300 on the standard conference rate – available on cash registrations only
- Save time – we'll send you your fast track entry badge so you can skip the queues onsite
- Priority One-on-One booking with the analyst of your choice

Special team discounts 4 for the price of 3

Register as a team of 3 or more and:

- Receive one additional free pass
- Get preferential access, as a team, to your preferred analyst of choice
- Exclusive meeting rooms for intra-team meetings onsite, subject to availability

Note: Available on the Standard Rate only. One discount applies

Gartner Clients: We also accept Gartner conference tickets as full payment for the Summit. An additional fee of €495 + 17.5% VAT for the third day will apply. If you are a client with queries about tickets, please contact your sales representative or email isoemea.enquiries@gartner.com.

Update Your Profile

Gartner Events realize your time is precious. That is why we only want to send you information that is relevant to your role. Update your profile with us and we will send you information that is best suited to you. Visit experiencegartner.com

Upcoming events

For further details on any of these events visit gartner.com/events

Gartner is the leading provider of research and analysis on the global information technology industry. Our goal is to support organizations as they drive innovation and growth through the use of technology.

As in our research, our events help clients make informed technology and business decisions by providing in-depth analysis and actionable advice on virtually all aspects of technology.

Gartner European Events in 2007/08

Application Integration & Web Services Summit
19 – 20 June 2007, Rome

Identity & Access Management Summit
25 – 26 June 2007, London

Portals, Content & Collaboration Summit
5 – 6 September 2007, London

CIO Summit
11 – 12 September 2007, Barcelona

Financial Services Technology Summit
24 – 25 September 2007, London

Enterprise Architecture Summit
26 – 27 September 2007, London

Data Center Summit
22 – 24 October 2007, London

Symposium/ITxpo
4 – 8 November 2007, Cannes

Gartner Strategie & Technologie Konferenz
3 – 4 December 2007, Frankfurt

Business Intelligence Summit
5 – 7 February 2008, Amsterdam

Customer Relationship Management Summit
18 – 19 March 2008, London

Wireless & Mobile Summit
23 – 24 April 2008, London

Business Process Management Summit
28 – 30 April 2008, London

Symposium/ITxpo
11 – 14 May 2008, Barcelona

Outsourcing & IT Services Summit
2 – 4 June 2008, London

Related Gartner US Events

Identity & Access Management Summit
14 – 16 November 2007, Los Angeles

IT Security Summit
8 – 11 June 2008, Washington DC

Compliance & Risk Management Summit
3 – 5 March 2008, Chicago

MEDIA PARTNERS



InformationAge



SECUREIT
www.secureit-online.com

silicon.com

ZDNet UK
www.zdnet.co.uk

Gartner
IT Security
Summit 2007

17-19 September 2007
Royal Lancaster Hotel, London