Track 5: Security, Risk Management & Compliance abstracts

Session 1: IBM Security Track Kickoff
Steve Robinson, VP Development, Strategy and Product Management, IBM Security Systems Division
Denis Kennelly, VP Security Development, IBM Ireland

Join us for this insightful stream keynote as we discuss how the boundaries of todays business infrastructures are being extended and sometimes obliterated by the emergence of cloud, mobility, social business, big data and more. During this session, IBM executives will address key security and compliance challenges, demonstrating how IBMs security intelligence solutions can become the enabler of a business without limits. From infrastructure security and threat mitigation to managing compliance and audit, this session will explore the latest research and methods on how address new security challenges.

Steve Robinson is the Vice President of Development, Strategy, and Product Management for the IBM Security Systems Division. He is responsible for a broad portfolio of commercial security solutions that help IBM clients with identity and access management, database activity monitoring, secure application development, network and endpoint security, and analytics that provide integration and intelligence to the security platform. Steve manages over 1000 technical professionals, 14 world wide Security software development labs, and IBM's X-Force security research team. He is a member of the Integration and Values Team (I&VT), a group of 300 senior leaders helping to steer the entire IBM business, as well as IBM's Cybersecurity Advisory Council which helps guide IBM's internal security policies and practices.
Steve has held many executive positions in sales, technical services, product management, and acquisition integration in IBM's Software Group. Steve joined IBM in 1984 as a programmer, was involved in many of the company's early projects around object oriented programming, and was instrumental in bringing both Smalltalk and Java to IBM. He was an early driver of IBM's distributed application development strategy as the Product Manager of IBM's VisualAge family, and introduced and launched technical services into IBM's Software Group. Most recently he was the GM of IBM Security Solutions, the precursor to the new division, and was responsible for formulating IBM's overall security product strategy. Steve earned his undergraduate degree from Wake Forest University and his MBA from Duke University.

Denis Kennelly is VP of Development for the Security Software team at IBM. Prior to Denis' recent appointment to the Security Software role, he was VP of Development and CTO for the IBM-Tivoli Network Management Product Portfolio. Denis has 20+ years experience in both the Telecommunications and IT industries. During this time, Denis has helped define and develop both network and service management products in a number of different industry segments. Denis joined IBM through the acquisition of Vallent Technologies which specialized in Cellular Network Service Assurance software and was acquired by IBM in February 2007. Before joining Vallent technologies, Denis helped define and lead the development of management products for Storage Networks, Cellular Networks, Transmission Networks and Servers for major companies such as EMC Computer Systems, Motorola and Digital Equipment Corporation. Denis has a master's with distinction in computer science from Trinity College Dublin, Ireland and a first class honours bachelor of engineering for electronics from University of Limerick, Ireland.

Session 2: Security Intelligence
Jeff Paddock, Senior Tech Director, Q1 Labs

Join Jeff Paddock, Senior Director, Worldwide Systems Engineering for Q1 Labs, for an insightful session as he discusses how the boundaries of today's business infrastructures are being extended and sometimes obliterated by the emergence of cloud, mobility, social business, big data and more. During this session, we will address key security and compliance challenges, demonstrating how IBM's security intelligence solutions can become the enabler of a business without limits. From infrastructure security and threat mitigation to managing compliance and audit, this session will explore the latest research and methods on how address new security challenges.

> Jeff Paddock leads the worldwide Q1 Labs technical sellers within IBM. Prior to joining Q1 Labs, Mr. Paddock worked for Application Security, Inc., Symantec, including Axent Technologies and Raptor Systems, Compuware's Ecosystems Division, Prime Computer and the US Air Force. He has held various positions in engineering, technical and marketing management in each of these companies.
> Mr. Paddock's experiences cover a wide range of areas from Account Management, Director of Systems Engineering to Director of Development for a UNIX administration tool. He has over 35 years experience in Business, Security, Networking, Databases and client-server technologies. Mr. Paddock holds a BS in Computer Science from the University of Maryland.

Session 3: Securing the Future Technology Revolution
Tor Jomar Nordhagen , Snr Exec leader, Security Consulting Practice, Accenture Australia

Technology is more important than ever to achieving business success. The world is on the verge of a new technology revolution, one that is present in every aspect of our lives. The lines between consumer and corporate technology continue to blur. On-premise and off-premise technology are melding to drive much quicker processing—and faster and better business results. The flexibility of new technologies and architectures is forcing us all to rethink how we harness IT to make it easier for our organizations to innovate. And security will underpin everything. In this session, Accenture will outline the six key technology trends from its 2012 Technology Vision that will be at the heart of the future of technology, and the risk and security implications arising from these trends.

> Tor Jomar Nordhagen has worked for Accenture since 1993. Tor has worked with clients across EMEA, USA and APAC, with a focus on managing profitability, risk and compliance, using technology as an enabler for High Performance delivery. His experience covers Financial Services, Telecommunications, Government and Retail industries, fulfilling roles such as CxO stand-in, advisory functions, and Delivery Architect / Project Management roles.

Session 4: Successful Identity and Access Management Case Studies
Lachlan McGill, ME Bank
Naomi Rafael, BioGrid

How are enterprises leveraging Identity and Access Management (IAM) in 2012 to support business-driven initiatives? What projects generate ROI the quickest, or get the fastest end user or executive buy-in? How does Identity and Access Management, and in particular IBM solutions, help address compliance initiatives? What are some benefits one can expect to see from an IAM deployment? Join this session for answers to these questions and more as you engage in an interactive discussion with a panel of security leaders from a variety of industries.

> Lachlan McGill is the Information Security Manager at ME Bank in Melbourne, Australia. He has had over 20 years experience in the IT industry including the last 10 years in information security. Lachlan has had experience at several organisations worldwide in a number of various roles related to architecture, design, identity management and security governance. His recent achievements include development of a Role Based Access Control framework and overseeing the design and implementation of identity & access management at ME Bank.

BioGrid Australia provides a multi-faceted technical platform for collaborative translational health research, preserving patient confidentiality and collegiate intellectual property. The numbers of data collections and users continue to grow. BioGrid has an established online Access Request System covering applicant agreement to terms and conditions, data custodian and ethics approval. But to remain scalable and secure, BioGrid needed to institute a reliable user provisioning system. This presentation describes BioGrid's experience deploying TIM in its environment: the challenges, insights and benefits.

Naomi Rafael is the Technology and Systems Manager of BioGrid Australia. She has a Bachelor of Science, Graduate Diploma in Computing and is currently studying Masters of Information Technology at the University of Melbourne. She began her IT career in 1988 working for various government and commercial organisations. Naomi joined BioGrid Australia in October, 2004. Her role encompasses management in the areas of security, system architecture, database, data integration, software engineering, metadata management, hardware specification and other technological areas utilised by BioGrid.

Session 5: Driving Effective Application Security in the Enterprise: An End-to-End Approach to Addressing One of the Biggest Threats to a Business
Steven Schmidt, CISSP, CISA, Security Specialist, IBM ANZ

The dynamic nature of Web applications creates new challenges for security and compliance. The widespread growth of Web applications and the business value they deliver attracts hackers and cyber criminals to target Web-based applications to steal data, disrupt operations, and infect clients. Most enterprises try to address Web application security by either 1) Finding and fixing the vulnerabilities; or 2) Blocking attacks against those vulnerabilities. However, best practices combine the two approaches to identify and correct vulnerabilities in the software development life cycle, while still protecting production applications with security measures specific to their vulnerabilities.

Steven Schmidt is a Technical Specialist on the IBM Security Systems team. Steven has been specializing in web application security since 2001 while leading the security assessment team for a large US bank. Steven joined IBM in 2007 as part of the Watchfire acquisition. Steven provides technical support for the AppScan portfolio, training for AppScan customers, security consulting within the software development lifecycle and web application vulnerability assessments.

Session 6: IBM Mobile Security Solutions: Empowering Innovation by Delivering Confidence
Vijay Dheap, Product Manager - IBM Master Inventor, IBM Mobile Security Solutions, IBM USA

We now live in a smarter mobile world. Not only are mobile devices becoming pervasive but people are increasingly embracing smartphones and tablets. With these powerful devices they are not only performing personal or entertainment tasks but also conducting business. This is increasing productivity, responsiveness and innovativeness of the organizations they work for. However, these devices can significantly increase the attack surface of an enterprise causing significant concern for enterprise security teams. Mobile Security needs to be approached holistically based an organization's operational priorities and can encompass mobile user security, mobile device/data security and mobile app security. As an organization evolves into a mobile enterprise it will require mobile security intelligence to gain visibility of its mobile security posture and be proactive in addressing the dynamic needs of mobile initiatives.

Vijay Dheap currently leads Mobile Security Solutions for IBM. He started off his career as a researcher in the field of Pervasive Computing, and then evolved his technical expertise as a developer on IBM's mobile portal product. He transitioned to an analyst role gaining experience formulating IBM's technical and business strategy for emerging technologies such as Web 2.0, Big Data and Mobile as a member of IBM's Emerging Technologies Team. He joined IBM's newly formed Security Division as a Product/Solution Manager. He has significant international experience having led several customer engagements on four continents. Vijay earned his Master's in Computer Engineering from University of Waterloo, Canada and his International MBA from Duke Fuqua School of Business.

Session 7: Title: A Next Generation Intrusion Prevention System and X-Force Threat and Risk Report
Dr. Paul Ashley, IBM Gold Coast Security Development Laboratory
Peter Param, St Vincents and Mater Health

Gartner proposes that a Next Generation Network Intrusion Prevention System (IPS) is differentiated from the current models of Network IPS because they are becoming "context aware". Context awareness means having additional information available to enhance the security capabilities of the device. This is primarily associated with knowledge of application and users. This means an enterprise should have visibility to which applications are running within their IT environment, visibility to which users are using those applications and be able to enforce a security policy that limits application access. An important point stressed by Gartner is that these additional capabilities should be available in the normal in-line model of a Network IPS resulting in no change to the deployment architecture and no reduction in IPS capability.

The first part of this presentation will outline IBM's implementation of a Next Generation Network IPS and some of the key development challenges. The second part of the presentation will cover practical experiences in deploying the Next Generation IPS in a live enterprise environment. It will discuss the deployment architecture, how users and applications were identified, and practical challenges experienced.

> 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.

Session 8: Applying Intelligence in the IAM portfolio
Chris Hockings, IBM Development Labs, IBM Gold Coast

This presentation focuses on the IBM Security Framework People (Identity and Access Management) portfolio. It will outline recent portfolio capabilities delivered to customers, as well as highlight strategic portfolio investment areas for 2012. With the IBM Security Systems division focused on Security Intelligence and integration, this session will provide local customer use cases driving People portfolio evolution, and in part, answer the question of what Intelligence means in the context of People and Identity. Presented by Chris Hockings, one of the technologists within the IBM Security Systems Australia Development Lab, attendees will get a glimpse into identity and access management integration scenarios being pioneered locally within the development labs, and outline how customers can get involved.

> Christopher Hockings is an Open Group Distinguished IT Specialist and is manager of the Lab Services team within the Australia Development Lab Gold Coast location. He is a member of the IBM Advanced Technology Group, as part of the world-wide Security SWAT mission. His area of expertise is in delivering customer focussed innovation around the Identity Management and Compliance solutions. Chris is a tenured member of the Technical Experts Council of A/NZ and is a keen and active inventor, with 2 issued patents and a further 11 under consideration with the US Patent Office.

Track 4, Session 9: Server and Network Protection - A Line of Defence
Chee-Nung Wong, Snr Sec Specialist, IBM ANZ
Jayson Walmsley , Mgr Info Sec, Bendigo and Adelaide Bank

Track 5, Session 9: A new approach to preventing attacks on your critical data
Andrew Muecke - Information Technology Security Advisor, South Australian Government's Department of Planning, Transport and Infrastructure.

Andrew will take you through the challenges faced by the Department in applying ISO Security Standards to the SA Registration & Licencing System, and the reasons for their choice of IBM Guardium Database Security. In addition, Andrew will also discuss the implementation process undertaken by the Department, and key lessons learned during their journey to a standards compliant, secure data infrastructure.

> Andrew Muecke has more than 20 years experience within the ICT industry, covering both private and public enterprise. With a focus on the 'business usage' of IT rather than its technical application, Andrew has extensive experience as a business analyst, project manager, contract manager and account manager. Andrew lists his

specialty area as 'communication' and is currently the Information Technology Security Advisor (ITSA) for the South Australian Government's Department of Planning, Transport and Infrastructure.

Track 4, Session 10: IBM Security Products and Services secure the IBM Enterprise
David Merrill, Strategist, IBM Chief Information Security Office, IBM USA

Learn how IBM, as an enterprise, is using it's own security products and services to reduce it's risk and leverage it's own portfolio to improve security internally. As a large global enterprise, IBM faces the same risks and challenges as it's customers. It also partners closely with it's products and services divisions to improve it's own security and provides linkage with it's own security strategy.

David Merrill is the strategist for endpoint security and malware protection in the IBM's Chief Information Security Office while also advising dozens of IBM's Fortune 500 clients. Previously, David served as IBM's Global Security Operations Manager where he directed the daily operation of IBM's worldwide internal IT security. David is a popular speaker and industry-recognized expert in the areas of endpoint, mobile, and cyber security.
Bloomberg News, eWeek, Network World, Baseline, CIO Insight, SiliconAngle, Forbes, and Institute of Advanced Security have all recently interviewed David. He was a keynote speaker at the Juniper Networks Mobile Security press launch and is a frequent presenter at Tivoli Pulse and SANS. The 2011 and 2012 X-Force Annual Trend and Risk Report features his mobile security insights along with sharing his thoughts and insights as a regular contributor to the Institute of Advanced Security. A multiple patent holder, David is also the inventor and architect of the IBM Threat Mitigation Service (ITMS), the automated malware response system in use within IBM today.

Track 5, Session 10: Social Mobile Security
Shane Weeden, Product Architect, IBM Security Systems

In this session, we show you how your development teams can construct a personalized dashboard/"social front end" to securely access all your enterprise applications -- spanning desktop, mobile using simplified security architectures. Come learn how to bridge the latest advances in security standards for mobile with existing legacy investments and IT systems leveraging traditional technologies like LTPA or SAML. This session will demonstrate how to use Tivoli Federated Identity Manager to lower the barrier of entry to application developers. This session will also show you how to seamlessly integrate third-party content and integration with SaaS capabilities.

Shane Weeden is the product architect for IBM Tivoli Federated Identity Manager. He has worked in IT security since 1992, and since 2000 has been working with Tivoli Security products including Tivoli Access Manager for eBusiness and Tivoli Federated Identity Manager. Shane now divides his time between customer focused engagements and core product development activities. He holds a Bachelor of Information Technology from the University of Queensland in Australia.