



Security Forum 2008
Managing Security And Risk Amid Business And IT Change
 September 4–5, 2008 • Westin Boston Waterfront • Boston, Mass.

EVENT AGENDA

Event Track Themes — An Overview

TRACKS	
A	<p>Security & Risk Best Practices This track draws on real-world experiences and case studies to provide practical advice for security executives looking to expand their influence, improve security and risk management processes, and implement technology more effectively.</p>
B	<p>The Future Of Security & Risk Management This track looks at how security and risk management is changing and will provide a look forward at the emerging principles, practices, and technologies on the horizon that will affect security and risk.</p>
C	<p>Beyond Security This track explores the expanding scope and influence of IT security and will provide to Security & Risk professionals the insights necessary to establish close working relationships with stakeholders both across and beyond IT.</p>

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

THURSDAY, September 4, 2008			
TIME	SESSION INFORMATION	TRACK	SESSION TYPE
7:30–8:30 a.m. <i>Grand Ballroom Foyer</i>	Event Registration And Continental Breakfast In The Technology Showcase		
8:30–8:50 a.m. <i>Grand Ballroom A</i>	Welcome And Setting The Stage Jonathan Penn, <i>Vice President</i> , Forrester Research	All	Keynote
8:50–9:35 a.m. <i>Grand Ballroom A</i>	State Of Information Security In 2008 Khalid Kark, <i>Principal Analyst</i> , Forrester Research The security organization is finally starting to get the visibility that it had been asking for, but now it doesn't know how to deal with it. Many chief information security officers understand that they need to align themselves with the business and provide strategic advice, but they don't know how. The results from Forrester's Enterprise And SMB Security Survey, North America And Europe, Q3 2007 highlight some of these issues, challenges, and priorities for CISOs. This survey covers: <ul style="list-style-type: none"> • Top issues, challenges, and priorities for CISOs in 2008 • The changing responsibilities of the security organization • Progress businesses have made in aligning security with other parts of IT and the business 	All	Keynote
9:35–10:20 a.m. <i>Grand Ballroom A</i>	Network-Based Security For Global Infrastructure Dr. Edward G. Amoroso, <i>Senior Vice President and Chief Security Officer</i> , AT&T This presentation will show trends in carrier-based detection of global attacks in the context of AT&T's network management and security infrastructure. The session will illustrate with recent examples shifts in attack methods from worms to botnets and discuss and illustrate DDOS filtering and other virtualized security methods. Attendees at this session will learn: <ul style="list-style-type: none"> • How trends are shifting in network-based attacks • Why botnets pose such a significant threat to global infrastructure • How carriers can significantly reduce the risk "in the cloud" of network attacks 	All	Keynote
10:20–11:05 a.m. <i>Grand Ballroom B - E</i>	Morning Networking Break In The Technology Showcase	All	Networking

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

THURSDAY, September 4, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
9:30 a.m.–5:00 p.m. <i>Grand Ballroom Foyer</i>	One-On-One Meetings With Forrester Analysts Each attendee is able to schedule up to two 20-minute one-on-one sessions with the Forrester analysts of their choice, depending on availability. These meetings are consistently rated as one of the most popular features of Forrester Events.		
11:05–11:45 a.m. <i>Grand Ballroom A</i>	<p>Intelligence and Intelligent Action: From Threat to Countermeasures Michael Denning, <i>Vice President, Enterprise Security Services, VeriSign</i> Joe Pepin, <i>Senior Manager, MSS Intelligence Team, VeriSign</i></p> <p>Implementing policy and prioritizing resources for staying on top of and dealing with an ever-evolving and elusive threatscape is an important step in protecting the enterprise. So is implementation of a network security architecture in your environment. But what to do when the latest attack trends are internet-wide and the scope of your policy and security devices aren't? The key is deep intelligence as an input to be aligned and synchronized with your own preventive, detective, investigative, and reactive processes. The most effective security governance doesn't stop with policy or prioritization of resources; it includes appropriate monitoring and control mechanisms to help assure both policy compliance and policy effectiveness through a reliable feedback mechanism enabling strategic and operational nimbleness in handling shape-shifting attack models and technologies. The result is a model for operational excellence in integrating and aligning archetypal global threat and vulnerability intelligence with your concrete security and compliance architecture to maximize the real value of the intelligence to you.</p> <p>This presentation will include a discussion on the importance of a deep level of intelligence about threats, including the styles, inclinations, and motives of the actors and those that enable them. It will also cover best practice for rigorously aligning your assets, signature policy, vulnerabilities, threats, and intelligence with each other and with your organizational security policy and risk management goals. This session will focus specifically on:</p> <ul style="list-style-type: none"> • The persons, motives, and business models behind the present day attacker • The importance of leveraging a "follow the enabler" model • The lifecycle management of intelligence and threat detection and response 	All	Keynote

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

THURSDAY, September 4, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
11:45 a.m.–12:30 p.m. <i>Grand Ballroom A</i>	<p>Exploiting Online Games Gary McGraw, Ph.D., <i>Chief Technology Officer</i>, Cigital</p> <p>This talk, based on a book of the same title (co-authored by Greg Hoglund), will expose the inner workings of online game security for all to see, drawing illustrations from massively multiplayer online role-playing games (MMORPGs) such as <i>World of Warcraft</i> to discuss:</p> <ul style="list-style-type: none"> • Why online games are a harbinger of software security issues to come • How millions of gamers have created billion-dollar virtual economies • How game companies invade your privacy • Why some gamers cheat • Techniques for breaking online game security • How to build a bot to play a game for you • Methods for total conversion and advanced mods <p>Ultimately, this talk is about security problems associated with advanced, massively distributed software. With hundreds of thousands of interacting users, today's online games are a bellwether of modern software yet to come. The kinds of attack and defense techniques that this presentation will describe are tomorrow's security techniques on display today.</p>	All	Keynote
12:30–2:00 p.m. <i>Grand Ballroom B - E</i>	Lunch And Dessert In The Technology Showcase	All	Meal
2:00–2:45 p.m. <i>Commonwealth Ballroom A</i>	<p>Best Practices For IT GRC Programs Marc Othersen, <i>Senior Analyst</i>, Forrester Research</p> <p>Many IT organizations are struggling with establishing effective governance practices. Failing to properly link together IT governance, risk, and compliance (IT GRC) programs is a leading cause of ineffective or inefficient efforts. This session will explore real-world practices used by successful IT organizations to establish robust IT GRC programs. It will include:</p> <ul style="list-style-type: none"> • A case study of a successful IT GRC program • A life-cycle-based framework defining a comprehensive IT GRC program • A set of leading practices regarding the establishment, automation, and management of an IT GRC program • A clear explanation of an IT GRC market space including a description of top vendors 	A	Briefing

_____ *Making Leaders Successful Every Day* _____

THURSDAY, September 4, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
2:00–2:45 p.m. <i>Commonwealth Ballroom B</i>	<p>Digital Credentials In 2018: Touchstones Of Trust Geoffrey Turner, <i>Senior Analyst</i>, Forrester Research</p> <p>For close to a hundred years, your identity has been essentially federated in the physical realm through the use of state-issued driver’s licenses. But as more aspects of everyday life migrate to cyberspace, that ubiquitous default identity credential has as yet been unable to make the same leap, and identity theft and online fraud are rampant. But the precursors of universal — and much more effective — digital identity credentials are already starting to appear. Leveraging them in commercial processes can significantly reduce identity authentication costs in the not-too-distant future. This presentation will address:</p> <ul style="list-style-type: none"> • Digital credential initiatives: REAL ID, enhanced driver’s licenses, and e-Passports • The emerging technology infrastructures for digital identity • Prospects for government-to-citizen (G2C) digital credential integration into mainstream business-to-consumer (B2C) processes 	B	Briefing
2:00–2:45 p.m. <i>Commonwealth Ballroom C</i>	<p>Web 2.0: Balancing Chaos With Control Gil Yehuda, <i>Senior Analyst</i>, Forrester Research</p> <p>Chaos is not generally a state Security & Risk professionals strive to achieve. And yet, Web 2.0, the anarchistic revolution of user-generated content, is coming to your organization; in fact, it may already be flourishing, with or without your knowledge. In a world where employees easily acquire Web 2.0 tools and use them to generate and share information in the open, control can be difficult to achieve. The old-fashioned methods, using policy documents and user education might help, but new answers lie within the Web 2.0 tools themselves. This session will cover:</p> <ul style="list-style-type: none"> • How to use Web 2.0 techniques to regain control and security • When to intervene and block the use of Web 2.0 tools • Where organizations will require new policies and practices to bridge the gap between chaos and control 	C	Briefing
2:45–3:00 p.m.	Intermission		

THURSDAY, September 4, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
<p>3:00–3:30 p.m. Commonwealth Ballroom A</p>	<p>Guest Executive Forum With Blue Coat Systems Web Gateway Layered Defenses Against Malware — How Honey Grids Are Changing The Game Tom Clare, Sr. Director of Product Marketing – Secure Web Gateway, Blue Coat Systems</p> <p>Since mid-2007, Web attacks have quickly evolved into injections into trusted and popular Web sites using multiple background hosts to quietly download malware onto users’ systems. An estimated 79% of malware is downloaded from popular Web sites, and the attacks often use custom encryption wrappers and obfuscation techniques to evade detection in Web gateways, leaving the desktop to defend itself. The game has changed, and analyzing all Web traffic for threats inline is not sufficient. Hybrid gateways use cloud services with honey grids to provide new layered defenses against malware. This session includes:</p> <ul style="list-style-type: none"> • An authoritative review of changing Web gateway defenses for new attack techniques. • An explanation of how to layer defenses in a hybrid Web gateway using honey grids, inline detection, and Web content controls. 	<p>All</p>	<p>GEF</p>
<p>3:00–3:30 p.m. Commonwealth Ballroom B</p>	<p>Guest Executive Forum With Lumeta The Network Perimeter And Defense In Depth Michael Markulec, Chief Operating Officer, Lumeta</p> <p>With low-cost connectivity, mobility, virtualization, outsourcing IT infrastructure and more, the network perimeter’s line has been blurred. However, as companies adopt a layered approach to building security into the fabric of their networks, they shouldn’t completely remove focus from the perimeter.</p> <p>The most advanced organizations consider the concept of the true, ever-changing perimeter as an integral part of having a focused, accurate defense in depth approach.</p> <p>Organizations still struggle to protect secure zones, such as research labs and SCADA networks. In this session, attendees will learn how to validate secure zones, protect critical infrastructure, and define the network’s true perimeter.</p>	<p>All</p>	<p>GEF</p>

THURSDAY, September 4, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
<p>3:00–3:30 p.m. <i>Commonwealth Ballroom C</i></p>	<p>Guest Executive Forum With HP ProCurve Networking Exposing Network Security Myths And Secrets Mauricio Sanchez, <i>Chief Network Security Architect</i>, HP ProCurve Networking</p> <p>As networks have evolved into crucial enablers of business competitiveness, the dangers posed by new technologies and those using them have similarly evolved. Navigating the stormy realm of network security — and appropriately balancing security with access — becomes more challenging all the time. This session offers useful direction for establishing effective network security amidst a climate of change, dispelling myths and revealing important security secrets. Myth no. 1: Shrink-wrapped products and patches are sufficient to protect your network infrastructure. Secret no. 1: You can actually spend less to make your network more secure. This session will expose these and more, offering practical guidance for designing and implementing an adaptive network that delivers the utmost protection.</p>	<p>All</p>	<p>GEF</p>
<p>3:30–4:15 p.m. <i>Grand Ballroom B - E</i></p>	<p>Afternoon Networking Break In The Technology Showcase</p>	<p>All</p>	<p>Networking</p>
<p>4:15–5:00 p.m. <i>Commonwealth Ballroom A</i></p>	<p>Keys To Successful DLP Implementations Thomas Raschke, <i>Senior Analyst</i>, Forrester Research</p> <p>As more intellectual property and sensitive corporate data assets are being exposed and transmitted, data leak prevention (DLP) will increasingly be a “must-have.” Today, customers focus on closing the most obvious data holes, and vendors have begun to promote greater integration with security infrastructure; longer term, DLP technology holds the promise to extend into document classification and policy-driven information management. Data-savvy organizations will anticipate these changes. This presentation describes how DLP solutions fight the insider threat, what you must look for in market-leading offerings, how you can successfully implement DLP, and what steps you need to take today to prepare for the data security tasks of the future, focusing on the following questions:</p> <ul style="list-style-type: none"> • How, where, and why do you need to prevent sensitive data from leaking? • What are trends, challenges, and market-leading offerings in the DLP space? • Where do you start, and what nontechnology challenges will you encounter? 	<p>A</p>	<p>Briefing</p>

Event Agenda

All track themes and sessions are subject to change.

THURSDAY, September 4, 2008 (continued)			
TIME	SESSION INFORMATION	TRACK	SESSION TYPE
4:15–5:00 p.m. <i>Commonwealth Ballroom B</i>	<p>Protecting Information Assets In 2018: Taking A Data-Centric Approach: A Panel Discussion Jeff Bardin, <i>Director, Risk Management, Global Security Organization, Office of Risk Management</i>, EMC Corporation Tim Stanley, <i>Chief Information Security Officer</i>, Continental Airlines Steve Whitlock, <i>Chief Security Architect</i>, The Boeing Company, and <i>Vice Chair</i>, The Open Group Security Forum Moderated by: Jonathan Penn, <i>Vice President</i>, Forrester Research</p> <p>The frequency and impact of security breaches have highlighted the importance of data protection at the executive level. On the other hand, business priorities have forced organizations to open up their networks to business partners and third parties. We all know that infrastructure and network protection is not enough anymore. As the perimeter disappears and your data travels to places where you have no control over the infrastructure, you will need to have a data-centric security strategy in place to protect your information assets. The presentation will address:</p> <ul style="list-style-type: none"> • Essential process for data-centric security • Moving from infrastructure to applications • Moving from securing the data center to ensuring ubiquitous security 	B	Briefing
4:15–5:00 p.m. <i>Commonwealth Ballroom C</i>	<p>What CISOs Need To Know About Virtualization: A Panel Discussion Natalie Lambert, <i>Senior Analyst</i>, Forrester Research Kevin Yeamans, <i>Director of Enterprise Security</i>, Security Benefit</p> <p>This year, you have been hearing a lot from your IT operations team about virtualization. They consistently tell you that, in addition to saving money and reducing power consumption, virtualization will increase security. But is this true? This session will discuss the reality of virtualization in the enterprise and call out the key items that every chief information security officer should know. In addition, you will hear from other CISOs who are running virtualization in their organization about the hurdles they overcame to get it up and running. This session will focus on answering the following questions:</p> <ul style="list-style-type: none"> • What are the security benefits and risks of virtualization? • What key obstacles are CISOs facing as they move toward virtualization? • How are CISOs making virtualization part of their security strategy? 	C	Briefing
5:00–6:30 p.m. <i>Grand Ballroom B - E</i>	Evening Reception In The Technology Showcase		

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

FRIDAY, September 5, 2008			
TIME	SESSION INFORMATION	TRACK	SESSION TYPE
7:30–8:30 a.m. <i>Grand Ballroom Foyer</i>	Event Registration And Continental Breakfast In The Technology Showcase		
7:30–8:20 a.m. <i>Commonwealth Ballroom A</i>	Breakfast Presentation With Ounce Labs Open Secrets: Issues Of Data Privacy In PCI Jack Danahy, <i>Co-Founder and Chief Technology Officer</i> , Ounce Labs The PCI Data Security Standard has raised the bar for information security, amplifying the need to safeguard sensitive data and bringing into the vernacular the tension point between data privacy and data usability, including the ways in which all customer data is collected, shared, and used throughout the organization.		
8:30–8:45 a.m. <i>Grand Ballroom A</i>	Day Two Opening Remarks Jonathan Penn, <i>Vice President</i> , Forrester Research	All	Keynote
8:45–9:30 a.m. <i>Grand Ballroom A</i>	Planning Your Enterprise Security Strategy In The Internet World Chenxi Wang, Ph.D., <i>Principal Analyst</i> , Forrester Research As enterprises are becoming increasingly connected to the Internet and as hard organizational computing boundaries are fast disappearing, chief information security officers are facing fresh challenges in enterprise computing. Some of these challenges include responding to never-ending new threats, dealing with complex interaction models beyond the company's intranet, and struggling to keep proprietary information secure in a collaboration-centric culture. To enable success in this environment, which must accommodate business innovation as well as security challenges, CISOs have to navigate a complex and fast-changing technology and threat landscape. In this session, we will address these issues relating to an open and collaboration-oriented enterprise computing model. More specifically, we will cover: <ul style="list-style-type: none"> • Global trends on Web 2.0 adoption, deperimeterization, and the consumerization of corporate IT as well as how these trends affect enterprise security • The top security threats and what you can expect for tomorrow in this increasingly open and connected world • Critical steps to help CISOs develop a security strategy to deal with today's and tomorrow's security challenges 	All	Keynote

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

FRIDAY, September 5, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
9:30–10:15 a.m. <i>Grand Ballroom A</i>	<p>Making The Case For Security: A Panel Discussion Bruce E. Jones, <i>Global IT Security & Risk Manager, WWIS Global Functions, Eastman Kodak Company</i> John Petrie, <i>Chief Information Security Officer, Harland Clarke</i> Sara Santarelli, <i>Chief Information Security Officer, Network Security Services, Verizon Business</i></p> <p>Information security managers around the globe are frustrated as they struggle to make sense of the reams of data being churned out in today's enterprise environment. The real challenge for them is not only to identify what is important but also to be able to tie this information from disparate tools to business-centric metrics so that senior executives can understand the data, take action, and be confident that the enterprise is secure. This session will outline the approaches that successful CISOs have taken to articulate their case for security.</p> <ul style="list-style-type: none"> • Developing operational metrics for your security environment • Articulating the case to senior management and the board of directors • Gaining executive support for security initiatives and budget 	All	Keynote
9:30 a.m.–3:30 p.m. <i>Grand Ballroom Foyer</i>	<p>One-On-One Meetings With Forrester Analysts Each attendee is able to schedule up to two 20-minute one-on-one sessions with the Forrester analysts of their choice, depending on availability. These meetings are consistently rated as one of the most popular features of Forrester Events.</p>		
10:15–11:00 a.m. <i>Grand Ballroom B - E</i>	<p>Morning Networking Break In The Technology Showcase</p>	All	Networking
11:00–11:45 a.m. <i>Grand Ballroom A</i>	<p>Developing A Collaborative Security Strategy Brian Wrozek, <i>IT Security and Disaster Recovery Manager, Texas Instruments</i></p> <p>In many organizations, IT security operational duties are being distributed across the entire IT organization. IT security managers must build successful partnerships across IT boundaries and influence the right security behavior without having direct control over resources and budget. Responsibilities often overlap with other organizations such as HR, legal, audit services, and physical security. IT security managers need to foster win-win relationships with these groups and still find ways to collaborate with business units and external partners.</p> <ul style="list-style-type: none"> • Identify where IT security roles overlap with other groups • Brand IT security as a shared responsibility • Promote and support IT security projects in other groups • Build a business-results-oriented reputation • Be more than an electronic security cop 	All	Keynote

_____ *Making Leaders Successful Every Day* _____

FRIDAY, September 5, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
11:45 a.m.–12:45 p.m. <i>Grand Ballroom A</i>	<p>The Future Of Security: A Panel Discussion Daniel E. Geer, Jr., Sc.D, <i>Vice President and Chief Scientist, Verdasys</i> Herbert H. Thompson, Ph. D., <i>Chief Security Strategist, People Security</i></p> <p>Every year at our Security Forum, we’ve run the “Future of Security” panel to look at what threats, defenses, and environmental shifts are on the near and distant horizon of IT security. This year, we continue that tradition by welcoming back Dr. Geer and Dr. Thompson who will peer deep into the industry’s crystal ball and discuss what’s next — threats and countermeasures in 2013:</p> <ul style="list-style-type: none"> • How will the threat landscape evolve from now until then? • What will we be able to measure? Will it matter? • What does “maturity” look like in the security industry? <p>Following their presentations, both speakers will participate in a moderated panel discussion and jointly address questions from the audience.</p>	All	Keynote
12:45–2:00 p.m. <i>Grand Ballroom B - E</i>	<p>Lunch And Dessert In The Technology Showcase</p>	All	Meal
2:00–2:45 p.m. <i>Commonwealth Ballroom A</i>	<p>Best Practices: Implementing An Enterprise GRC Platform Chris McClean, <i>Analyst, Forrester Research</i></p> <p>Rolling out an enterprise governance, risk, and compliance platform continues to present substantial challenges. Besides the technical obstacles of implementation, earning organizational support from other departments, executives, and business managers is critical. This session will detail specific cases of successful GRC implementations and identify the common best practices for achieving success. It will cover:</p> <ul style="list-style-type: none"> • Common obstacles and pitfalls to understand and avoid during an enterprise GRC implementation • Common success factors critical to a successful enterprise rollout • A detailed look at case studies that demonstrate both obstacles and best practices, including lessons learned from each 	A	Briefing

Event Agenda

All track themes and sessions are subject to change.

FRIDAY, September 5, 2008 (continued)			
TIME	SESSION INFORMATION	TRACK	SESSION TYPE
2:00–2:45 p.m. <i>Commonwealth Ballroom B</i>	<p>CISOs In 2018: What Will It Take To Succeed In The Role? Khalid Kark, <i>Principal Analyst</i>, Forrester Research</p> <p>The security and risk management landscape has changed tremendously in the past 10 years. The chief information security officer role is transforming from one belonging to a techie deep within the IT organization to that of a business-driven executive whose responsibilities span across the whole organization. Many CISOs have also taken on additional responsibilities such as managing regulatory compliance and business continuity. The current CISO skill set and approach will be obsolete in the next 10 years. This presentation will identify the characteristics and perspectives of a successful CISO in 2018. The presentation will address:</p> <ul style="list-style-type: none"> • Characteristics to look for in your future CISO • The ever-changing role of security within the organization • How to equip yourself for the transition 	B	Briefing
2:00–2:45 p.m. <i>Commonwealth Ballroom C</i>	<p>Securing Information Services: The Next Generation Of Data Security Noel Yuhanna, <i>Principal Analyst</i>, Forrester Research</p> <p>Web 2.0 data feeds and other new use cases are driving security and information management pros toward new ways of securing integrated information in flight, rather than at the original source. Only by applying security policies at the point of access, in context, can the challenge of making information widely available be met in a secure way. This security imperative is only one of the drivers for the increased use of information services and other new SOA-based approaches to data integration, but for security pros it presents unique new challenges, coupled with the opportunity to transform the way information is secured in the enterprise. The business is demanding real-time access to reliable and high-quality information, which is seamlessly integrated with existing systems around the world and available 24x7 in the right place and time. This session will highlight best practices for implementing your own next-generation strategy for information security and explore how to meet the challenges of data protection in this new world of information-as-a-service, including:</p> <ul style="list-style-type: none"> • Managing centralized authentication and entitlement management • Developing and enforcing proper data and policy governance structures • Providing for appropriate delegation of control. 	C	Briefing
2:45–3:00 p.m.	Intermission		

_____ *Making Leaders Successful Every Day* _____

Event Agenda

All track themes and sessions are subject to change.

FRIDAY, September 5, 2008 (continued)			
TIME	SESSION INFORMATION	TRACK	SESSION TYPE
3:00–3:45 p.m. <i>Commonwealth Ballroom A</i>	<p>The Inside Story Of PCI: Confessions Of A QSA John Kindervag <i>Senior Analyst</i>, Forrester Research</p> <p>As a former Qualified Security Auditor (QSA), John Kindervag is uniquely positioned to help companies understand the seemingly Byzantine PCI security requirements. This session will provide the audience with an insiders view of PCI and help provide a framework for simplifying compliance. Specifically, this session will provide:</p> <ul style="list-style-type: none"> • Details as to what the PCI auditor is looking for • A way to rethink PCI to positively impact security • Understandable and actionable steps to become PCI compliant 	A	Briefing
3:00–3:45 p.m. <i>Commonwealth Ballroom B</i>	<p>Identity And Access Management In 2018: The Three Centers Of Gravity Andras Cser, <i>Senior Analyst</i>, Forrester Research</p> <p>As the current tools and processes mature, identity and access management (IAM) technologies and processes will consolidate into three centers of gravity: access management technologies, user account provisioning, and identity federation. There will be other IAM functions — such as entitlement management, outsourced identity management, trusted broker networks, and adaptive authorization — that will need to integrate into the above gravity centers. To equip themselves for the future, organizations will need to understand these three gravity centers and their relationships with external tools and technologies. The presentation will address:</p> <ul style="list-style-type: none"> • Preparing your organization to select technologies that will be viable tomorrow • Leaping beyond security and compliance and showing the business value of identity management to the executive team • Evolving the ownership and selection process of identity and access management solutions in organizations 	B	Briefing

_____ *Making Leaders Successful Every Day* _____

FRIDAY, September 5, 2008 (continued)

TIME	SESSION INFORMATION	TRACK	SESSION TYPE
<p>3:00–3:45 p.m. <i>Commonwealth Ballroom C</i></p>	<p>Bridging Business Continuity And Disaster Recovery Stephanie Balaouras, <i>Principal Analyst</i>, Forrester Research</p> <p>Firms often see business continuity (BC) planning as a one-time or annual event rather than an ongoing program or process integrated with corporate functions such as IT operations and risk management. Too many BC plans are simply disaster recovery plans, and enterprises typically do not have well-developed BC programs that enforce standards, consistency, and quality across a distributed organization. To address these challenges, leading enterprises are taking a more formal approach to BC strategy and planning, creating central BC program offices and adopting tools to help manage the program. This session will cover:</p> <ul style="list-style-type: none"> • The distinction and relationship between business continuity and disaster recovery • Best practices in ongoing business continuity management • How to develop a centralized BC program that coordinates with enterprise architecture, IT operations, and security and enterprise risk management functions 	<p>C</p>	<p>Briefing</p>
<p>3:45 p.m.</p>	<p>Event Ends</p>		