

## Gartner Information Security Summit 2009



June 28 – July 1, 2009  
Washington, D.C. (National Harbor, MD)

*Evolve your role. Optimize value. Protect the business.*

The 2009 Gartner Information Security Summit was held June 28 – July 1 in Washington, D.C. at the Gaylord National Resort & Convention Center, with more than a 1,000 IT security professionals in attendance. This report provides event highlights.

### Overview

At the 2009 conference, Gartner's on-site team of 25 Information Security analysts explored the organizational and market dynamics impacting the role of IT security professionals over the next five years. But that was just part of the in-depth analysis the event's 6 tracks delivered. Focus areas included:

- >> Today's critical security technologies
- >> How to keep data and applications requirement-ready and secure
- >> The latest developments in privacy profiles and protection tools
- >> Emerging trends and new Federal initiatives regarding cyberspace.
- >> Cost-optimization strategies that can accommodate security and compliance mandates
- >> The growing interconnectedness of Security, Information Assurance, Business Continuity and Risk

### REMINDER! You can earn CPE credits

As an attendee to this event, any sessions in which you participated may earn CPE credits.

Gartner is an Official (ISC)<sup>2</sup>® CPE Submitter and can submit up to 18 Type A or 2 Type B CISSP®, CAP, CSSLP, SSCP credits. Contact Tracy Runko at [tracy.runko@gartner.com](mailto:tracy.runko@gartner.com) for details.

ISACA CPE hours (CISA, CISM, and CGEIT) may be available as follows as outlined in their Continuing Education Policy at [www.isaca.org](http://www.isaca.org).

### Conference Highlights

- **An on-site team of 25 Gartner IT Security Analysts** was complemented by 14 guest speakers from a range of organizations and industries that included eBay, Time Warner, General Dynamics, British Consulate, Motorola, Providence Health & Services, and the U.S. Dept. of Justice among others.
- **Six complimentary, pre-conference tutorials** got attendees up to speed on communications skills, IAM basics, the vulnerabilities in social software and more.
- **Six tracks and 55 analyst-led presentations** covered such hot topics as data loss prevention, cloud computing, virtualization, IT consumerization and Information Security, compliance, privacy, security market forecasts, and more.
- **A compelling line-up of keynote speakers** brought incisive thinking to the day's big issues, among them were *New York Times* correspondent David Sanger and the National Security Council's Cybersecurity Director Christopher Painter.
- **Six end-user case studies** provided an inside look at how organizations are grappling with a range of challenges from massive data losses to implementing a cohesive security governance framework.
- **16 analyst-user roundtables** gave attendees the chance to trade insights with peers in a relaxed, small-group setting.
- **82 solution providers showcased** new and enhanced tools and technologies on the conference exhibit floor and walked through real-world implementations and deployments at 29 end-user case studies.
- **2009 conference additions** included an all-new workshop track, with an exclusive focus on management and organizational issues. Three new virtual tracks — dedicated to government, health care and financial services — provided specialized content for IT security pros in those respective fields.

### SPECIAL EVENTS WITHIN THE CONFERENCE INCLUDED:

- Executive Women's Meet and Greet Networking Reception
- Lunch and Evening Networking Receptions
- Birds of Feather Networking Reception
- 11 Sponsor Hospitality Suites
- Q&A Breakfast with the Analysts
- "Analyst-in-a box" sessions presented on the exhibit floor

## Keynote Sessions

### Your Role in Information Security

In which direction should you set your career in information security? Gartner analyst Chris Byrnes laid out the possibilities in the conference's opening keynote. Consider the future prospects. IT security jobs will become less about security technology and much more about risk management strategy. Although there will always be a demand for security experts, the role is headed for a profound disruption as security becomes more integrated and "less human-intensive." **The result:** "fewer people needed with in-depth knowledge of individual technologies," Byrnes said.



**Chris Byrnes**  
Managing VP

But if information security technologists expect to thrive, they'll need to master disciplines typically associated with the business – risk management, relationship management, and process management. Security executives will need the type of communication skills that can readily translate information risks into a language business understands. "If you're in a leadership role in information security, you'll have to figure out how to do this within the next five years," Byrnes noted. Expect a rapid increase in demand for security analysts capable of effective communication with non-IT staff. The new business-oriented skill set will be important to how the entire profession moves forward.

### CISO Skill Set

**PANELISTS:** Joyce Brocagila, CEO & Founder, Executive Women's Forum, Alta Associates, Inc.; Alan Paller, Director of Research, SANS Institute; David Foote, CEO & Chief Research Officer, Foote Partners LLC

In the current job market what makes a great CISO? And how do you get there? Three panelists, experts on recruitment, compensation and workplace management issues, shed light on some of the "must have" skills needed for the role. Topics discussed included: what's driving change in the information security job market; the difference between a technically focused and a holistically focused CISO, the importance of mentorship, and how to get a seat at the board table.

**BOTTOM-LINE:** At many organizations, the top IT security position is shifting focus to a "risk strategic" role. Companies are looking to hire prospective CISOs with an executive level skill set, knowledge of the business, and the ability to communicate adeptly. It's not the technology skills in demand but the soft communication skills. The CISO's job is to find people who can solve the "security" problems. And for that you don't have to know IT security from top to bottom but, rather, hire people who do.

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

**PANELISTS:** Dr. Tommy Augustsson, Chief Information Officer & Vice President of Information Technology, General Dynamics; Eric Cowperthwaite, CISO, Providence Health & Services; Jeff Goeke-Smith, Security Engineer, Michigan State University; Ken Mory, Chief Auditor, County of San Diego

Four panelists, each representing roles central to IT Security – engineer, CISO, CIO and auditor – offered their individual perspectives on a range of shared problems from governance and accountability to the evolving nature of cyberthreats. Here's their take on how the role of IT security has evolved over the last 10 years.

**Eric Cowperthwaite, CISO, Providence Health & Services:** "Security is now much more an advisor to the business. The evolution has gone from being engineer to being a risk manager."

**Jeff Goeke-Smith, Security Engineer, Michigan State University:** "Security is visible now. Our experience with internet worms like Code Red, SQL Slammer and Blaster has dramatically altered management's viewpoint -- specifically at the network level."

**Dr. Tommy Augustsson, Chief Information Officer & Vice President of Information Technology, General Dynamics:** "About four or five years ago we came under a severe attack. After that, IT security became a very high priority for us. We now approach it from a risk management perspective, which is becoming more ingrained in the DNA of the company."

**Ken Mory, Chief Auditor, County of San Diego:** "IT security has changed quite a lot, and we're not keeping up. Compliance has made a big difference. Senior managers are held accountable. But the threats are much greater. And they're coming not just from outside the country and from criminals, but from within the organization itself. These parasitic attacks, coming from the inside, are a big concern to auditors."

#### What attendees had to say:

"Very interesting, useful session. Loved the interaction. Good questions and responses."

"Outstanding! Everyone should hear this!"

"Good spectrum of viewpoints."

### Mark Your Calendar for Next Year's Summit

Gartner Security & Risk Management Summit  
June 21-23, 2010  
Washington, DC  
Gaylord National Resort & Convention Center

## Keynote Sessions, continued

### The Inheritance: Challenges to the New Administration in CyberSpace



**Presenter:** David Sanger, Chief Washington Correspondent for *The New York Times* and Author of *The Inheritance*.



**David Sanger**  
Author

In a compelling and thought-provoking keynote address, David Sanger, Chief Washington correspondent for *The New York Times* and best-selling author of *The Inheritance*, examined cybersecurity issues within the broader context of global conflicts. As old crises intersect with new technologies, the results can be unpredictable. One of the toughest challenges for policymakers looking to remake the nation's cybersecurity operations is how to deal with a new world of geopolitical upheaval, where foreign enemies route cyberattacks through servers located in friendly nations, or even in the United States itself.

#### What attendees had to say:

*"Excellent, brings it all together on how Web 2.0 has become part of our way of life and how relationships are changing in a global world."*

*"Sanger is a great presenter. I thoroughly enjoyed his speech while learning a tremendous amount"*

### Towards a National CyberSecurity Strategy: A Report Card on Federal Information Security

**PRESENTERS:** Christopher Painter, Cybersecurity Director at the National Security Council; Howard Schmidt, President, Information Security Forum; Gary McGraw, CTO, Cigital.

What steps should the federal government take to increase the security level of critical infrastructure – an infrastructure which consists of agency-owned-and-operated network computing and control systems, as well as private, commercially operated facilities? Is it by example, or can the federal agencies responsible regulate and define standards and approaches subject to mandates?

In this Townhall session, Christopher Painter, Director of Cybersecurity at the National Security Council, outlined the key findings of the recent Federal Information Security review commissioned by the White House and unveiled in late May. Central to the initiatives presented is the formation of a new position to coordinate cybersecurity policy across agencies, Congress and the private sector.

Making a video appearance at the Townhall session were Howard Schmidt of Information Security Forum and Gary McGraw, CTO of software security firm Cigital. Although skeptical of the need for a cybersecurity czar, McGraw said he was cautiously optimistic that some of the report's focus on reducing software vulnerability and cybersecurity threats will have a positive impact.

## End-User Case Study Sessions

In six end-user case study presentations, IT and business executives from leading multinational organizations shared their own valuable experiences with the audience, discussing specific technologies and solutions adopted in their own environments. Highlights from two case studies follow.

### >> Eaton Corporation: The Forensics Investigator in a Manufacturing Environment

**Presenter:** Jeff Miller, eDiscovery Program Lead, Eaton Corporation

This session examined the rapidly growing field of computer forensics — the practice of identifying, extracting and considering evidence from digital media such as computer hard drives.

Jeff Miller, eDiscovery Program Lead for the Eaton Corporation — a large diversified power management company with more than 75,000 employees and a customer based spread across 150 countries — presented his experiences in creating an internal center of excellence for computer forensics. Discussions focused on how to initiate an internal investigation, tool selection and forging a relationship within the organization between Legal and IT Security.

### >> Heartland Payment Systems: The Costs and Cures of Data Breaches

**Presenter:** Robert Carr, CEO, Heartland Payment Systems

In 2008, Heartland Payment Systems — a top-ten U.S. payment processor — suffered through one of the most sophisticated and publicized data breaches in history. The U.S. Secret Service and two breach forensics teams were called in to investigate. Ultimately, they uncovered the source of the breach: A piece of malicious software planted on the company's payment processing network that recorded payment card data as it was being sent for processing to Heartland by thousands of the company's retail clients. What did Heartland do next?

CEO Robert Carr discussed the proactive security steps taken to turnaround a nightmarish situation. Among them was the development of an end-to-end encryption solution. Carr strongly emphasized the need for collaboration within the payments processing ecosystem and noted that knowledge of security threats should not be viewed as a competitive advantage.



## Key Takeaways

Here are just a few of the key takeaways participants gained after three-days of intensive interaction with Gartner analysts, industry experts, and their peers. Selected sessions are spotlighted.

### A1. What Every Security Professional Needs to Know About Risk

Focus on results, not details. Instead of telling management how many incidents the company experienced last year, security professionals should focus on how well they managed those incidents. Follow these action steps: Formalize a risk and security program. Map Key Risk Indicators (KRI) into Key Performance Indicators (KPI). Don't use operational metrics in executive communications. And link risk initiatives to corporate goals.

### B1. Staying Ahead of Next-generation Threats

Use a two-pronged strategy: Get more efficient at dealing with old threats (platforms, vulnerability avoidance, sourcing). And get more effective at dealing with new threats (web security gateway, security in the cloud, application control, data protection.) Be sure to institutionalize a threat assessment step in all new business IT projects. Keep in mind that regulations are rarely a long-term friend to security. So protect the business first, and demonstrate compliance later.

### C1. Application Security Scenario

Application security is in a "perpetual arms race." Consider taking these steps to deal with it. For the near future (next 12 to 18 months): Develop mitigation processes on the assumption that content and software will be abused, stolen and attacked by outsiders and insiders; apply application security along the entire software life cycle. For the longer term (next five years): Build security into applications and/or buy software with it already built-in. Arrange SLAs with content and service providers. Demand security and IP certificates from OSS and vendors.

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

Although privacy is an immature function, organizations should consider implementing privacy programs with dedicated resources and budgets. To get started, define what privacy means for your business and set up a governance model mapping to your industry and specific needs. Implement privacy and security contract terms and conditions with all third parties. Work with IT and Info Security on a technology and vendor strategy that meets privacy program requirements around encryption, Web site/application privacy and DLP.

### A2. Articulating the Business Value of Information Security

Because InfoSec activities typically focus on reducing risk and preventing financial loss they could be regarded as insurance premiums. With that in mind, be careful about basing projects on ROI projections. It can result in unrealistic expectations. Instead, justify the investment by clearly identifying value propositions derived from expected benefits, such as enabling collaboration, regulatory compliance, competitive differentiation, risk mitigation, improved accountability and reduced liability.

### B3. Securing Virtualization, Virtualizing Society

Virtualization will transform how we secure and manage IT workloads during the next decade, dramatically reducing costs and increasing infrastructure's ability to adapt to changing business requirements. But don't let operations-led projects lower your security profile. Be sure to take advantage of virtualization TCO savings so that you can fund security efforts. Pressure your security vendors to provide tools that support virtualized environments — VMs, host OSs, hypervisors. And define your standards for secure VM and VMM configuration.

### D3. Why You Can't Count on Consumer Authentication

Criminals continue to compromise the credentials of your employees, contractors or customers by stealing them from systems and applications often outside your enterprise's control. Here's how to combat it. Use a layered security approach, and focus on end-to-end security to protect systems and data from intrusion and theft. Fraud detection and customer authentication must work across multiple channels, functions and other customer touch points, and that often means integrating multiple best-of-breed products. Priority should be given to analytics, alerts and case management, so that fraud analysts can effectively manage and stop fraudulent activities.

### A6. Doing More with Less

Focus on reducing inefficiencies and use those savings to address gaps. A long-term strategy that includes some near-term tactical steps can help you weather tough times and position you for later growth. If you must make cuts that result in reduced security service levels, be sure to take a stand on not reducing service below regulatory levels for regimes, such as PCI, HIPAA, FISMA, etc. Recovery is coming. So take advantage of today's budget turmoil and plant the seeds for future increases.



## Key Takeaways, continued

### **F7. Security Process Maturity Management**

Because process maturity is a well-understood discipline in many organizations, its metrics can provide a foundation to effectively communicate risk posture to an executive audience and help set priorities to close unacceptable risk gaps. The resulting benefits: easier budget justification, more visibility into the value delivered by risk management, and a bridge to business engagement in the acceptance of risk. Keep in mind that it should not replace formalized risk assessments.

### **B8. What You Need to Know About Cloud Computing and Security**

Many cloud-based offerings don't provide service-level commitments that are typically needed for critical business processes. How can you remedy the situation? Develop a strategy for safe use of externally provisioned services that allows you to do the following: Implement requirements and processes to assess the security, continuity, privacy and regulatory compliance risks. Identify appropriate use cases for different service delivery methods, based on risk level and corporate risk goals. Develop new contracting expertise. Choose and implement compensating controls before going operational.

### **A4. Integrating Physical and Information Security**

Fewer than 5% of large enterprises will converge their physical and logical security functions before 2012. However integration of the disciplines will increase, as demonstrated by projects in 70% of large enterprises by 2012. The principal drivers of integrated security are Common Access Cards, Video Surveillance, Business Continuity and Data Center Security.

### **C8. A million Lemmings Can't Be Wrong: Selecting New Authentication Methods**

**Immediate Steps:** Plan for the implementation of risk-appropriate authentication based on regulations, risk analysis and feasibility in multiple-use cases. **Near Term Actions:** Adopt a consistent methodology — such as Gartner Authentication Method Evaluation Scorecards (GAMES) — to evaluate the relative authentication strength, relative ease of use and absolute TCO of candidate methods. Choose an authentication vendor that can meet most of your needs with the simplest infrastructure. Invest in open, flexible authentication architectures to facilitate the current and future use of multiple methods.

### **D5. Security in Healthcare: How to Prepare for Inevitable HIPAA Enforcement**

Develop a breach notification process that aligns with new guidance. Refresh HIPAA security and privacy risk assessments to identify control gaps. Refresh HIPAA compliance documentation to support assertions of compliance. Review new requirements with your compliance officer and legal counsel to determine the impact on privacy and security policies, HIPAA training and business associate agreements. Watch for new guidance issued by HHS under the HITECH Act. Identify ePHI at risk for unauthorized disclosure, and implement encryption as a security control to avoid breach disclosure requirements.

### **E4. Protecting the Endpoint**

The expansion of endpoint protection — from traditional signature-based detection and personal firewalls to data protection and PC life cycle tools — is well under way. So be prepared to take these steps: Phase out point products for anti-virus (AV) and anti-spyware tools, host-based intrusion prevention systems (HIPSs) and personal firewalls and replace them with an EPP suite as support contracts expire. Recognize the declining effectiveness of signature-based malware detection. Evaluate non-signature-based techniques of EPP vendors. Consider your PCLCM and data protection strategy when looking for alternative EPP suites.

### **F8. Workshop Exercise: Security Program Maturity Assessment**

Don't reinvent the wheel — use these documented "good behaviors" to support your efforts. Learn from your operations and service management colleagues. Don't work in isolation, but rather understand integration and relationship points with other IT services and operations processes. Improve one level at a time. Implement an iterative, ongoing maturity process. Balance efforts across process groups. Use process performance metrics and be sure to have realistic objectives.

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

A security risk-aware culture can only be created and maintained when line-of-business managers take personal ownership of all risks, including IT risks. To drive this, the culture change program must position risk management as a mechanism for improving the profitability and productivity of the enterprise. Risk is owned by the revenue generators. By taking charge of it, business managers are able to remove inefficiencies in their own processes and organizational structures. Review your current awareness program: Does it have objective metrics? Are executives involved and participating?

## Audience Polling

Throughout the conference, electronic polling was used at key sessions to survey attendees on a variety of topics. Here's a sampling of results:



### K2. My Role in Information Security: Four Perspectives

- **How many of the following disciplines – risk management, business continuity, privacy and compliance – are part of your responsibility as a security officer:** 51% of attendees polled said that their responsibility extended to at least three to four of the following areas – ITRM, BCM, Compliance and Privacy. Only 12% said their responsibility was exclusively focused on security.
- **Which role best describes your responsibility:** 52% said CISO, 32% indicated security engineer, and 16% responded that the role that best describes their responsibility was CIO.

### B7. The Changing Face of NAC

- **The status of NAC in your organization:** 60% indicated they were in the planning stages; 30% said NAC was fully deployed, while 10% indicated that it was partially deployed.
- **The biggest obstacle to deploying NAC in your organization:** 50% attributed it to expense and budget issues; 30% said deployment obstacles were related to other issues; 20% connected it to political and operational concerns.
- **How has the economic downturn impacted NAC plans:** 80% of respondents felt no impact; 20% said that it resulted in 6 to 12 month delay; the remaining 10% have cancelled NAC plans for the foreseeable future.

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

- **What's the focus of your security risk awareness program:** 50% of attendees polled said skills and knowledge; 33% said culture and skills equality; and the remaining 17% indicated their program was lacking a focus.
- **How was the content of your awareness program developed:** 50% said by focusing on what seemed important; 33% said policy content; 17% responded that the same topics were used each year.
- **Is your organization ready to support true culture change:** 50% said they were unsure if support exists; 33% said yes; 17% no.

### E4. Protecting the Endpoint

- **Has your company been infected by malware in the last 12 months:** 73% responded yes; 27% no.
- **What next component from your incumbent Endpoint protection will you install:** 46% said data loss prevention; 27% full disk encryption; 9% HIP; 9% device control; 9% mobile data protection.
- **Will security and operational tools converge in your organization:** 56% responded that it would likely happen within the next 18 months; 36% said within the next 30 months; 9% said it already has.

### C5. Securing SharePoint

- **Is your organization officially deploying SharePoint:** 50% indicated there are widespread deployments; 38% said there were a few deployments; 12% said yes but that they were in testing phase.
- **Was information security involved in the planning and implementation of SharePoint?** 43% said yes, security was involved after deployments had started; 43% no; 14% yes, since the beginning.

### E2. Using Data Loss Prevention to Reduce Privacy Costs

- **Has your organization already deployed a DLP solution:** 67% responded no; 33% yes.
- **Is your current or planned DLP provider the same as your endpoint/desktop Anti-virus provider:** 80% said no; 20% yes.
- **How much have you spent or plan to spend on a DLP solution:** 80% indicated less than \$100,000; 20% between \$200,000 and \$400,000.
- **Is your current or planned deployment primarily for Compliance or Intellectual Property protection:** 80% said it was an even mix; 20% said intellectual property.
- **Is your DLP solution performing:** 100% responded yes



## TEN BEST-RATED SESSIONS

- Your Role in Information Security
- Keynote Panel: My Role in Information Security from Four Perspectives: Engineer, Auditor, CISO and CIO
- Keynote Panel: The CISO's Skill Set
- What Every Security Professional Needs to Know About Risk
- Staying Ahead of Next-generation Threats and Vulnerabilities
- Four New Network Security Technologies You Should Know About and Four Predictions
- The Inheritance: Challenges to the New Administration in Cyberspace
- Securing Virtualization: Virtualizing Security
- Gartner Keynote Panel: Worst Best Practices and Useless Useful Technologies Unmasked

## SNAPSHOT OF ATTENDEES

### Who participated in the 2009 conference?

More than 1,000 IT security professionals from across North America, Europe and Asia. Seventy percent were end-users representing more than 15 industries. The audience included:

- **Decision makers:** more than 40% were at the senior management level.
- **Cross-section of industries:** the top-5 highest-attending verticals were the government and public sector, services, manufacturing, financial services and health care.
- **Buying power:** 70% had an annual IT budget of more than \$6 million and higher.

## Thanks to our 2009 Summit Sponsors

Many thanks to our sponsors for helping make Gartner IT Security Information Summit 2009 an outstanding educational event for everyone involved.

### Premier



### Platinum



### Silver

Absolute Software	Cyber-Ark Software, Inc.	IronKey, Inc.	PGP Corporation	Symark International, Inc.
Alert Enterprise	Cyveillance, Inc.	Liquid Machines	Proofpoint, Inc.	Tenable Network Security
Archer Technologies	Damballa, Inc.	LogLogic, Inc.	Protegrity	Terremark
ArcSight	DeviceLock, Inc.	LogRhythm, Inc.	Purewire	Thales
AT&T	Direct Computer Resources	Lumension	RedSeal Systems	TippingPoint
BeCrypt	eIQnetworks, Inc.	Motorola	SailPoint	Trusted Computing
Beta Systems Software	Entrust	MX Logic	Secunia	Tufin Technologies
BeyondTrust Corporation	Finjan Inc.	NetIQ Corporation	SenSage, Inc.	Veracode
BigFix, Inc.	ForeScout Technologies	NitroSecurity, Inc.	Softtek, Inc.	Zix Corporation
Blue Coat Systems, Inc.	Guardium, Inc.	nuBridges, Inc.	Splunk Inc.	Zscaler
Brazil IT	Hirsch Electronics + SCM	Nuspire Networks	SunGard Availability Services	
Core Security Technologies	Microsystems	Ounce Labs		



Play. Stop. Rewind.

## Gartner Events On Demand.

[GartnerEventsOnDemand.com](http://GartnerEventsOnDemand.com)

## More than 90% of conference attendees said they would recommend the Summit to their colleagues

Special Note: All conference attendees have access to presentation slides which can be uploaded using their specially assigned documentation key on Agenda Builder (See conference website: [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity)) Those who have purchased the "Events on Demand" multimedia offering can review presentation slides and audio for the conference sessions. (For more information regarding "Events on Demand," e-mail the following – [eventsondemand@gartner.com](mailto:eventsondemand@gartner.com))

# Gartner® Security & Risk Management Summit 2010

It's exciting. It's new. It may even change how you approach the business.

Once in a while, a shift in perspective changes how you view your world. At Gartner, we're about to announce just such a change. It involves the new **Gartner Security & Risk Management Summit** and we're about to unveil all of the new and exciting features and sessions!

## Stay tuned...

What we unveil may mean you'll get a different perspective in how you approach and think about your business. And it will certainly lead to exciting progress in how you view security, risk management and business continuity.

The announcement is right around the corner and when the time is right, you'll be the first to know.

@ Watch your inbox for 'the big announcement'.

▶ Visit [gartner.com/us/itsecurity](http://gartner.com/us/itsecurity) for updates.

**Gartner**  
Security & Risk Management  
Summit 2010  
June 21 – 23, 2010  
Washington, DC (National Harbor, MD area)



Gaylord National Resort & Convention Center  
Same convenient location.  
Same excellent service.