Gartner Information Security Summit 2009

June 28 – July 1, 2009
Washington, D.C.

Evolve your role. Optimize value. Protect the business.

EARN CPE CREDITS!
See Page 7 for details.

Conference Co-Chairs

Vic Wheatman
Managing VP

Chris Byrnes
Managing VP

John Pescatore
VP Distinguished Analyst

Gartner
Information Security
Summit 2009

Evolve Your Role.
Optimize Value.
Protect the Business.

Information Security is evolving – fast. You can thank the hackers and cyber-attackers for that. But now what? The economy has toughened. And IT Security budgets may soon feel the squeeze. Meanwhile "the bad guys" are on the prowl – ready to compromise your data, your customers and your infrastructure. The good news? Protecting the business at a time like this may be the perfect opportunity to optimize value for the organization and enhance your role as an Information Security Pro.

Here's how to make that opportunity work for you. **Attend Gartner Information Security Summit, June 28 - July 1 in Washington, D.C.**

Our focus is two-fold and encompasses both the short- and long-term objectives you're juggling in an uncertain business environment. **Regarding the here and now:** which tools, technologies and management practices do you need to run a security operation that's efficient, safe and economical? **And about the future:** how will you position yourself inside and outside the organization and increase your effectiveness as an Information Security Professional over the next five years?

The 2009 agenda casts a comprehensive net of analysis and insight from the network to the boardroom. With drill-down vigor, our team of analysts will examine your role in Information Security Management, discuss the technologies critical to the network, offer guidance on keeping your data and applications requirement-ready and secure, explore privacy policies and privacy protection tools, and consider emerging trends and new Federal initiatives regarding cyberspace. You'll discover how to:

- **Understand** the growing interconnectedness of Security, Information Assurance, Business Continuity and Risk.
- **Communicate** your value to the business more effectively at an especially urgent time.
- **Keep pace** with evolving information security technologies.
- **Assess** your career path and its potential trajectory inside and outside your organization.
- **Pursue** cost-optimization strategies while continuing to meet security and compliance mandates.

Turn to page 11, for a full description of each of the six compelling conference tracks. There are more than 75 sessions in all, across three and half days.

Register today for Gartner Information Security Summit, June 28 - July 1. See page 15 for details or go to gartner.com/us/itsecurity.

Regards,

Vic Wheatman
Managing VP

Chris Byrnes
Managing VP

John Pescatore
VP Distinguished Analyst

CISO INVITATIONAL PROGRAM

This program, running concurrently with the Summit, is by invitation only to qualified senior-level decision-makers with budget authority from large or midsized organizations/agencies whose on-the-job experience is three years or less. For details and to submit an Application, please visit **gartnerinfo.com/ciso**.

New Dynamics, Stresses and Threats. It's Getting Personal

Information Security is getting personal. And it's just not about data and identity theft. It's about how you view your role within the organization at a time of economic and organizational stress. Can you increase your professional effectiveness and optimize the value you provide? Do you have the right tools to move forward? Gartner Information Security Summit shows you how to get it right…how to protect the business at this critical juncture and strengthen your on-the-job performance – now when it counts more than ever. Guided by our noted of team of Information Security analysts, you'll see how to:

- **Assess** security and risk specific to your industry.
- **Articulate** the business value of information security and implement effective techniques to optimize the costs of current projects and initiatives.
- **Tighten** your security with quick payoff strategies to stay on top of evolving threats.
- **Find out** the most efficient and effective ways to protect your data and applications.
- **Ensure** your security spending strategies support the core-competencies of the business and the needs of the customers driving the bottom line.
- **Understand** what boards of directors and line-of-business execs really want from risk management, GRC and security.
- **Discover** best practices for network testing and evaluation.
- **Make sure** your security policies and procedures meet future business and legal requirements.
- **Assess** your professional skill-set and enhance both your technical and business perspectives in tough times.

New and Notable for 2009

- **Interactive workshops** exclusively focused on your management and organizational issues from security metrics to dealing with managed providers – **Track F: Professional Effectiveness Workshops**
- **Get the real story behind the headlines –** timely and insightful case studies address what's happening in key industry sectors, including manufacturing, health-care and financial services
- **Special sessions** on the latest security issues surrounding cloud computing, virtualization, social networking, consumerization of IT and more
- **Industry experts discuss** the best career path to the C-level
- **Keynotes and panel discussions** examine the role of the Information Security professional from a variety of perspectives

Who Should Attend

- CIOs, CSOs, CISOs, and CTOs
- IT vice presidents and directors
- Network managers
- Risk managers
- Auditors
- Senior business executives
- Anyone involved in enterprise-wide security and critical infrastructure protection

Meet the Gartner Analysts

65% of the Fortune 1000 and 85% of the Global 500 support their key technology decisions with Gartner insight; these varied and worldwide connections produce insights that benefit all our clients.

Ant Allan
Research VP

Coverage Area: Information security topics, chiefly identity and access management and user authentication

Chris Byrnes
Managing VP

Coverage Area: Technology direction, security trends and best practices

Perry Carpenter
Research Director

Coverage Area: Security/Risk/Privacy/Comp; Secure Bus Enablement; Secure Business Enablement

Joseph Feiman
VP & Gartner Fellow

Coverage Area: Applications security technologies and methodologies enabling secure software life cycle, data privacy, security of large systems and packaged applications, legacies, SOA, Web 2.0 and security as a service

Peter Firstbrook
Research Director

Coverage Area: Client security best practices and technologies, including antivirus, spyware and spam

John Girard
VP Distinguished Analyst

Coverage Area: Business security & privacy solutions for wireless & mobile road warriors, extranet, remote offices and teleworkers

Arabella Hallawell
Research VP

Coverage Area: Security markets such as antivirus, e-mail security and Web filtering

Jay Heiser
Research VP

Coverage Area: IT risk management and compliance, security policy and organization, forensics, and investigation, trust-enabling technologies and processes, investigation and case management tools, and the control of user-developed applications

Adam Hils
Principal Research Analyst

Coverage Area: Information security trends in the small and midsize business (SMB) marketplace

Kelly Kavanagh
Principal Research Analyst

Coverage Area: Professional and managed services for network and Internet security

Avivah Litan
VP Distinguished Analyst

Coverage Area: Financial fraud, authentication, identity theft, fraud detection and prevention applications and other areas of information security and risk

Neil MacDonald
VP & Gartner Fellow

Coverage Area: Operating system and application-level security strategies

Mark Nicollet
VP Distinguished Analyst

Coverage Area: Vulnerability management, patch management, security information and event management and network access control

Lawrence Orans
Research Director

Coverage Area: Integration of security within internal networks, with a particular emphasis on network access control, VOIP and content filtering

Eric Ouellet
Research VP

Coverage Area: Digital rights management, PKI, cryptography, secure e-mail, directories, identity and password management, biometrics, BCP/DRP and risk management

617 Combined Years of Experience
Gartner analysts presenting at the 15th annual Information Security Summit have a combined 617 years of experience in the IT industry. You'll benefit from their real-world experience covering the areas as they evolved into the technologies we know today.

Earl Perkins
Research VP

Coverage Area: Security & identity, identity and privacy, Web services and DOA security, Software-as-a-Service (SaaS) security

John Pescatore
VP Distinguished Analyst

Coverage Area: Network security, Windows security, wireless LAN security, hardware security platforms and payment card industry security

Paul Proctor
Research VP

Coverage Area: Legal and regulatory compliance, event log management, security monitoring (host/ network IDS/IPS), security process maturity risk management programs, forensics and data classification

Tom Scholtz
Research VP

Coverage Area: Security management strategies, technologies and trends, information security policy design, security organizational dynamics and security management processes

Ray Wagner
Managing VP

Coverage Area: Public key infrastructures and related applications, as well as the five-year security scenario

Jeff Wheatman
Research Director

Coverage Area: Security program management, security metrics, risk and vulnerability assessment, risk management and database security

Vic Wheatman
Managing VP

Coverage Area: Public key infrastructures and related applications, as well as the five-year security scenario

Andrew Walls
Research Director

Coverage Area: Information security practices and markets in the Asia/Pacific region

Roberta J. Witty
Research VP

Coverage Area: Business continuity management and disaster recovery

Greg Young
Research VP

Coverage Area: Network security

John Pescatore named among *Baseline Magazine's* 50 Most Influential People in Business IT.

Our community of **650 analysts** answers **200,000 one-to-one client** inquiries each year.

Keynote Sessions

Chris Byrnes
Managing VP

Opening Keynote Session: Your Role in Information Security

Information security only started maturing in the 1990s, when distributed computing and pervasive networking resulted in a dramatic increase in business dependency on IT. This coincided with a dramatic increase in risk. Maturation implies change. Using other examples of IT maturation, we can better understand what an information security professional will look like five and more years from now.

- What are the key roles and responsibilities of information security practitioners today?
- How will those key roles change over the next five to seven years?
- Which direction should you set for your career in information security and risk?

Paul Proctor
Research VP

"My Role in Information Security" from Four Perspectives: Engineer, Auditor, CISO, and CIO

This session features a panel of seasoned professionals who view information security from different perspectives at very different organizations. Topics for discussion include the evolution of information security, how to address today's challenges, and the relationship among the four different information security stakeholders. The session concludes with a cage match between the auditor and the CISO! Just kidding.

Ray Wagner
PhD

The CISO's Skill Set

This panel is uniquely positioned to address the skills a successful CISO needs. The job of CISO has evolved from one requiring in-depth technical knowledge into one requiring a well-rounded business perspective. But an understanding of the technology is still key to informed decisions. Furthermore, links among security, information assurance, business continuity and risk have strengthened.

- What are the cool jobs in information security?
- What is the market looking for in information security professionals?
- What is the best career path to the C-level?

David Sanger
Author

The Inheritance: The Challenges to the New Administration in Cyberspace

The race for the presidency in 2008 was one of the most consequential in modern American history. When Barrack Obama settled into the Oval Office, he inherited an agenda of problems unseen in Washington since the Cold War. Beyond Iraq lie problems more directly related to American security than any being fought out on the streets of Baghdad.

In his keynote, Mr. Sanger walks the audience through three scenarios that depict terrorism vulnerabilities: a crude, low power nuclear device set off in Washington D.C.; biological weapons; and a cyber attack capable of disrupting electronic communications, commerce and financial transactions, destroying power generators and transmission lines and neutralizing our defenses.

In a talk that takes us inside the Bush White House, and then propels us into the future, Mr. Sanger explains how we got here and where we may be going next.

Worst Best Practices and Useless Useful Technologies, Unmasked

In this interactive "just-for-fun" session, a panel of Gartner analysts debates recommended practices and hyped technologies, which may be a bit off-the-mark. Audience members can make nominations and give their opinion. In turn, analysts will debate the merits of each nominated technology or practice.

Track Descriptions

Explore. Assess. Advance.

Understand the role you play and the value you bring.

Six tracks and more than 75 sessions. The 2009 agenda is designed around the chief organizing principles that support a sound master strategy for IT security in today's economy.

A

The CISO's Role: Information Security Management Planning

The job of Chief Information Security Officer has evolved. Sometimes you came up through the ranks, maybe from network security, maybe from the audit department. You may know something about "the business" or maybe you're focused – too much – on technological solutions to infosec problems. These sessions will help you round out your knowledge and skills to meet the challenge of the job.

B

The Network Security Professional

Connectivity. Without it we're isolated and can't do business. The perimeter is porous, the challenges growing, the threats mutating and the bad guys are getting more and more creative. Keeping up means understanding how the tools are evolving, where they fit, where they overlap and where they truly show value.

C

Applications and the Security Role

Applications run the business. The first task is to make sure they work and meet the requirements. Too often, the question "is it secure?" is an afterthought. Let's fix that.

D

Security and Risk in Your Industry

Each industry sector is a little bit unique. Some industry initiatives are specific, some more general, but all offer something from which other businesses can learn.

E

Privacy and Data Security: Working with the Chief Privacy Officer

Privacy is the consumer version of security, but it also applies to corporate privacy, i.e., protecting intellectual property and the data your company or agency has been entrusted to protect. How can privacy be addressed within the information security domain?

F

Professional Effectiveness Workshops

Combining tutorials and interactive exercises, these sessions provide the tools and techniques needed for individual success in your information security and risk management programs.

Earn CISSP® CPE Certification

Any CISSP® holder who attends the Gartner IT Security Summit will receive Group "A" Credits. An attendee can provide their name and certification number when they register onsite at the registration desk. Gartner will submit the request on the attendee's behalf.

Get Valuable CPE Credit

Earn ISACA Continuing Professional Education Credits (CISA, CISM and CGEIT) by attending those conferences sessions that advance your knowledge and skill in the following areas: management, information security, audit and control, and governance. For information on which Summit sessions qualify for accreditation, contact certification@isaca.org.

Agenda At a Glance

Analyst/User Roundtable sessions are designed for peer knowledge exchange about key issues. For a complete topics listing, please see **page 22**.

Sunday, June 28, 2009

2:00-7:00pm	Pre Registration		
Pre-Conference Tutorials (Free)			
4:15pm	**T1.** Security Market: Market Shares and Forecasts for Providers* **For High-Tech and Telcom Providers Only*		**T2.** Data Loss Prevention Tutorial
5:30pm	**T4.** Security for SMBs – Opportunities and More Opportunities		**T5.** IAM 101

Monday, June 29, 2009

7:00am-6:30pm	Registration		
8:00am	**Welcome and Introductions: Vic Wheatman**		
8:15am	**Opening Gartner Keynote: Your Role in Information Security NEW**		
9:30am	**Gartner Keynote: My Role in Information Security from Four Perspectives: Engineer, CIO,**		
10:45am	**Gartner Keynote: The CISO's Skill Set NEW**		
11:45am	**Solution Showcase Dessert Reception and Analyst in the Box Show Floor Presentations:**		
	11:45am-12:05pm: Intrusion Prevention Systems Magic Quadrant		
1:45pm	**TRACK A: The CISO's Role**	**TRACK B: The Network Security Professional: Addressing the Threats**	**TRACK C: Applications and the Security Role: Doing Business**
	A1. What Every Security Professional Needs to Know About Risk: 5 Tips	**B1.** Staying Ahead of Next Generation Threats and Vulnerabilities	**C1.** Application Security Scenario
3:00pm	**Solution Provider Sessions and Case Study Presentations**		
4:15pm	**Solution Provider Sessions and Case Study Presentations**		
5:30pm	**A2.** Articulating the Business Value of Information Security	**B2.** Four New Network Security Technologies You Should Know – Four Predictions **NEW**	**C2.** The Role of the Identity and Access Manager
6:30pm	**Solution Showcase Reception**		

Tuesday, June 30, 2009

7:00am	**Networking Breakfast**		
8:00am	**Keynote Session: The Inheritance: Challenges to the New Administration in CyberSpace,**		
9:15am	**A3.** Don't Be a Dr No: A Framework for Positive Information Security Management	**B3.** Securing Virtualization, Virtualizing Security	**C3.** The Role of the Business Continuity Manager
10:30am	**A4.** Integrating Physical and Information Security **NEW**	**B4.** Deploying a Multi-Function Firewall: Scenarios and Best Practices **NEW**	**C4.** New Technologies, New Technologists – IT Consumerization and Information Security **NEW**
11:30am	**Solution Showcase Dessert Reception and Analyst in the Box Show Floor Presentations:**		
	11:30-11:50am: Business Continuity Hype Cycle		
1:30pm	**Solution Provider Sessions and Case Study Presentations**		
2:45pm	**A5.** Do You Know Security? Prove It!	**B5.** Securing the Web Gateway	**C5.** Securing SharePoint **NEW**
4:00pm	**Solution Provider Sessions and Case Study Presentations**		
5:15pm	**A6.** Doing More with Less: Security and Risk Management in Economically Challenging Times	**B6.** Working Remotely: Telework and Network Security **NEW**	**C6.** Balancing Control and Creativity: Five Alternatives to Desktop Lockdown **NEW**
6:15-9:15pm	**Hospitality Suite Event**		

Wednesday, July 1, 2009

7:30-8:30am	**Breakfast with the Analysts**		
8:30am	**Keynote Session: TBA – Towards a National CyberSecurity Policy NEW**		
9:45am	**Solution Provider Sessions and Case Study Presentations**		
11:00am	**A7.** Integrating Security into ITIL v3 Strategies: Case Study and Best Practices	**B7.** The Changing Face of NAC	**C7.** Aligning Security Assessment and Monitoring with Business Objectives **NEW**
12:00pm	**Solution Showcase Reception and Lunch on the Showfloor**		
1:30pm	**A8.** Policies: Proactive Plan for Protection or Purposeless Pile of Paper? **NEW**	**B8.** What You Need to Know about Cloud Computing and Security **NEW**	**C8.** How You Can Select – and Implement – New Authentication Methods
2:30pm	**General Session: Worst Best Practices and Useless Useful Technologies Unmasked NEW**		
3:45pm	Closing Remarks		

	T3. Your Avatar's Role in the Social Software Revolution **NEW**	
	T6. How to Sell Yourself: A Workshop **NEW**	

CISO, and Auditor NEW

Concise twenty-minute sessions in the conference show floor theater.

12:35 - 12:55pm: MSSP Selection Criteria

TRACK D: Security and Risk in Industry Today and Tomorrow	**TRACK E: Privacy and Data Security: Working with the Chief Privacy Officer NEW TRACK**	**TRACK F: Professional Effectiveness Workshops NEW TRACK**
D1. Case Study: The Forensics Investigator in a Manufacturing Environment **NEW**	**E1.** The Privacy Role: Best Practices, Budgets, Organizational Models, Technologies And Services for Success	**F1.** Workshop Tutorial: What Should My Security Team Look Like?
D2. Case Study Interview: How General Dynamics Built Effective Security Governance	**E2.** Using Data Loss Prevention to Reduce Privacy Costs	**F2.** Beyond Security Awareness: Creating a Corporate Risk Management Culture

David Sanger, Journalist and Author

D3. Why You Can't Count on Consumer Authentication	**E3.** PKI Makes a Comeback	**F3.** Metrics and Reporting Workshop Part 1
D4. CASE STUDY: From Crisis to Security Program Maturity **NEW**	**E4.** Protecting the Endpoint	**F4.** Metrics and Reporting Workshop Part 2

Concise twenty-minute sessions in the conference show floor theater.

12:20 - 12:40pm: Defining Security in 8 Easy Pieces

D5. Security in Health Care – How to Prepare for Inevitable (?) HIPAA Enforcement **NEW**	**E5.** Case Study: The Costs and Cures of Data Breaches **NEW**	**F5.** Recruiting the Right CISO to Run Your Program **NEW**
D6. Case Study: Effective Enterprise Single Sign-On (ESSO) Implementation **NEW**	**E6.** Protecting Data and Applications from Hackers' and Employees' Attacks	**F6.** Managed Security Service Provider Selection Criteria and Requirements Workshop **NEW**
D7. Why Your IAM Project is Doomed To Failure: Big Mistakes vs. Best Practices	**E7.** Security, Privacy and the Email Administrator	**F7.** Security Process Maturity Management
D8. Case Study: Top Ten Security Lessons I Learned from Implementation of SOA for a Large Enterprise **NEW**	**E8.** Privacy Over the Airwaves Use Cases **NEW**	**F8.** Workshop Exercise: Security Program Maturity Assessment

Case Study Sessions

A7. Integrating Security into ITILv3 Strategies: Case Study and Best Practices

Tom Scholtz, Gartner

ITLv3 takes a life-cycle view of service management, as opposed to the functional approach of previous versions. While this is a major improvement, it does have major practical implications on IT security, risk and compliance strategies. This presentation addresses:

- What's new in ITILv3, and how does it impact security management strategies?
- How has a multinational organization integrated their security and risk management program into their ITILv3 program?
- What are the best practices in using ITILv3 to align security and service management strategies?

D1. Case Study: A Day in the Life of a Forensics Investigator

Jeff Miller, Eaton Corp.

This session examines the rapidly growing field of computer forensics and its application in the private sector. The case study presented illustrates how one manufacturing company created an internal center of excellence for computer forensics, the steps used to develop an internal investigation process, and tool selection for conducting their investigations.

- How and why should enterprises approach computer forensics?
- What tools are available for enterprise forensic investigations?
- What is the relationship between computer forensics and e-discovery?

D2. Case Study Interview: How General Dynamics Built Effective Security Governance

Tommy Augustsson, CIO, General Dynamics

An enterprise-wide information security governance board can improve security risk management in even the most complex environments. The most critical elements are senior-level commitment, enterprise-wide involvement and explicit accountability. General Dynamics addresses security risks via a highly advanced Information Security Review Board, with those elements represented from across the entire company.

- How did General Dynamics' Information Security Review Board (ISRB) establish an effective overall standard of security governance across a highly distributed set of primarily autonomous business units?
- How do you secure senior-level commitment and accountability?
- How can you organize governance function with representatives from many different disciplines and many different business units and organizations?

D6. Case Study: Effective Enterprise Single Sign-On (ESSO) Implementation

Mark Eggleston, Manager, Security and Business Continuity, Health Partners of Philadelphia, Inc.

There are many different methods of enabling single sign-on within an organization. Choosing the method that is best for your organization requires careful consideration and knowledge of not only your applications but also your users. Effective strategies and best practices in SSO architecture, how to meet specific HIPAA security regulations, methods for self-service password reset and provisioning will be presented, to include some lessons learned to help your SSO implementation succeed.

D8. Case Study: Top Ten Security Lessons I Learned in the Implementation of SOA for a Large Enterprise

Tom Ray

Since 2004, Tom Ray has been implementing a services oriented approach at Washington Mutual Bank as its SOA Security Architect. In that timeframe the company has successfully rolled out numerous internal /external services across its Credit Card, Commercial and Retail business units, enabling secure banking in and across each. In this session, Tom will share some of the key insights and experiences gained by the business along the way and shed some light on the critical technologies involved:

- 24x7 availability
- Continuous operations
- Business continuity management

Our interactions with **60,000 clients, representing 10,000 distinct organizations worldwide,** enable us to understand patterns and discover trends no other research firm can envision.

Pre-Conference Tutorials

T1. Security Market Marketshares and Forecasts for Providers

A session for security vendors that offers a snapshot of how their positions have changed, relative to last year, and where they now stand with competitors. Given global economic pressures and shifting customer dynamics, we'll look at how the market may change in the future.

- Which security vendors are gaining market share in their specific focus areas?
- Given the current economic environment, how are customer dynamics and the security market changing?
- Which vendors will prosper in 2010?

Adam Hils and Greg Young

T2. Data Loss Prevention (DLP) Tutorial

There are multiple technologies fitting the definition of Data Loss Prevention. DLP is designed to protect intellectual property and sensitive data. Understanding each potential element in a DLP program is necessary to better control and protect sensitive assets.

- What is DLP and how should it be approached?
- Which DLP tools are the most cost-effective?
- What is the relationship between DLP and Digital Rights Management, Identity and Access Management and other initiatives?

Eric Ouellet

T3. Your Avatar's Role in the Social Software Revolution

Social software is popping up everywhere, and security is playing catch up yet again. Blogs, wikis, twitters, social networks and virtual worlds simultaneously pose serious security challenges and major opportunities for security managers to prove their value and relevance to current and future business operations.

- What are the critical security issues in social software deployments?
- What are the security tools and techniques that can be applied to social software?
- How can security use social software to improve security performance?

Andrew Walls

T4. Security for Small- and Medium-size Businesses (SMBs): Opportunities and More Opportunities

As large enterprises have devoted more buying cycles to laying solid security foundations, opportunity has shifted to small and midsize companies. Smaller companies must protect themselves, their customers, and partners from threats as they follow industry compliance regimes. SMBs are devoting more money than ever to become secure. This session covers the security issues facing SMBs and how best to build, package and sell right-sized SMB solutions – internally and in the marketplace.

- How much security does an SMB need?
- How can an SMB balance risk against cost when budgeting security?
- What do SMB customers expect from security vendors?

Adam Hils & Greg Young

T5. IAM 101

Identity and Access Management (IAM) is well established as a cornerstone of information security and can deliver real business value beyond its contributions in efficient and effective security, risk management and compliance. Here we look at the pieces of the IAM jigsaw puzzle, and how they fit together.

- What are the drivers for, and benefits from, IAM?
- What are the key elements of an IAM program?
- What are the IAM technologies? Which are core, and which are fringe? Which are tactical, and which are strategic?
- How can you articulate the business value of IAM?

Earl Perkins & Perry Carpenter

T6. How to Sell Yourself: A Workshop

Whether you are looking to move into a leadership role within your organization's security team or are trying to convince management of project, you must know how to sell yourself. This presentation focuses on the strengths you bring to the security and risk program. And you'll learn to identify the tools you need to "close."

- What are the tools needed to sell yourself to senior leadership?
- How can you demonstrate the value of your abilities?
- How can you position yourself for increased levels of responsibility?

Debra Wheatman, CPRW, CPCC

Sessions

Track A: The CISO's Role: Information Security Management Planning

A1. What Every Security Professional Needs to Know About Risk: Five Practical Tips to Link Risk and Security to Corporate Performance

A board wants to know that the organization is appropriately protected against reasonably anticipated risk. CIOs, CISOs, and RMOs struggle to link risk management efforts in security, privacy, business continuity, and compliance to the value they provide at line-of-business and executive levels. Based on a handful of companies' experiences, here are five practical tips to help you meet the challenge.

- What do boards of directors and line-of-business executives want from risk management, GRC, and security?
- How do the risk-based disciplines of security, privacy, business continuity management, and compliance impact corporate performance?
- How can CIOs, CISOs, and RMOs present a defensible case for the value and effectiveness of risk management to executive audiences?

Paul Proctor

A2. Articulating the Business Value of Information Security

The security management program is a big-ticket budget item. As budgets tighten, security expenditures will be increasingly difficult to justify. This presentation answers these key issues:

- What are the best strategies for obtaining and maintaining executive support for security initiatives?
- What is a practical model for communicating the business value of an information security program?
- What are some effective techniques for cost-benefit analyses for security project investment?

Tom Scholtz

A3. Don't Be a Dr. No: A Framework for Positive Information Security Management

Because security controls are inherently restrictive, the nickname of many organizations' information risk and security management is "Dr. No." However, there are a number of governance, process, cultural and technological actions that information security leaders can implement to align their programs closer to business strategies and needs.

- What are some of the symptoms, causes and consequences of the security control problem?
- What's the relationship between the governance, process, cultural and technical characteristics of a business-aligned security practice?
- What are short- and long-term actions you can take to more effectively align information security practices with business requirements?

Jay Heiser & Tom Scholtz

A4. Integrating Physical and Information Security

What are the prospects for merging physical and IT security systems? Focusing on the possibility of implementing a more comprehensive security posture, this presentation examines the organizational structure and changes associated with this type of operational merger. We'll also discuss the benefits, pitfalls, and best practices for getting started by using a project-based approach.

- What are the potential benefits of integrating physical and cybersecurity?
- How should organizations structure their security functions across physical and IT security?
- What are the major obstacles to integrating physical and IT security?

Vic Wheatman

A5. Do You Know Security? Prove It!

In times when even venerable IT security jobs may be at risk, you need a little bit extra to stand out from the crowd. Having a security certification can help, but it can also pigeon hole you in terms of perceived skills and capabilities. When just about everyone has some certificate or accreditation, what can you do to ensure you not only have the right kind to benefit your organization's security team, but also to advance your professional career?

- What are the benefits of IT security, privacy and risk management certifications?
- How do training, exam structure, peer review and continuous education requirements influence the value and reputation of each certification, and which ones should you consider?
- What skills and certifications should an employer look for when optimizing the team structure?

Eric Ouellet

A6. Doing More with Less: Security and Risk Management in Economically Challenging Times

How does an economic downturn impact your security and risk management strategies? Although difficult economic times can potentially increase the corporate risk profile, there are often fewer resources available to handle it.

- How can risks increase in down economic environments?
- What is the best approach to security management strategies in a down market?
- Which tools, techniques and tactics can you use to manage the situation?

John Pescatore

A7. Integrating Security into ITILv3 Strategies: Case Study and Best Practices

See page 10.

A8. Policies: Proactive Plan for Protection or Purposeless Pile of Paper?

Are policies really the foundation of information security management and the mechanism to direct the selection and implementation of security measures? Or are they piles of virtual paper with an ever-increasing last access date? This presentation discusses how to elevate policies to the status of a key control.

- What are the common problems with policy development and implementation?
- How do you ensure policies are relevant to your organization?
- How do you translate policies into actual implementable controls?
- What tools are there to help with policy development, distribution and compliance?

Chris Byrnes

Track B: The Network Security Professional

B1. Staying Ahead of Next-generation Threats and Vulnerabilities

Cyber criminals and other attackers are developing new threats just as fast as global economic conditions, business processes and IT delivery methods change. Successful businesses will take approaches to stay ahead of these threats and protect business and customer data to build customer trust.

- What changes in business processes and IT support will be required to stay ahead of evolving threats?
- Who will be the winners and losers in the future security market?

John Pescatore

B2. Four New Network Security Technologies You Should Know About and Four Predictions

Today's networks are based upon older technologies that can lead to serious vulnerabilities. The DNS protocol is flawed. IPv4 has a shortage of addresses. Most data travels unencrypted, "in the clear" over networks. Many wired networks lack authentication – any device can gain access. New technologies will help. Hear Gartner's predictions for when and how you will deploy them.

- Will the DNS vulnerability of 2008 lead to widespread DNSSEC adoption?
- How and when will 802.1AE/af lead us to encrypt data in motion?
- Will 802.1X be as commonplace in our wired networks as it is in our wireless networks?
- When, if ever, will you deploy IPv6?

Lawrence Orans & John Pescatore

B3. Securing Virtualization, Virtualizing Security

Virtualization offers an opportunity to radically transform our approaches to information security, but we must first make sure that we securely deploy the virtualized environment. Virtualization can then be used to perform introspection on hosted workloads – delivering host-based IPS without agents. Trusted hypervisors, malicious code isolation, trusted compliance watchdogs and deep-packet inspection will all be enabled using virtualization technologies.

- How should virtualization technologies be deployed securely?
- How can virtualization be used today to improve security?
- How can virtualization be used in the future to radically transform security?

Neil MacDonald

B4. Deploying a Multi-function Firewall: Scenarios and Best Practices

Today network security professionals hear much about terms like UTM, "enterprise class" UTM, and XTM. Gartner calls them what they actually are: Multi-function firewalls. This session cuts through the marketing hoopla to describe use cases and best practices appropriate to multi-function firewalls.

- In what situations is it appropriate for enterprises to deploy an all-in-one network security platform?
- Which functions should remain stand-alone?
- What should you insist upon from your vendor to extract the most value?

Adam Hils

B5. Securing the Web Gateway

The Web is simultaneously becoming more important and more dangerous to modern business. Web-based applications and services such as Skype and Salesforce.com have the ability to cut costs and improve productivity, yet few organizations have adequate solutions to effectively manage and filter Internet traffic that is flooding the LAN.

- What are the trends and implications of the evolving Web applications and Web-based malware?
- What are the key features and requirements of a secure Web gateway?
- Which vendors will your organization rely on to secure the Web gateway?

Peter Firstbrook

Sessions

B6. Working Remotely: Telework and Network Security

Conventional rules for security and privacy fail when users connect anytime and anywhere from remote locations. This session analyzes new ways technologies and business practices must converge to maintain a picture of who is getting access, where they are and what they are doing.

- How do remote telework and mobile work styles increase identity management and access control problems?
- Which security technologies will help or hinder company efforts to regain control?
- What are the best practices for designing and managing remote access security policies?

John Girard

B7. The Changing Face of NAC

NAC implementations in 2009 and beyond will be very different than what was envisioned back in the early days of NAC in 2003. Here we look at the usage cases for NAC in 2009 and share best practices for NAC and guest networking deployments.

- What key trends are shaping NAC in 2009 and beyond?
- Which vendors are leading the way with NAC?
- What are the best practices for NAC?

Lawrence Orans

B8. What You Need to Know about Cloud Computing and Security

You need visibility into your supplier's processes to ensure the appropriate level of information protection. You also need to assess the security features and service levels, and determine how well they're implemented and maintained. Proven risk assessment practices can provide a useful level of assurance that a product or service is reliable, including its capabilities to resist both accident and human manipulation.

- What type of information facilitates provider transparency, and how do you get it?
- What are the three basic ways to assess the risk associated with a supplier?
- What are the compliance concerns associated with cloud computing?

Jay Heiser

Track C: Applications and the Security Role

C1. Application Security Scenario

As attacks become more financially motivated and as organizations get better at securing their infrastructure, risks have shifted to the application level. To address these new risks, new application security marketspace has emerged. It includes security technologies such as static and dynamic application security testing, data privacy and obfuscation, software composition analysis, application hardening and shielding, security implementation practices, and service offerings.

- What new threats are applications facing?
- What technologies will secure application logic, code and data?
- What are optimal implementations of application security?

Joseph Feiman, PhD

C2. The Role of the Identity and Access Manager

IAM's role in providing effective information security is increasing. The organization for providing IAM must evolve to meet the changing role and to ensure a consistent approach in delivery. IAM must have management accustomed to rapid change and provide the direction required to be successful.

- What is the state of the current IAM market and its impact on the enterprise?
- What are some potential organizational forms to address IAM?
- What are the key skills and roles of an IAM manager?

Earl Perkins

C3. The Role of the Business Continuity Manager

The business continuity manager's job has dramatically changed over the last several years – moving from an-IT-only focus to one that is integrated into the daily business operations. But only the most mature BCM programs have made the transition. The rest are struggling to position themselves as a business change agent.

- How have mature BCM programs become a business change agent?
- How can BCM managers leverage the Gartner BCM Activity Cycle to mature their programs according to the needs and culture of their enterprises?

Roberta J. Witty

Build your own customized Agenda online.

Visit gartner.com/us/itsecurity

C4. New Technologies, New Technologists: IT Consumerization and Information Security

The consumerization of IT means that the IT organization is losing control of the hardware, software and services that productive employees will use. IT can no longer say "no" to Skype, Google Apps, Facebook, Macintosh laptops or iPhones. Combined with the growth of financially motivated, targeted threats, this trend is causing major rifts to old, rigid security programs. Here's a methodology for matching the most effective and efficient approach to staying secure while taking advantage of consumer-grade technologies.

- What new threats on the horizon will impact information security programs?
- What are the key security processes, controls and architectures that will be required to deal with the increased exposure caused by the consumerization of IT?
- Who will be the winners and losers in the security marketplace as consumerization drives changes in information security?

John Pescatore & Mark Nicolett

C5. Securing SharePoint

SharePoint is the fastest growing product in Microsoft history. Most organizations have many SharePoint instances deployed, often without regard for security or the involvement of central IT. Providing a comprehensive framework for securing SharePoint, this presentation discusses best practices and security considerations for secure deployments.

- How should SharePoint be deployed securely?
- How will entitlement and authorization management solutions evolve to secure SharePoint?
- How are security vendors evolving their offerings to address SharePoint security shortcomings?

Neil MacDonald

C6. Balancing Control and Creativity: Five Alternatives to Desktop Lockdown

As the cutting off of oxygen to bacteria forces them to go anaerobic, our attempts to lockdown desktops forces users to go anerobic. The result: an explosion in unmanaged devices that are attaching themselves to our network and systems and placing enterprise information at greater risk. Instead of locking down desktops, we offer multiple alternatives to support end-user computing using techniques such as virtualization, portable personalities and application control.

- Why have efforts to lockdown desktops failed?
- How will organizations balance the need for end-user creativity with the need for enterprise information security?
- How will future end-user computing environments evolve to support this balance?

Neil MacDonald

C7. Aligning Security Assessment and Monitoring with Business Objectives

Security event management and configuration and vulnerability assessment need to have intelligence about business processes that are accessed by monitored users and which are supported by the IT assets that are being assessed.

- Why is business alignment needed for security monitoring and assessment?
- How can IT GRCM, resource dependency mapping and IAM integration provide business context to security monitoring and assessment?

Mark Nicolett

C8. A Million Lemmings Can't Be Wrong! How You Can Select – and Implement – New Authentication Methods

Common practices are not necessarily best practices. While many enterprises continue to invest in OTP tokens for remote access and smart cards for workforce access, other risk-appropriate, easy-to-use and low-cost choices exist.

- How do you choose new authentication methods?
- How can you evaluate new authentication methods using Gartner Authentication Method Evaluation Scorecards (GAMES)?
- How does authentication fit within adaptive access control?

Ant Allan, PhD

Track D: Security and Risk in Your Industry

D1. Case Study: A Day in the Life of a Forensics Investigator

See page 10.

Jeff Miller, Eaton Corp.

D2. Case Study Interview: How General Dynamics Built Effective Security Governance

See page 10.

Tommy Augustsson, CIO, General Dynamics

44,000 technology and business professionals from around the globe benefit from the information, insight and networking opportunities at our 62 annual events; we are the world's leading IT conference provider.

Sessions

D3. Why You Can't Count on Consumer Authentication

This session positions best practices for identifying and verifying online customers and transactions against a background of increasing attacks against sensitive personal and financial data. Also examined are recommend methods for monitoring unusual activity at your site.

- What are the latest trends in attacks?
- How are customer attitudes changing because of them?
- What are the best practices for securing sensitive enterprise information using fraud detection and user authentication?
- What differentiates the key vendors supporting this fragmented market?

Avivah Litan

D4. Case Study: From Crisis to Security Program Maturity

D5. Security in Health Care: How to Prepare for Inevitable HIPAA Enforcement

There has been much noise, along with a few significant audits and an increase in calls, related to HIPAA enforcement. HIPAA security- rule enforcement has been complaint-driven and, according to the OIG, provides no visibility into the implementation of the security rule. OIG spot audits have shown significant deficiencies and have recommended that CMS establish policies and procedures to conduct security rule compliance reviews. Are care-delivery organizations ready?

- How is HIPAA enforcement likely to develop?
- How can you get your organization ready for HIPAA Security rule compliance?
- How can you pass a theoretical HIPAA audit?

Paul Proctor

D6. Case Study: Effective Enterprise Single Sign-On (ESSO) Implementation

See page 10.

Mark Eggleston, Manager, Security and Business Continuity, Health Partners of Philadelphia, Inc.

D7. Why Your IAM Project is Doomed to Failure: Big Mistakes vs. Best Practices

Your company's IAM project will be one of the most technically and logistically challenging efforts undertaken. That being the case, a high mortality rate for such projects is not surprising. This session helps you avoid common project pitfalls – both technical and non-technical – so that you can structure your project for success.

- How do you have realistic expectations for what can and can't be done in an IAM project?
- How do you manage IAM vendors?
- What are the best practices for managing your management team, i.e. expectation management and quick wins?

Perry Carpenter

D8. Case Study: Top Ten Security Lessons I Learned in the Implementation of SOA for a Large Enterprise

See page 10.

Tom Ray

Track E: Privacy and Data Security: Working with the Chief Privacy Officer

E1. The Privacy Role: Best Practices, Budgets, Organizational Models, Technologies and Services for Success

This session explores the following: new governance models for privacy, which includes Gartner survey data, the setting up of an effective privacy function and program, and terms and conditions to detail with partners and providers. Also up for discussion: detail privacy related tools and services from DLP, encryption, data masking and application security, privacy scanning and implementation and strategy, and the best and worst practices.

- How are privacy requirements evolving?
- How should enterprises set up a privacy function?
- Which tools and services supporting the privacy function are good investments, and which are bad?

Arabella Hallawell

Cost Containment is a Huge Priority Today

That's why we've developed a series of sessions on the best way to optimize your IT security investments, including the following:

A2. Articulating the Business Value of Information Security

A6. Doing More with Less: Security and Risk Management in Economically Challenging Times

E2. Using Data Loss Prevention to Reduce Privacy Costs

E6. The Costs and Cures of Data Breaches

E2. Using Data Loss Prevention to Reduce Privacy Costs

A new wave of organizations are planning to introduce DLP technologies to better control and protect sensitive assets at the perimeter, within data stores and document management systems, and at the endpoints. Once these now expensive tools become mainstream within organizations, they will impact and challenge traditional views of data classification, protection and access controls.

- Exactly what is DLP, how much of it do you need, and in what form?
- How and what kind of DLP should be leveraged to maximize effectiveness within organizations at the lowest cost and in a way that minimizes the Christmas- tree effect?
- What are the logical and most beneficial integration points with other technologies such as EDRM, IAM and others?

Eric Ouellet

E3. Public Key Infrastructure (PKI) Makes a Comeback

PKI continues to have the support and interest of corporate and government organizations world-wide. Organizations need to get a solid understanding of the real pros and cons, as well as the latest technology breakthroughs to finally leverage these concepts in a usable, scalable and cost-effective way.

- What is fueling the PKI life support?
- What are the lessons learned in actual successful and in-use PKI deployments?
- What are the trends for future deployments of PKI/PKO and other centralized cryptographic key management?

Eric Ouellet

E4. Protecting the Endpoint

The expansion of endpoint protection from traditional signature-based detection and personal firewalls, to data protection and PC lifecycle tools is well underway. This session examines what makes sense in an endpoint security package and which vendors are leading the way. We also examine the converging roles of operations and security and list the top procedural changes that will enhance the security posture of endpoints.

- What are the advantages of security and operations integration?
- What features, configuration options, and procedural enhancements will be critical for future endpoint security success?
- Which vendors are leading the way and how to negotiate effectively to get the best deal?

Peter Firstbrook

E5. Case Study: The Cost and Cures of Data Breaches

Check gartner.com/us/itsecurity for updates.

E6. Protecting Data and Applications from Hackers' and Employees' Attacks

Although it's common thinking that hackers are the greatest threat to an enterprise's data and applications, employees can pose just as serious a risk. Complying with industry regulations, a new set of technologies and practices is emerging to protect sensitive data and applications from insider and outsider attacks.

- What harm do outsiders and insiders pose?
- What data should be masked?
- How should applications be fortified?
- Which criteria should be applied to technologies and vendor selection?

Joseph Feiman, PhD

E7. Security, Privacy and the Email Administrator

This session explores e-mail and Web security trends, vendor dynamics, the role of SAAS, and how to consolidate functions including Data Loss Prevention, encryption and other features. Additionally, advice on how to negotiate with vendors, for better and less expensive protection is provided.

- What should e-mail administrators know about security and privacy?
- How can sensitive email be protected?
- How can organizations evaluate the security of third-party providers of email services?

Arabella Hallawell

E8. Privacy over the Airwaves Use Cases

The security protocols and standards for WiFi have stabilized, but the use cases for WLANs and other forms of wireless continue to evolve. The challenge today is not whether the technology is good enough to use securely. But rather which architectures, interoperability and integration are the key to secure business use of wireless technologies. This presentation explores use cases of wireless technology and provides decision frameworks for choosing the most efficient and effective security solutions.

- What strategies, best practices and technologies will enable wireless privacy?
- Which technologies, devices, infrastructure, applications and services should be integrated to assure secure use of wireless technology?
- How will future wireless standards and technologies impact today's enterprise security approaches?

John Girard

Sessions

Track F: Professional Effectiveness Workshops

F1. Workshop Tutorial: What Should Your Security Team Look Like?

Figuring out what your security team should look like, where it should report, and who owns what is always a challenge. This presentation helps clients understand the pros and cons of several common approaches to building a security and risk management program.

- What are the options for information security organizational structures?
- Where should the CISO function report?
- How can you structure your organization so it is flexible over time?

Jeff Wheatman

F2. Beyond Security Awareness: Creating a Corporate Risk Management Culture

The biggest IT risks today involve misuse and leakage of valuable information and misunderstandings of data importance by line-of-business managers. Traditional security awareness efforts are insufficient to prevent data leakage. What's more, they don't support good decisions about data criticality and business continuity needs. An effective information risk management culture requires a strategic alignment between the business and the IT risk mangers.

- How can information security evolve from figurehead status into an integral part of the business?
- Which activities encourage management support?
- What can prevent employees from circumventing security controls?
- How to ensure that business units don't negatively impact one other's security?

Andrew Walls & Perry Carpenter

F3. Metrics and Reporting Workshop, Part 1

The days of management funding for risk and security programs because it is "the right thing" are gone. It is now necessary to demonstrate to management how successful our programs are at managing and addressing security risks. This session discusses what to measure and how to measure it.

Jeff Wheatman

F4. Metrics and Reporting Workshop, Part 2

Participants work on the tools used to evaluate their enterprises, with a focus on metrics and how those measurements are conveyed to management. At the session's conclusion, participants will report back to the group for a peer review.

Jeff Wheatman

F5. Recruiting the Right CISO to Run Your Program

Finding the right leader for your security and risk program is a huge challenge. Do you look for technical skills, business leadership skills or some combination of the two? Where can you find the right candidate and how close to perfect does he or she need to be? This workshop helps senior IT leaders make the right choice in selecting a leader for one of the most important functions in any organization.

- What are the characteristics of the right leader?
- How do you interview for both hard and soft skills
- How do you make sure the fit is right, both for you and your new CISO?

Debra Wheatman, CPRW, CPCC
ResumesDoneWrite, Inc., Jeff Wheatman

F6. Managed Security Service Provider (MSSP) Selection Criteria and Requirements Workshop

From global providers with a broad array of offerings to pure-play specialists, there are many options available when selecting a managed security service provider. This workshop helps you establish criteria for choosing the service provider who best meets your requirements and service expectations.

- How can an organization clarify requirements for outsourcing security monitoring and management?
- What are the strengths and weaknesses of different types of MSSPs?
- How should organizations collect specific information from MSSP candidates to support analysis and selection?

Kelly Kavanagh & Andrew Walls

F7. Security Process Maturity Management

Assessing the maturity of security management processes is the foundation of continuous improvement in security performance. Consistent reporting on process maturity supports increases executive awareness and support. Furthermore, process maturity can also be interpreted as an indicator of the risk posture of the organization. This session examines the following:

- How should organizations define a security and risk process catalog?
- What are the steps for formalizing security and risk management processes?
- What are effective techniques for measuring security and risk process maturity?

Chris Byrnes

F8. Workshop Exercise: Security Program Maturity Assessment

Historically, it has been very difficult to assess process maturity. This session helps you leverage the Gartner Security & Risk Management Program Maturity Assessment tool to identify the current state of maturity of your program.

Paul Proctor & Jeff Wheatman

Immediate Return on Investment

In a shifting business environment, you may not know what's next, but we all know what's needed: trusted advice to navigate the cracks in the system.

A Gartner Summit is a smart investment in an uncertain economy. You'll get robust education and access: more than 75 hours of analyst-led sessions, including tutorials, case studies and keynote presentations; up to 14 hours of networking; one-hour private session with a Gartner analyst, 12 hours of Gartner Analyst/User Roundtables and more than 14 hours of interactive and streamlined vendor access and evaluation.

11 Solid Takeaways to Help You:

1. **Link risk and security to corporate performance.**
2. **See how to improve security when using virtualization.**
3. **Spot the trends in cyber security and prepare for their impact.**
4. **Evaluate the latest trends in new network security technologies.**
5. **Assess the compliance concerns associated with cloud computing.**
6. **Know which technologies will secure application logic, code and data.**
7. **Implement the very best security management strategies in a down market.**
8. **Use best practices for designing and managing remote access security policies.**
9. **See how privacy requirements are evolving and know which best practices to follow.**
10. **Understand the latest email and Web security trends plus the vendor dynamics driving them.**
11. **Connect the dots between Data Loss Management (DLP), Digital Rights Management, and Identity and Access Management (IAM).**

The Evolving Role of the Information Security Professional

Get ready to assess the part you play in information security and determine where you're headed next.

Protecting your business comes down to personal and professional effectiveness on the job. Discover how to enhance your initiatives, affect change and further your own capabilities at key sessions that focus on:

- The strengths and weaknesses you bring to your organization's Risk and Security program
- Your role in Information security seen from four different perspectives
- The skill set you need to hone to reach the C-level
- How the job of information security practitioner will change over the next five years

Solution Showcase

PREMIER SPONSOR

Google email security and archiving services, powered by Postini, enable organizations to make their existing email infrastructure more secure, compliant, and productive. The services protect against from spam and messaging threats as well as provide a central archive to locate email quickly in the event of a litigation. As a service, there is nothing to install or maintain, so organizations can simplify their IT architecture and lower costs. **www.google.com/messagesecurity**

Symantec is a global leader in providing security, storage and systems management solutions to help our customers – from consumers and small businesses to the largest global organizations – secure and manage their information-driven world against more risks at more points, more completely and efficiently. Our software and services protect completely, in ways that can be easily managed and with controls that can be enforced automatically – enabling confidence wherever information is used or stored. **www.symantec.com**

VeriSign Enterprise Security Services is a portfolio of complementary services for IT professionals seeking a balance between escalating information security demands and resource availability. VeriSign leverages proven processes, people, and technology to deliver cost-effective solutions to the many issues challenging today's IT executive. The Enterprise Security Services suite includes Managed Security Services, iDefense Security Intelligence Services, and Global Security Consulting. **http://entsecurity.verisign.com/**

Verizon Business helps companies get data in the hands of decision makers—quickly and securely; enhances business continuity strategies; improves global customer service; drives green initiatives; reduces risk; modernizes and globalizes infrastructure; increases reach and speed to market; enables the remote workforce; decreases hardware; facilities and IT operational costs through its managed services offerings. Verizon Business' breakthrough technology and continued innovation embody the company's heritage and customer-centric focus. http://**www.verizonbusiness.com/**

Websense, Inc. (NASDAQ: WBSN), a global leader in integrated Web, data and email security solutions, provides Essential Information Protection™ for more than 43 million employees at more than 50,000 organizations worldwide. Distributed through its global network of channel partners, Websense software and hosted security solutions help organizations block malicious code, prevent the loss of confidential information and enforce Internet use and security policies. For more information, visit **www.websense.com**

PLATINUM SPONSOR

CA Inc. (NASDAQ: CA) is the world's leading independent information technology (IT) management software company. We help companies manage IT to better perform, compete, innovate and grow their businesses. With our Enterprise IT Management (EITM) vision and technology, customers can unify IT and simplify the management of complex computing environments.

Cisco solutions for business security provide advanced visibility and control to protect against data leakage, botnets, and malware. By enforcing business policies and protecting critical assets, Cisco security can help your organization minimize security and compliance IT risk, reduce the IT administrative burden, and lower total cost of ownership. **www.cisco.com**

Enterasys delivers Secure Networks™ that ensure the confidentiality, integrity, and availability of IT services and the business users that rely on them – without sacrificing performance. Thousands of enterprises worldwide rely on our convergence, connectivity and compliance solutions to deliver granular, policy-based visibility and control of individual user and application priority and security. **www.enterasys.com**

Fortify Software's Software Security Assurance solutions protect companies and organizations from today's greatest security risk: the software that runs their businesses. Fortify 360 from Fortify, is the market leading suite of solutions for containment, removal and prevention of vulnerabilities in software. It detects over 380 types of vulnerabilities in 17 different development languages. **www.fortify.com**

As a global leader in information technology, **HP** applies new thinking and ideas to simplify our customers' technology experiences. Our goal is to continuously improve the way our customers – from individual consumers to the largest enterprises – live and work by providing simple, valuable and trusted experiences with technology. **www.hp.com/security**

The disciplines of IT operations and security management are converging, yet the point products keep multiplying, piling on more cost and complexity. With **LANDesk** you can control and secure your mixed IT environment from a single console and simplify your world for less money and training, and with little or no new infrastructure.

McAfee is the world's largest dedicated security technology company. We relentlessly tackle the world's toughest security challenges. McAfee's comprehensive solutions enable businesses and the public sector to achieve security optimization and prove compliance and we help consumers secure their digital lives with solutions that auto-update and are easy to install and use. **www.mcafee.com**

MessageLabs, now part of Symantec, provides a range of managed services to protect, control, encrypt and archive electronic communications. Listed as a leader in the Gartner Magic Quadrant, and with more than 19,000 clients located in more than 86 countries, MessageLabs services are widely recognized as a market leader in the messaging and web security market. **www.messagelabs.com**

Interested in Sponsorship?

Stephen Gibertoni (Companies A-G)
Senior Account Manager Events
+1 203 316 6360
stephen.gibertoni@gartner.com

David Calabrese (Companies H-R)
Account Manager Events
+1 203 316 6298
david.calabrese@gartner.com

David Sorkin (Companies S-Z)
Senior Account Manager Events
+1 203 316 3561
david.sorkin@gartner.com

PLATINUM SPONSOR

ORACLE

QUALYS

Qualys, Inc. is the leading provider of on demand IT security risk and compliance management solutions – delivered as a service. Qualys' Software-as-a-Service solutions are deployed in a matter of hours anywhere in the world, providing customers an immediate and continuous view of their security and compliance postures. **www.qualys.com**

RSA
The Security Division of EMC

RSA offers industry-leading solutions in identity assurance & access control, data loss prevention, encryption & key management, compliance & security information management and fraud protection. These solutions bring trust to millions of user identities, the transactions that they perform, and the data that is generated. For more information, please visit **www.RSA.com.**

ScanSafe

ScanSafe, the pioneer and largest global provider of SaaS Web Security, helps companies keep malware off corporate networks and enables secure Web usage. Powered by its proactive, multilayered Outbreak Intelligence™ threat detection technology, ScanSafe processes over 20 billion Web requests and 200 million blocks each month for customers in over 100 countries.

SecureWorks

SecureWorks has become one of the leading Security as a Service providers safeguarding over 2,000 organizations. Focused exclusively on security services, we protect our clients through a combination of our on-demand Security Management platform, applied research from the SecureWorks Counter Threat Unit™ and 24x7 monitoring and management by their team of GIAC-certified experts. **www.secureworks.com**

SOLUTIONARY
MAKING SECURITY MANAGEABLE

Solutionary delivers exceptional information security and excellent customer service for clients seeking to improve data security and address compliance requirements. Organizations world-wide depend on Solutionary's managed security platform, information security and compliance expertise, custom service delivery and strong commitment to solving security challenges and business issues. **www.solutionary.com**

SOURCEfire®

Sourcefire® Inc., a world leader in intrusion prevention, is transforming the way organizations manage and minimize network security risks in real time with its 3D Approach —_D_iscover, _D_etermine, _D_efend. The Sourcefire 3D™ System provides an automatic and integrated process of discovering policy non-compliance, vulnerabilities, and threats; determining impact; and taking appropriate defensive action. **www.sourcefire.com**

TREND MICRO

Trend Micro, a global leader in Internet content security, is advancing integrated threat management and data protection technologies to protect personal information and organizational data from malware, spam, data leaks and the newest Web threats. Trend Micro's security solutions are sold through its business partners worldwide. For additional information, visit **www.trendmicro.com.**

webroot

Webroot® Security Software-as-a-Service (SaaS) provides on-demand web, email and archiving solutions that offer flexible and cost-effective alternatives to on-premise security. Services require no additional hardware or software, are easy to manage, and are maintained by a global security company with a history of innovation. To learn more, visit **www.webroot.com** or call (800) 772-9383.

SILVER SPONSORS

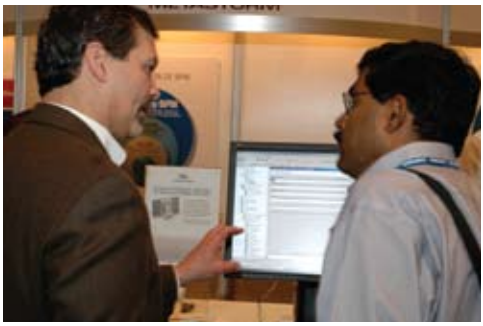
Absolute Software
Alert Enterprise
Archer Technologies
ArcSight
AT&T
BeCrypt
Beta Systems Software
BigFix, Inc.
Blue Coat Systems, Inc.
Brazil IT
Core Security Technologies
Cyber-Ark Software, Inc.
Cyveillance
Dambella, Inc.
DeviceLock
eIQnetworks, Inc.
Entrust
Finjan Inc.
ForeScout Technologies
Guardium, Inc.
IronKey
Liquid Machines
LogLogic, Inc.
Lumension Security
MX Logic
NetIQ Corporation
NitroSecurity, Inc.
nuBridges, Inc.
PGP Corporation
Proofpoint, Inc.
Protegrity
RedSeal Systems
SailPoint
Secunia
SenSage, Inc.
Splunk, Inc.
SunGard Availability Services
Symark International, Inc.
Thales
TippingPoint
Trusted Computing
Tufin Technologies
Veracode
Zix Corporation

MEDIA PARTNERS & ASSOCIATIONS

BANK INFO SECURITY
SSW SecurityStockWatch.com
TEC Technology Evaluation Centers
WSTA Wall Street Technology Association

And There's More…

Why a Gartner Event is Unique



The Gartner Information Security Summit presents timely, actionable content in the kind of engaging formats that set us apart from typical IT security events:

- Exclusive access to Gartner's team of 25 leading security analysts
- Complementary pre-conference tutorials
- Interactive audience polling
- The world's major solutions providers presented in a no-hype environment
- Timely case studies pulled from the headlines
- Informative sessions with Gartner analysts, including Analyst One-on-One, Analyst/User Roundtable, Analyst in the Box and breakfast sessions

Leverage These Tangible Benefits

- **Gain free Web access** to conference documentation for Gartner-led sessions with speaker notes included.
- Make important **business and industry contacts** and continue the dialogue, post-event.
- **Save time and effort** by accessing key solution providers in one place. Create a short-list of vendors after visiting our Solution Showcase.

Analyst/User Roundtable Sessions

(End-users only, limited attendance, pre-registration required)

- Network Access Control
- Outsourcing Security Issues and Concerns
- Retail Security Issues: Fraud, Shrinkage and PCI
- Authentication Trends
- IPS and Firewall Management
- Threats and Vulnerability Management in Financial Services and Other Industries
- IAM Issues in Government and Other Industries
- Security Organizational Structures
- SSO and Password Management
- Key Management and Data Loss Prevention

Analyst/User Roundtables are a great forum to share experiences with your peers. Gartner analysts moderate and add relevant research findings and user experiences to the discussion.

- Security Awareness Training
- Forensics Tools, Technologies, Techniques
- E-Discovery
- Security, Operations and Facilities and BCM
- Secure Software Development
- IAM War Stories

How to Register

EARN CPE CREDITS!
See Page 7 for details.

Prepare for the conference now and **BUILD YOUR CUSTOMIZED YOUR AGENDA ONLINE.** You can also access your Agenda from a mobile device. Visit gartner.com/us/itsecurity for details.

TEAM REGISTRATION DISCOUNT

When you register (5) five colleagues from the same company at the same time with credit card payment, the (5) fifth colleague may attend for free. Standard pricing applies.
Discount invalid for Gartner ticket holder and special pricing options.

NEW! ATTENDEE JUSTIFICATION TOOLS

Track the value of a Gartner Summit while you are onsite with these easy to complete documents. Record what you've learned with the **Trip Report Summary** and **ROI Session Worksheet** with space for highlights, tips and items you want to refer to in the future or share with your team. Pre-event, you can use the customized **Summit Overview Letter** that details the benefits and features you'll find onsite that can help justify your attendance. Download the documents today at gartner.com/us/itsecurity.

3 WAYS TO REGISTER

Web: gartner.com/us/itsecurity
Phone: +1 866 405 2511
Email: us.registration@gartner.com

Priority Code
Please help us to better serve your needs by providing the priority code when you register. It's located in the box above your address information on the back page of this brochure.

Registration Fees
Conference registration fee includes: conference attendance, documentation and planned functions.

Gartner Clients
We accept Gartner conference tickets as full payment. If you are a client with questions about tickets, please contact your sales representative.

Interested in becoming a Gartner client?
E-mail: client.info@gartner.com
Phone: +1 203 316 1111

Money-Back Guarantee
If you're not completely satisfied with this Gartner conference, please notify us in writing within 15 days of the conference, and we will refund 100% of your registration fee.

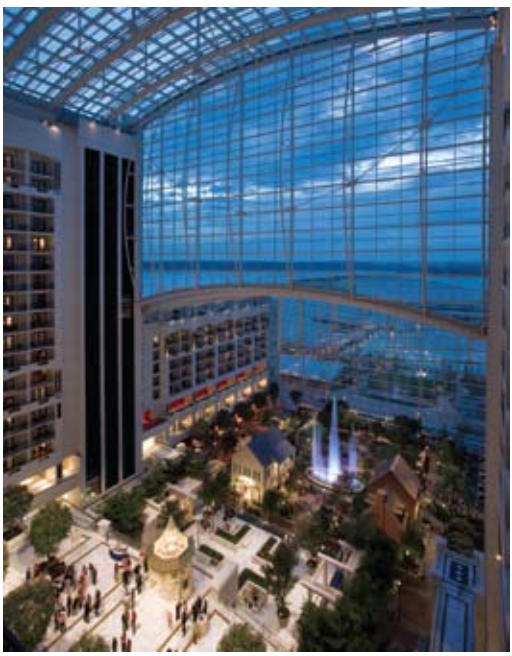
PRIVACY POLICY
Go to gartner.com/privacy

Hotel/Travel Information

U.S. $230.00 for single or double occupancy. Please call the hotel directly to make your hotel reservations. A $10 Resort Fee also applies. A limited block of rooms has been reserved at the Gaylord National. As these can only be held until May 26, 2009 we recommend that you contact the hotel as soon as possible. To obtain the group rate of $230.00 for a single or double occupancy room, please indicate that you are attending the Gartner Information Security Summit when making your reservation.

Gaylord National Resort & Convention Center
201 Waterfront Street
Washington, DC 20745
Phone: +1 301 965 2000

• **Air Fare/Rental Car Savings:** For details on travel discount information, go to gartner.com/us/itsecurity and click on Hotel/Travel.



Gartner
56 Top Gallant Road P.O. Box 10212
Stamford, CT 06904-2212 USA

Gartner Information Security Summit 2009

Evolve Your Role. Optimize Value. Protect the Business.

See Inside.

Agenda-at-a-glance

Gartner
Information Security
Summit 2009

June 28 – July 1, 2009
Washington, D.C.
www.gartner.com/us/itsecurity

Upcoming Related Events

Risk Management & Compliance Summit
April 29 – May 1, 2009
Chicago, IL
gartner.com/us/risk

Business Continuity Management Summit
April 27 – 29, 2009
Chicago, IL
gartner.com/us/bizcon

Identity & Access Management Summit
November 9 – 11, 2009
San Diego, CA
gartner.com/us/iam

As an attendee to this event,

some sessions you participate in that advance your knowledge within that discipline may earn **Continuing Professional Education** credits.

For more information see page 7.

Please use priority code below when you register:

Priority Code: **WEB09**