

Pulse2011

Meet the people who can optimise your infrastructure

IBM Pulse - July 27th & 28th, 2011 Security, Risk Management & Compliance Sessions

Session 1: IBM Directions in Security, Risk Management and Compliance

Ravi Srinivasan, Program Director, IBM Security Product Management

The more interconnected, intelligent and instrumented your business, the more security threats you have the potential to face. Enterprises who are committed to innovation know they are adding risk. The challenge is managing that risk holistically, consistently and proactively across the enterprise, including its employees and supply chain. We'll jump-start the security dialog at Pulse with a discussion on how security projects can support enterprise initiatives to innovate, address dynamic regulatory and compliance challenges, accelerate returns on investments to counter shrinking IT budgets, and secure the enterprise against a barrage of new and evolving sophisticated threats and risks.

Ravi manages the IBM Tivoli security and compliance portfolio product management based in Austin, Texas. He has over 15 years of experience in market strategy, product management and development in software and services industries. In this client facing role, Ravi meets and consults with senior management, lines of business owners and IT operations management around the world on their key security, risk, and compliance initiatives. He's also a frequent speaker at trade, analyst conferences and customer events to share a worldwide perspective and insight into addressing compliance, data and application security needs. Prior to joining IBM in 2006, Ravi held several senior marketing and product management roles at Synopsys and Texas Instruments Inc.

Session 2: The Converging of Identity, Access and Threat Management

Dr Paul Ashley, PhD, CISSP, Engineering Manager for IBM Internet Security Systems Solutions, IBM Gold Coast Security Laboratory

The presentation outlines the fundamental change occurring in the threat management area. Traditionally threat management focussed on firewalls, identifying and blocking intrusions and malware prevention. Although these protections are still valid today, there is now a new focus on the threat posed by applications. Organisations have lost control of which applications are being used within their network, how much bandwidth is being consumed and currently have very little control of application use. Additionally applications are the major cause of data leakage in the organization. The presentation will focus on this new area of threat management, that is, application and user control. The presentation will outline some of the key technical challenges and show how the convergence of identity and access management with threat management is a key to solving these new problems.

Dr Ashley has seventeen years of experience in information security working in identity and access management, SOA security, web services security and now in threat management. He has written a book titled *Practical Intranet Security*, authored two editions of the IBM redbook titled *Understanding SOA Security Design and Implementation* and has written numerous technical papers. He is a regular speaker at industry and academic conferences. He has six patents granted in the area of information security and received awards at IBM for patent filing and authorship.

Special Interest: Meet the Security Developers

Get up close with the people who develop IBM's security solutions. This Birds of a Feather special meeting will allow you to link up directly with engineers from our Gold Coast IBM Development Labs, home of our world-class product development, support and services experts. Ask the hard technical questions, lobby for valuable product features, and get the inside story from our patent holders and engineers.

Wednesday July 27, 1pm - 1.30pm

Location: M11



Pulse2011

Meet the people who can optimise your infrastructure

Session 3: Policies, Passwords and Proofing: High Security In the Online Transaction Age

Mike Cartwright, CTO, Pirean

In the beginning there was simply the logon - username and password and maybe, possibly, multi-factor. Today online businesses have evolved their needs to more sophisticated and controlled user access, using multi-factor, self-service, versatile authentication, risk scoring, attestation and even anti-phishing and post-session processing. Attend this session to hear how Pirean have addressed these requirements for secure business systems that link with partners, customers, suppliers and agencies. Hear about their experience managing the user lifecycle across the spectrum: from simple username and password to protect a portal, to smartphone apps and multi-factor authentication for banking, to the integration of Secret Questions / SMS passcodes for workers accessing secure systems from remote mines and oil rigs. With 10+ years of experience, you won't want to miss their lessons learned from the front line.

Session 4: Safely Driving A Successful Identity and Access Environment

Paul Di Matteo, Caltex Australia

As the world evolves to cloud computing, governance requirements increase and the hacker communities evolve, Identity and Access Management becomes a control that is required to be effective and efficient. Caltex Australia is Australia's leading transport fuel supplier and convenience retailer and the only integrated oil refining and marketing company listed on the Australian Securities Exchange. Caltex's commitment to operational excellence includes the protection of information and access to systems across its Retail, Engineering and Corporate businesses. Hear about what they achieved in this challenging environment and how they delivered a solution for Identity and Access Management, delivering better value to shareholders through the Information Security teams ability to streamline business processes for staff and customers.

Paul Di Matteo has worked in Information Risk Management for over 10 years. Paul's experience has focused on robust processes that deliver Information Security controls and frameworks. Having worked with Identity and Access Management solutions for large Australia and International corporate, Paul brings a sound understanding of common challenges faced in today's environments of increased compliance and governance.



Pulse2011

Meet the people who can optimise your infrastructure

Session 5: Enterprise Single Sign-on at Telstra Global Operations Centre

Herman Recinos, Telstra and Robert Trotter, IBM Software Group Services

The Telstra Global Operations Centre (GOC) manages Telstra's entire network infrastructure across Australia. Routers, Switches, Cables, Power, PSTN, Fibre, Base Stations and more. With over 200 applications for operators to authenticate against – it would take some of the 500 staff over 20 minutes just to log in at the start of a shift. Telstra with the assistance of IBM Software Group Services deployed TAM ESSO (Tivoli Access Manager for Enterprise Single Sign-On) 8.1. We developed over 80 application profiles covering a huge range of platforms (such as custom in-house applications, Commercial Windows Apps, Java, Web, Command Line). Learn about the successes and challenges of the project, tips about fostering user buy-in and support, and profiling examples of the flexibility of TAM ESSO.



Session 6 (Track 6): Cleaning your TAM WebSEAL with AJAX and other Web 2.0 Challenges

David Siviour Systems Designer, CenITex

Join the technical expert from CenITex to hear about their experience in implementing Tivoli Access Manager for eBusiness. This will be a deep dive technical session that will show how their TAM for eBusiness and WebSEAL architecture work together to deliver a secure environment across their intranets and extranets. David will cover:

- Briefing on what TAMeB and WebSEAL are.
- What is the role of a reverse proxy.
- How WebSEAL is used in a multi-tier environment.

Web 2.0, AJAX and WebSEAL

- How does Web 2.0 and AJAX give WebSEAL heartburn.
- What solutions does WebSEAL have that allow it to act as an antacid.
- Problems that each solution does not cover.

Case Study of the implementation of a Kronos application

- What were the issues.
- What solutions we tried.
- What was the final solution.
- How the final solution was implemented.
- How has this changed the way we handle these issues now.

David Siviour has been working as a Systems Designer with Tivoli Access Manager for eBusiness for over seven years, firstly with the Department of Human Services and then with CenITex.



Pulse2011

Meet the people who can optimise your infrastructure

Session 6 (Track 1): Cloud Computing: Getting the benefits while navigating the security challenges

Neil Readshaw, CISSP, Cloud Security Lead Architect, IBM GTS Architecture & Technical Solution Design Security and Compliance Specialty Service Area

Cloud computing offers enormous potential for the efficient delivery and consumption of IT resources. Appropriate security, privacy and compliance capabilities are paramount before the benefits of cloud computing can be realised. In this session, learn about the security, privacy and compliance challenges with cloud computing; how they are similar to and differ from those of traditional IT; and how IBM Security solutions are being built into cloud infrastructure, and being used to integrate cloud and on-premise IT.

Neil Readshaw is a Cloud Security Lead Architect within IBM Global Technology Services. Neil is responsible for driving secure, compliant solutions for IBM's Cloud offerings. Neil also works with customers to provide solution architecture and drive their security requirements into future Cloud offerings. Neil was previously a Chief Programmer and Security Architect in Tivoli.

Session 7: Tivoli Security Information and Event Management

Peter Stevenson, IBM Advanced Technology Group Security, Worldwide SWAT Team

This session will focus on proven practices, design principals and key considerations common amongst successful business with GRC solutions. Businesses are realizing great value in developing a comprehensive compliance and risk management program across a variety of risk domains, including operational risk, financial controls management, IT risk, compliance and internal audit. The result is an aggregated, enterprise-wide picture of all risk exposure, helping CFOs and CIOs understand how risk can impact the organization's future performance. We will examine several success stories and provide deeper insight into how organizations can employ an integrated set of products to automate the process of identifying, measuring and monitoring all the different areas in an organization that risks will impact.

Pete has over twenty-five years of experience in information technology, ten years in network security, and six years in the Audit and Compliance space. Pete works extensively with many of the world's largest companies to help address their Security, Risk and Compliance challenges. Pete currently manages IBM's Advanced Technology Group (ATG) Security SWAT team and is responsible for deploying expert resources worldwide to support customers with immediate needs. Prior to that he led the Tivoli Security and Compliance technical sales team supporting North America and he is an expert in IBM's audit, compliance, and privileged user monitoring solution, Tivoli Security Information and Event Management (TSIEM). Pete joined IBM with the acquisition of Consul Risk Management in February 2007 and he also founded and ran his own security company for ten years before it was acquired by Consul in 2004.

Session 8: Threat Management and Perimeter protection ... don't let the bad guys in!

Chris Polkinghorne, Melbourne IT, and Chee Nung Wong, Senior Technical Consultant, IBM Tivoli ANZ

How do you protect a network of 490,000 kids – who use countless applications, receive millions of e-mails, update Facebook constantly and might be potential targets for spammers and predators? Given the task of protecting the network of one of Australia's largest government education bodies, systems integrator Melbourne IT decided that protocol analysis via ISS Proventia appliances was the right strategy. Come to this session to hear about the factors that sealed their decision, and some of the fascinating things they learned during the implementation. In addition we'll look at the risks in your VMWare architecture and why assuming you have adequate protection may be a mistake. Hear how IBM solutions can protect every layer of the VM and not let the bad guys in, whoever they are!

Chris Polkinghorne is the security technical lead for Melbourne IT, responsible for oversight of all security operations and incident management. Chris promotes security concepts and requirements across all technology streams, introducing security solutions into the company. Prior to his role at Melbourne IT, Chris has managed security in the defence intelligence and banking industries.



Pulse2011

Meet the people who can optimise your infrastructure

Special Interest Roundtable: Your Security Exposed - Will your organisation be next in the headlines?

Tommy Viljoen, Security Practice Leader, and Greg Janky, Partner, Risk Services, Deloitte.

Join this special briefing for an up-close-and-personal roundtable with the risk and security experts from Deloitte. Based on their extensive client experience, hear about their views on the Australian security landscape compared to International markets and learn about the industry issues and how they are being viewed from the boardroom to everyday technology users. The roundtable will consider their recommendations to address organisational needs for architecting, managing and sustaining complete end to end security. A must for any organisation reviewing their end-to-end security program in a constantly demanding era of risk. Places will be limited.

Thurs July 28, 12.30pm - 1pm

Location: M11

Session 9: Smarter IAM - The Education Challenge

Mark Johnston, Solution Architect, Qld DET – Identity and Access Management Program, IBM Security Solutions

The Queensland Department of Education and Training (DET) has embarked on a 100 million dollar smarter classrooms initiative to provide, integrated information services to schools and training institutes to improve outcomes for both students and staff. The new initiative will help shift traditional pen and paper methods into the digital-age, allowing teachers and parents to better track a child's progress through a suite of integrated, secure, online applications. The key to ensuring the success of such a vast program is the successful alignment of Identity and Access Management (IAM) standards across the entire organisation. 700,000 users, 300,000 desktops, 15 Active Directory Forests and 10 enterprise applications in the initial scope present many hurdles on the path to an integrated solution for an entire state.

Hear how IBM leveraged skills from across different IBM business lines and IBM business partners develop a solution that met the unique challenges presented by an organisation the size and complexity of QLD DET.

Session 10: Hot topics for Application and Data Security

Steven Schmidt, CISSP, CISA, A/NZ Technical Sales Specialist, IBM Security Solutions and
Steven Gibson, Senior Consultant, Data Security and Compliance, IBM Information Management Australia

A data breach can cost an organisation millions of dollars not to mention damage to their reputation, customer loyalty, loss of revenue and the possibility of fines or other penalties. Two key strategies for making sure your business applications are protected: (a) build the application with security in mind and test it before it goes into production and (b) then monitor and track who has access to sensitive information. Attend this quick-hitting session to understand two 'Best in need' technologies for avoiding data exposures and ensuring compliance: Rational AppScan and The InfoSphere Guardium and Optim solutions.

