Gartner
IT Security Summit 2008

Information Security: Explore – Strategise – Envision – Implement

19 September, Swissotel Merchant Court, Singapore

CONFERENCE CHAIRS

Eric Ouellet
Research VP

Andrew Walls
Research Director

Register Today!
gartner.com/ap/itss

Gartner
IT Security
Summit 2008

Introduction from the Conference Chairs

More than ever, a proactive IT security strategy is vital to success. As new generations of technology-savvy users and a growing wave of gadget-prone communication services are making their way into the workplace, they bring with them new security threats as well as new technical and management paradigms. All of this rapid change has the potential to create considerable chaos in security operations and the security marketplace.

Security remains a top concern for every C-level executive and security managers at all levels – for good reason. The proliferation of wireless devices, e-enabled applications, and advanced global systems for both employees and collaborative efforts with business partners and customers puts your data in the hands of more people in more places than ever before.

Security is most effective when it is integrated with core business processes. With thousands of security products and services on the market you need to know where to make strategic investments, how to govern security, and how to optimize process for the greatest efficiency.

We've created an Agenda that covers the security landscape, including emerging threats, the demands of compliance, planning for the unexpected and for new security infrastructures, and developing new processes to conquer these challenges.

The Gartner IT Security Summit 2008 will help you take advantage of emerging opportunities. Our Gartner Analysts will present a detailed vision of the future of IT security and show you how to strategically plan and tactically implement a successful security program.

We urge you to attend this important event, where you will forge strong connections with high-level professionals like yourself, view upcoming technologies and delve into your own critical issues in one-on-one sessions with our Analysts and security technology solution providers.

We look forward to seeing you in Sydney this September.

Eric Ouellet
Research VP

Andrew Walls
Research Director

Get answers to your most pressing challenges

- How do I optimise my security spending in a time of budget constraints?
- Are we keeping pace with new developments?
- What threats are we not protecting against?
- What new threats will occur?

Find out how key trends will impact your IT security strategy

- Creating and managing the right security strategies for a changing threat landscape
- Information security architectures and data protection: the right content and structure
- Risk management for information security practitioners
- The process-oriented activity cycle for security and risk management
- Effective processes and technologies for identity and access management, vulnerability and threat management, risk and control assessment, communications and relationship management
- Regulatory compliance and corporate governance
- Achieving maturity in business continuity management and disaster recovery
- Building security metrics that actually mean something
- Latest analyses of information security markets and vendors
- Managing the security impact of social network services

Two Tracks

Information Security: Explore – Strategise – Envision – Implement

As the business demands measurable results and threats expand exponentially, security managers have to anticipate and plan effective solutions for tomorrow. Through hundreds of client interactions and feedback, we've identified the key elements for you to develop an effective security control program.

Track A

Managing Security, Compliance and Risk

Compliance and risk management are not about technology. However, the fact is this: IT systems support the way an organisation lives and breathes. So how can you help business units within your organisation understand and manage IT-related risks and achieve compliance confidently? By systematically addressing IT risks across the enterprise and improving critical business and security management processes. Such a proactive approach enables top-line growth while still maintaining necessary levels of control in the complex areas of governance, regulations, risks, performance, sourcing, security, access control and vendor selection. This track focuses on the tools, strategies and tactics characteristic of a coordinated program for addressing regulatory, commercial and organisational risk effectively.

Track B

Secure Business Enablement

Innovative business models challenge security teams to envision new and more effective approaches to security in rapidly changing environments. Once you build it, it must be secure. Legacy access control technologies, fragmented user administration processes and directories, spoofable e-mail, and single-platform security administration products are all typical examples of business 'disabling' approaches that are no longer sufficient. You need techniques and tools that are business enablers. These sessions focus on best practices in defining and managing identity and access management, secure messaging, and supporting enhanced mobility.

Benefits of attending

- New breakthrough research
- New cutting-edge recommendations
- New best practices
- Understand emerging trends and your best defenses
- Sharpen the way you communicate security to the business
- Drive down the cost of compliance while harvesting the benefits

Who should attend?

Anyone involved in enterprise-wide security and critical infrastructure protection including:

- CIO / CTO / CISO
- VPs, Heads, Directors, Managers of: security, risk, compliance, identity, access, fraud, e-commerce, privacy, governance, facilities, audit, data protection, disaster recovery

The Gartner difference

- Leading provider of events for IT professionals
- Highly discerning research that is objective, defensible and credible
- The largest and most informed team of research analysts
- Independent, not vendor driven
- Balance between strategic and practical

Meet the Gartner Analysts

Worldwide expertise at your fingertips

For over 25 years, Gartner analysts have been the trusted advisors to many of the world's largest and most demanding companies. No one sees the implications of technology so clearly, so consistently.

Gartner analysts draw constantly from the real-life challenges and solutions experienced by more than 45,000 Gartner clients worldwide. The value of this resource, combined with our deep analysis of technology vendors, is unrivalled.

Eric Ouellet,
Research VP, Canada
Focus areas: Encryption and rights management, wireless security, smartcards, identity and access management, security certification, business continuity

Earl Perkins,
Research VP, US
Focus areas: Identity and access management, enterprise application, web services, service-oriented architecture (SOA), and software as a service (SaaS) security and identity issues; and secure development life cycles

Tom Scholtz,
Research VP, UK
Focus areas: Security management and operations, security architectures, budget and spending, secure outsourcing

Andrew Walls,
Research Director, Australia
Focus areas: APAC security markets and issues, security management, governance and compliance, policy, risk management

Agenda at a glance

DAY 1 Friday 19 September	
08:00	Registration
08:30	Morning Sessions
09:30	Opening Keynote
12:10	Lunch
12:55	Afternoon Sessions
16:45	Closing Keynote
17:30	Conference Close

Plenary Session

Opening Keynote

Myths, Misconceptions and Paranoia's Breaking Down the Barriers to Effective Security Management

As organisations embark on a security management program they run into many real and perceived obstacles that distract them from focusing on business priorities. Organisations who are not disciplined in effectively addressing myths, misconceptions and paranoia's will continue to fail and lower the value of their security programs. In our opening keynote session, Gartner's leading security analysts will show you how to break down these barriers in order to Explore, Strategise, Envision, and Implement more effectively.

Closing Keynote

Magic Quadrant Powerhouse Session

Meet the Gartner analysts at their best - adhoc on stage. Get the latest information on the IT Security tools and markets to help you explore, strategise, envision, implement. Ask questions about vendors or tools. Hear the Gartner position on the technology providers relevant to your immediate requirements – unscripted, unfiltered, unbiased.

Track A

Managing Security, Compliance and Risk

Emerging IT Governance Risk and Compliance Technologies

Tom Scholtz

IT Governance, Risk and Compliance Management (GRCM) is a set of capabilities that can improve an IT organisation's external audit posture, reduce compliance reporting costs, and improve an organisation's ability to effectively address IT risks. Technology selection and deployment advice is provided for this emerging market.

- How can IT GRCM technology reduce compliance costs and improve an organisation's ability to assess risk?
- Who are the major IT GRCM technology providers?
- How can organisations effectively deploy IT GRCM technologies?

Managing Security Information and Emerging Vulnerabilities

Eric Ouellet

Organisations need to implement new ways to find and fix security weaknesses as threats evolve and new delivery methods are adopted. The technologies and new IT delivery methods that will be needed to manage security information and eliminate vulnerabilities will be evaluated in this session.

- What are the essential components of an effective emerging vulnerability management program?
- What new technologies and services should organisations employ to manage new vulnerabilities and security information?
- What policies, procedures and rules are appropriate for an agile application organisation?

The Impact of ITIL V3 on Governance, Risk and Compliance Strategies

Tom Scholtz

The new release of ITIL takes a life-cycle view of service management, as opposed to the functional approach of previous versions. It emphasises the engineering of risk and security components into the 'service platform warranty' for business and IT services. While this is a major improvement in approach, it does have major practical implications on IT security, risk and compliance strategies.

- What is new about ITIL V3?
- How will these changes impact SRC strategies (for the better and for the worse)?
- What can you do to prepare for and leverage ITIL V3?

New-Age E-Discovery for Security Practitioners

Andrew Walls

If you thought e-discovery of internal Electronically Stored Information (ESI) was bad, just wait. The problems posed by e-discovery are worsening as litigators and regulators focus on the digital persona of e-discovery custodians well beyond the firewalls of their organisations. This means that personal e-mail accounts as well as social networking sites and virtual reality may become the targets of litigators and regulators. If it can be established there is a relation to their work that may be information relevant and a cause for action.

- What is the e-discovery mandate organisations must address?
- How are organisations deploying resources to address the e-discovery mandate?
- Why is the e-discovery mandate evolving and growing in complexity and what does this mean for information security?

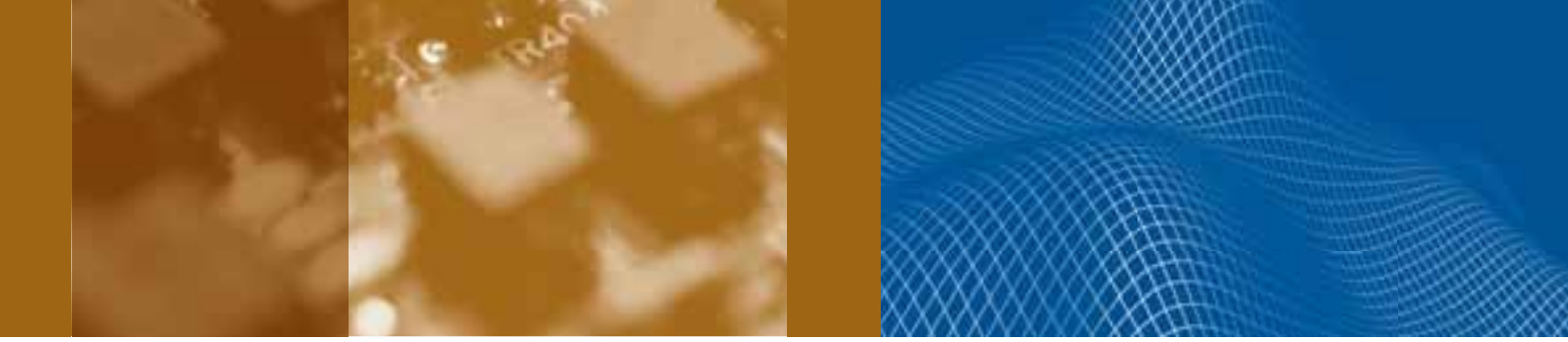
Tailored Security on a Budget: 'Off the Rack' Security Is so 2008

Tom Scholtz

Today's security-conscious enterprise is compelled to buy many different, often overlapping, security functions in the form of hardware, software, and services. It is challenging to navigate the muddle of vendor marketing, solution packaging, and industry FUD to decide how best to derive value from capital and operational expenditures while maintaining adequate security. In ten years, the budget-and security-conscious enterprise will have the ability to build a dynamic services-based security architecture comprising 'push' and 'pull' services, paid from a master security debit account.

- How do enterprises overreact to the latest attacks?
- How can security budgets be impacted by large, panic-driven capital projects?
- What new delivery modes for information security will raise the security baseline?

Agenda subject to change



Track B
Secure Business Enablement

Identity at Your Service(s): The Rise of Service-Based Identity and Access Management

Earl Perkins

Will there ever be a day when customers can 'buy' Identity and Access Management (IAM) services, rather than installing products within their enterprise? Is that day already here? Are the IAM products themselves built as service-oriented architecture (SOA) based solutions to make such implementations easier, whether implemented in-house or by service providers?

- How viable is service-based IAM? What form will it take?
- What are the key questions customers must ask before using service-based IAM?
- What is the current state of service-based IAM architecture?

Real Security for Virtual Spaces

Andrew Walls

Virtual worlds, social network applications and real world mapping environments are merging and integrating to form complex, geographically distributed social and business interaction environments. As corporations move into these dynamic environments to access new markets and to enhance customer interaction and staff collaboration, new security risks are created for the organisation and for the individuals that work within the virtual environments. The assurance of security within these new and rapidly changing environments requires a well coordinated and fluid approach to risk management with strong support and participation by business stakeholders.

- Why does security in virtual spaces require skills and knowledge in physical, personnel and IT security operations?
- How can staff be prepared for potentially offensive interactions within virtual environments?
- How will vendor support for security in virtual worlds vary and be influenced by local legal issues?

Getting to the Problem of the Root: Best Practices for Managing Superuser Privileges and Shared Account Passwords

Earl Perkins

Organisations are under increasing pressure to reduce the number of users having permanent full superuser privileges, and to implement better control over, and greater accountability for, use of shared accounts with similar privileges.

- How can you most efficiently and effectively contain use of full superuser privileges?
- How can you manage individuals' use of shared privileged accounts in a controlled and auditable manner?
- What are the best practices for dealing with embedded application-to-application passwords?

The Next 10 Years in Secure Messaging

Eric Ouellet

New forms of spam are emerging. Requirements for monitoring outbound email are increasing. Sender reputation is becoming an important issue. IM, consumer web mail and web 2.0 are redefining the scope of messaging, and what it takes to secure it.

- How should organisations prevent the introduction of malware through messaging vectors?
- What policies and procedures are relevant to monitoring employee email?
- What are the most effective methods of implementing proper levels of messaging hygiene?

The Lessons Learned: Buying, Deploying and Managing IAM Systems

Earl Perkins

What does the ideal RFP or tender contain for IAM systems? What kind of questions should be asked before buying a system? Are there best practices for deploying user provisioning? Once a system is installed, what organisational structure is best suited for ensuring the best use of the system can be realised? These and other questions will be explored in a survey of customer experiences.

- What goes into an ideal RFI, RFP or tender for IAM?
- What are key best practices in IAM program implementation?
- How do you manage an installed IAM system effectively?

Agenda subject to change

Hotel Accommodation

Swissôtel Merchant Court
20 Merchant Road, Singapore 058281

Distance by taxi: Changi International Airport – 30 minutes

We recommend delegates book their accommodation early as high occupancy is expected during this time. Please ensure you indicate: **Gartner – IT Security Conference (19 Sep 08) on your booking.**

Contact:

Stephanie Busse
Group Coordinator

Phone: **+65 6239 1775**

Fax: **+65 6336 9993**

Email: **stefanie.busse@swissotel.com**

Pricing Options

Single Registration	Prices
Early Bird – Save SG$300! (Register & Pay by 5pm Friday 15 August 2008)	**SG$1150.00** (plus taxes)
Standard Single	**SG$1450.00** (plus taxes)

Register Online Now!

Web
gartner.com/ap/itss

Enquire Now!

Phone **+65 6377 4476**
Email **gartner_itsecurity@circusmax.com**

Platinum Sponsors

as at 16 June 2008

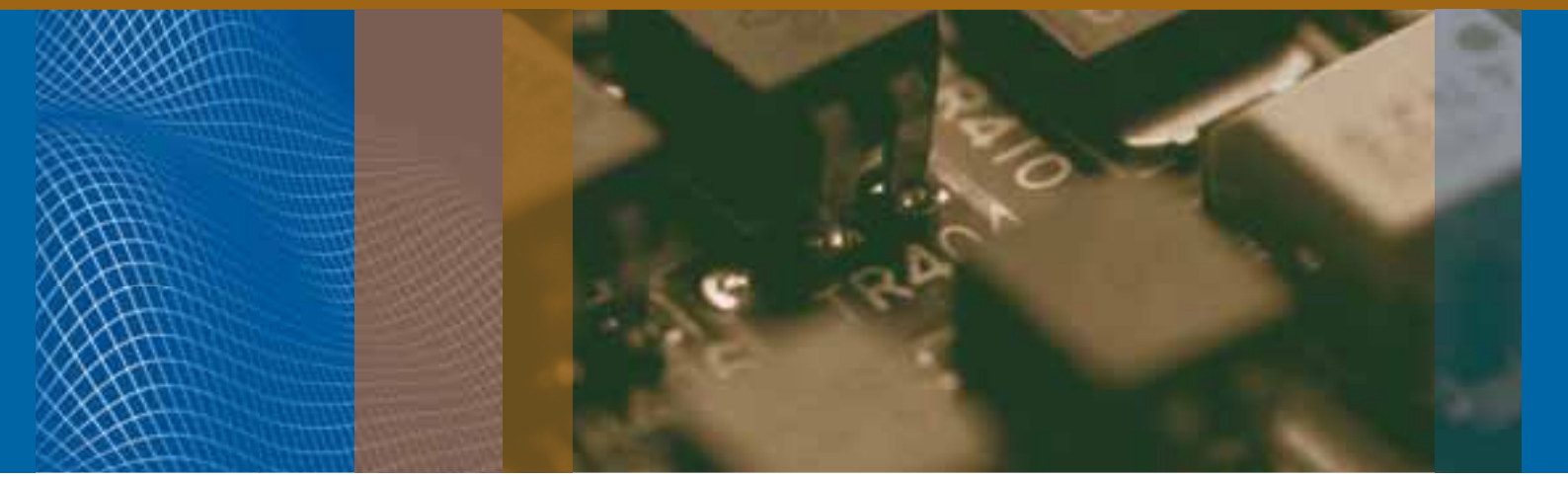
NOKIA

Silver Sponsors

as at 16 June 2008

Novell®

TATA COMMUNICATIONS
TAKING YOU FARTHER™



Upcoming Gartner events, great solutions…

Service Orientated Architecture Summit	Tokyo, Japan	15-16 July
IT Governance Forum	Tokyo, Japan	3-4 September
Enterprise Architecture Foundation Seminar	Canberra, Australia	10-11 September
IT Security Summit	Singapore	19 September
	Sydney, Australia	23-24 September
Symposium/ITxpo	Tokyo, Japan	27-29 October
Symposium/ITxpo	Sydney, Australia	11-14 November
China Outsourcing Summit	Chengdu, China	18-20 November

For more information about Gartner's events, please visit **gartner.com/ap/events**

Media Sponsor

as at 16 June 2008

THE WALL STREET JOURNAL.