Gartner Summits

Gartner **Security & Risk Management** Summit 2012

16 – 17 July 2012 | Sydney, Australia

gartner.com/ap/security

TRIP REPORT

Strategic Roadmaps to Secure the Enterprise and Manage Risk

INTRODUCTION

The **Gartner Security & Risk Management Summit 2012** was held 16 – 17 July, at the Sydney Convention & Exhibition Centre, Australia. The Summit drew attendees from a wide range of industries and organizations. This report provides highlights from the two-day event.

OVERVIEW

At the Gartner re-launch of the Security & Risk Management Summit, attendees sought out ways to: structure and manage each individual IT security and risk program; balance and coordinate those programs, make them more efficient and effective; select approaches and vendor solutions; learn to articulate security and risk requirements in business language; integrate business continuity management with overall risk and security program; and much more.

This year's summit attendees participated in on-site benefits, hearing the latest IT security, risk management and compliance, identity and access management, and business continuity management presentations from the Gartner Research community on today's most pressing topics, attending workshops and To The Point sessions run by expert analysts and industry leaders, hearing real-life experiences during peer case studies, engaging in analyst-user roundtables and one-on-one meetings with Gartner analysts, and checking out the latest solutions at Solution Showcase.

KEY FINDINGS

Here are key recommendations from this year's Gartner analyst sessions — especially useful for your 2013 planning and strategy considerations.

KEYNOTES

Opening Keynote: Strategy into Action — Road Maps to Secure the Enterprise

In this well-attended opening keynote, Gartner analysts, Rob McMillan, Paul Proctor and Andrew Walls discussed how enterprise success depends on security and risk management, making it necessary for security leaders to define multiyear strategic road maps and simultaneously drive tactical operations that respond effectively and efficiently to changing business needs and rapidly evolving threats. Each analyst then explored what it means to translate strategy into action through a strategic road map that drives business success. The keynote provided attendees with trends and insights that will allow them to meet future challenges and enhance the success of their role, team and organization.

Rob McMillan
Research Director

Paul Proctor
VP Distinguished Analyst

Andrew Walls
Vice President

Gartner Closing Keynote: Security Enabling the Business Is Not a Fairytale — Risk-Adjusted Value Management

In this closing keynote, Paul Proctor highlighted the approach needed for outlining the value within security and risk programs. His hard hitting messages and advice is captured in the following: Security and IT risk management enabling the business is not a fairy tale; You, your program, and the organization's perception of you are huge inhibitors; You are your own worst enemy; Do not perpetuate the outdated dogma of a traditional IT security function; Define desired business outcomes and supporting business processes; Establish the causal links between risks and desired outcomes; Ask yourself what decisions your data supports above the line and Put all communication in a business context.

Paul Proctor
VP Distinguished Analyst

GUEST SPEAKER PRESENTATIONS

Mock Court International — You be the Judge® — Guilty of Failing to Protect Confidential Information?

Set in a court room format, the jury (represented by the audience) watched and listened to the cross examination by lawyers to a case alleging that National Credit failed to ensure the protection of customer confidential information, to wit, names, address, contact and bank account details and alleged customer loan default details. As a result of that public disclosure and the negligence of the defendant, the plaintiffs have suffered damages. A total of $22,000,000 in damages is sought by the plaintiffs (class action) which includes financial loss and reputational damages (to businesses and individuals involved). Through a series of witness accounts, the judge delivered the verdict of Guilty and stated that "the evidence of this case leads to the conclusion that the underlying causes that gave rise to the inadvertent release of confidential information lay higher up in the organization. From top to bottom the organization was infected with the disease of complacency and gross inattention to the detail of a practical IT security risk management system.

Anthony Morris
Director, Mock Court International

Bruce Whitehead
Director, Mock Court International

Ignore Culture at Your Own Risk — The Four Stages of Culture Adaptation

In his keynote, Michael Henderson, The Corporate Anthropologist, outlined why organizational culture when misaligned with the business strategy should be regarded as a significant risk. Michael highlighted that culture is highly influential when it comes to business outcomes. Culture can be thought of as a group mind set, mind share or mind shift. When anyone one of these categories or combinations of a culture are misaligned with the strategy, the group mind set wins!

Michael noted that risk as a concept is in fact a cultural perception. What is considered risky in one culture can quite literally be considered entertainment in another. Michael also suggested that organizations that fail to pay deliberate attention to their culture are often at risk of finding their culture has in fact become their number one competitor.

Michael Henderson
The Corporate Anthropologist

END-USER CASE STUDIES

ING Direct Australia: Identity Governance Don't Just Do It!

Removing unauthorised access to data was the driver for financial institution, ING Direct Australia, to implement an identity and access management control system in 2011. Prior to the implementation of SailPoint IdentityIQ, the bank had too many users with unverified access to core banking systems. This problem needed to be solved to comply with the Australian Prudential Regulatory Authority (APRA) regulations covering access rights. According to Sestanovic, ING Direct Australia learnt nine lessons from the identity and access management implementation:

- **The importance of upfront analysis** — enterprises should not jump into "just do it mode" with IT projects but take time with the implementation.
- **Secure project sponsorship** — Senior executive sponsorship was critical as identity governance offering often spans many business areas that need to commit to identity and access management (IAM).
- **Engage business users** — Get buy-in from the top and drive the program top down. Select champions from the business to work with you on testing the functionality and enhancements of the system.
- **Establish a governance committee, working group** — share and leverage work to accelerate enterprise level deployment. Use a small team for delivery. The technical delivery works best if dedicated and centralised.
- **Secure commitment of subject matter experts** — These experts should include application support, technical infrastructure, information security and risk managers because systems such as IAM affect the whole business.
- **Employ a technical project manager** — This technical project manager should have a deep knowledge of governance, risk management and compliance as well as understand the company's environment and be able to guide the implementation team through company standards and policies.
- **Engage audit and compliance** — Engage an auditor to work with the company as early as possible and be a joint stakeholder in the program.
- **Stick to your guns** — IT staff needed to hold true to the scope and the problem they were trying to resolve. Stay focused and work through the challenges, the benefits will come.

Anthony Sestanovic
Head of IT Performance, ING Direct

Source: **ING Direct Australia removing identity management risks**
Hamish Barwick, CIO, 16 July 2012

Boral: Next Generation Firewalls — The Experience at Boral

An outbreak of malware on its network in 2009 forced Australian construction materials supplier, Boral, to ditch its 20-year-old firewall system and install a next generation firewall. The traditional port firewalls were no longer effective and could not deal with Web based threats and applications lurking in social networking sites or Google Apps.

Boral saw the number of exploits targeting Adobe Flash and HTML/Jscript rising with the release of the Blackhole kit which is used by hackers. If you are not patched for Java or Adobe exploits, you might get a malware infection. This was exactly what happened when a Boral company PC--which was not fully patched and had Java/Adobe vulnerabilities-- visited a website containing exploits. It was subsequently compromised and the company had to deal with a malware infection in 2009. After going to market in 2010, the company selected a next generation firewall system which would perform deep inspection of Web traffic and blocking of attacks such as SQL scripting. Since the implementation, the company has been able to block viruses, spyware and exploits, control non-work related Web surfing and prevent potential threats associated with high risk apps. According to Chaudhuri, Boral can also identify users regardless of internet protocol (IP) addresses. In addition, employees can browse the Web at normal speeds while the security system is scanning for threats.

The introduction of the next gen firewall meant Boral consolidated its security controls and saved $120,000 per annum in licensing and maintenance of uniform resource located (URL) filtering. Boral has also minimised data loss prevention and improved employee productivity by allowing access to specific applications.

Sonali Chaudhuri
IT Security and Risk Manager, Boral

Source: **Boral hammers security threats with next gen firewall**
Hamish Barwick, CIO, 17 July 2012

SELECTED SESSIONS

To the Point: Quo Vadis CISO? Developing a Realistic Information Security Management Strategy

Your strategy needs to be crystal clear on three elements:

- Where we are?
- Where we are going?
- How we will get there?
- Be methodical and use an evidence-based approach.
- Set expectations about what is achievable and what is NOT achievable (at least this time…)

Tom Scholtz
VP Distinguished Analyst

To the Point: Optimizing the Information Security Organization — Using a Client-Focused Approach

Monday Morning

- Assess the current state of your security and risk management organizational structure — map skills to activities.
- Ensure that current roles and responsibilities are defined and communicated.

Your Next 90 Days

- Develop a service catalog as a precursor to defining a service delivery model.
- Explore how your organization supports the goals and objectives of the business.

Your Next 12 Months

- Evaluate your current organization structure and develop a plan to address gaps.
- Develop a plan to improve information security governance and its place in corporate governance.

Jeffrey Wheatman
Research Director

Bits, Bytes and Balanced Scorecards — Creating Security Metrics That Matter

- Focus on matching your metrics to the solution of business problems, not technology problems.
- Implement a tiered architecture for metrics mapping the content and context to the audience.
- Make sure metrics have ALL five characteristics and are flexible.
- Create some SLA-based metrics.
- Leverage additional reporting tools:
  - Balanced scorecard
  - Risk adjusted value management
  - Four I Model
  - Risk register
  - Process maturity assessment.

Jeffrey Wheatman
Research Director

Security and Risk Governance — It's Much More Than Just Reporting

- Formalize a common definition of security and risk governance in your organization.
- Define and implement an information security and risk governance function that is integrated with the organization's corporate and IT governance functions.
- Focus on the governance processes and functions, rather than on the organizational position of the activities.

Tom Scholtz
VP Distinguished Analyst

To the Point: Articulating the Business Value of Information Security

- Establish the foundations:
  - Listen to the business; understand the context
  - Implement relevant governance structures and communication channels
  - Establish a feedback loop.
- Communicate the business value of the program:
  - Articulate the benefits in business terms
  - Map the business drivers to actions and expected value.
- Justify project investment in business terms:
  - Use balanced price/performance analysis
  - Report back.

Tom Scholtz
VP Distinguished Analyst

Why Your Security Awareness Program Is Doomed (and What You Can Do to Rescue It)

Action Plan for CISO's

Monday Morning

- Review your current program for objectives and behavioral outcomes.
- Identify security objectives that depend on staff behavior.

Next 90 Days

- Define two to three behavioral outcomes for this year's focus.
- Develop new media capabilities: tools and skills.
- Test market media and messages.
- Measure behaviors related to the defined behavioral outcomes.

Next 12 Months

- Innovate message content and delivery mechanisms, frequent change is good.
- Explore new social models for support of behavioral outcomes.

Andrew Walls
Vice President

Developing an Effective Identity and Access Management Program

Recommendations

- Establish an IAM program with a vision and strategy that closely aligns with and tracks business imperatives.
- Seek business value beyond traditional efficiency and effectiveness benefits — but focus on what is most appropriate to your organization.
- Embrace the challenges and opportunities of the nexus of forces and mature your IAM program to maximize value to the business.

Earl Perkins
Research VP

Improving Your Social Risk IQ

- Evaluate strategic business objectives for related social issues.
- Include the effect of social amplification when assessing risks to business objectives.
- Ensure that CSR programs are built on a solid foundation of compliance and risk management, as well as employee, business partner and customer engagement.
- Improve your social risk IQ:
  - Include social risk assessments in strategic planning
  - Establish a weather bureau to track, shape and respond to social risks
  - Proactively manage enterprise reputation
  - Apply social media strategies to tune social amplification.

French Caldwell
VP & Gartner Fellow

Can I Recover Through the Cloud? Managing IT Resilience

Action Plan

- Evaluate and pilot the use of recovery-as-a-service:
  - Qualify system image replication and failover support
  - Consider: virtual only? VMware only? What about bare metal recovery? What about IBM, HP and Solaris platforms?
  - Assess which CSFs are most important to you as well as how candidate providers stack up.
- Assess alternative providers
  - Determine scope of self-service support
  - Obtain credible documentation of provider operations controls
  - Measure actual versus committed recovery times
  - Gain a complete understanding of potential service benefits as well as the level of management support that the in-house IT team will need to provide.

Tom Scholtz
VP Distinguished Analyst

To the Point: Lawyers, Users and IT Security — Ten Ways to Limit Risk and Improve Governance

Action Plan for CISO

Monday Morning

- Identify the state of your information governance program.
- Assess the level of involvement of information security in IG.

Next 90 Days

- Develop a road map for classification and architectural integration into IG.
- Create a data security awareness campaign.

Next 12 Months

- Implement a strategy for long-term integration of security and IG.
- Define a set of critical success factors and measures for security integration.

Jeffrey Wheatman
Research Director

To the Point: Six Risk Techniques to Please Your Board

- CISOs should adopt the six risk management techniques to improve enterprise risk intelligence and risk reporting to the board.
- When communicating directly with the board, focus on:
  - What enterprise objectives and strategies matter most?
  - What's the potential impact of IT risk on those things?
  - What are the current and proposed approaches to managing these risks?
  - What are the next steps?

French Caldwell
VP & Gartner Fellow

That Socrates Was Wrong — A Debate on Human Nature and Its Relevance to Security

Action Plan for CISOs and Risk Officers

Monday Morning

- Review your security awareness training — have you done it?
- Review your policy framework — is it a litany of rules that no one understands, or does it have usable, understandable guidance?

Next 90 Days

- Survey your users — do they know or care about the value of security?
- Survey your users — do they know what to do but lack the tools?

Next 12 Months

- Refresh your security strategy to provide the tools, policies and awareness programs that your users need.
- Develop a marketing program to educate the organization about the importance of security.

Rob McMillan, Earl Perkins, Tom Scholtz, Andrew Walls, John Girard

Seven Keys to Successful and Cost-Effective Risk Oversight

- Review your company's current risk oversight practices to determine the overall level of maturity and alignment with public disclosures.
- Cultivate a greater understanding and awareness of risk through increased dialogue and an emphasis on the strategic priority of risk oversight.
- Weave risk oversight practices into the fabric of the business, while adopting a balanced and practical approach to risk management.
- Streamline risk oversight practices by clearly defining accountabilities, and by utilizing technology as an enabler of more effective risk management.

French Caldwell
VP & Gartner Fellow

To the Point: The Realities of Cyber insurance Top 10 Considerations When Purchasing Cyberinsurance

- Buying in to the sales pitch.
- Your insurance broker.
- Policy complexity.
- Policy qualification.
- The pre-insurance survey.
- Filing claims.
- Selecting coverage.
- Understanding exclusions.
- The cloud.
- Payment of claims.

Paul Proctor
VP Distinguished Analyst

Teleworking Through a Disaster — Case Studies of Disaster Recovery and Business Continuity

- Don't expect telework to help in every disaster; sometimes employees just need to survive.
- Practice telework as a business process, not as an occasional drill.
- Offer relevant training for managers and their staff.
- Make certain that all employees know how to use remote access, even if they are not full-time teleworkers.
- Ensure that your remote portals provide up-to-date links to the resources employees need.

John Girard
VP Distinguished Analyst

Monitoring Users for Security Intelligence — Threats and Opportunities

- Establish effective governance first.
- Involve legal counsel and HR in formation of guidelines.
- Announce monitoring/surveillance to everyone in advance.
- Define the specific techniques and tools that can be used and when/where they can be used.
- Make sure surveillance capabilities and actions always support agreed-upon objectives and nothing more.

Andrew Walls
Vice President

To the Point: The DLP Process — More Than Just a Piece of Technology

- Ask yourself, "Is my DLP platform an expensive brick or is it clearly contributing value?"
- Manage the DLP platform so that it does not become a security risk itself.
- Work with colleagues across the organization to determine responsibilities and develop a RACI chart.
- Put the onus on the lines of business to define what they worry about, and turn it into a policy.
- Develop a meaningful metric to reflect what the events generated by that policy really mean.
- Tie this in with business-value-oriented metrics.

Rob McMillan
Research Director

Deep Dive Into Internet Infrastructure Attacks

- Treat Internet access/availability like electricity circa 1995.
- Include Internet infrastructure disruption in incident response and business continuity plans.
- Prioritize certificate management processes and tools.
- When looking at wireless data service, consider mobile users and the Internet of things with an integrated approach.

Lawrence Orans
Research Director

To the Point: Managing Identity and Access in a Hybrid World

- Develop a Strategy for Leveraging IAM Services in a Hybrid World.
- Partner with business leaders to include security/IAM assessments as part of the planning process when procuring cloud-based business application services.
- Judge enterprise readiness to adopt IDaaS based on corporate risk goals.
- Understand your costs for providing internal IAM functions as a prelude to comparative shopping for cloud-delivered IAM.
- Plan for mobile user use cases that will include employee- or consumer-owned devices and direct access to SaaS.

Gregg Kreizman
Vice President

TRIP REPORT

Protecting Your Network in the BYOD Era

- Aim for a "contain" strategy initially.
- Evolve to an "embrace" strategy by:
  - Developing policies to complement mobile strategy
  - Implementing technologies (for example, MDM and HVD) that mitigate the security risk of BYOD

Lawrence Orans
Research Director

Architectural Approaches to Reduce Mobile Computing Risks

- Use "managed diversity" to decide which platforms can be supported for typical company use cases and to decide how much support will be offered.
- Use "trust boundaries" and the supporting strategic mobile security technologies to decide how much the information will be made available to mobile users.
- Give up on the idea of trusting the platform.
- Require BYOD users to opt-in to company MDM in a trade for access to business systems

John Girard
VP Distinguished Analyst

To the Point: Developing and Implementing a Superior Mobile Device Policy

- Require users to opt-in to company MDM in a trade for access to business systems.
- Use "trust" and the supporting technologies as a decision point for the information made available to mobile users.
- Where possible, limit user access to basic PIM functions; filter sensitive materials; and deliver rich applications via portals, rather than storing data on the mobile device.
- Place the responsibility and the liability for consumer device security and policy compliance where it belongs: with the business units and the users.

John Girard
VP Distinguished Analyst

THANKS TO OUR 2012 SPONSORS

PREMIER SPONSORS

ca technologies

ORACLE

PLATINUM SPONSORS

CITRIX

paloalto NETWORKS the network security company

Symantec

vmware

SILVER SPONSORS

airwatch mobile device management

BlueCoat

Centrify

DELL SonicWALL

FIRST POINT GLOBAL

Good

Netbox BLUE

NetIQ

Ping Identity

SHELDE

SOURCEfire

TrustSphere

websense

SAVE THE DATE

Gartner **Security & Risk Management** Summit 2013 will take place in Sydney on 19 – 20 August 2013.

Be sure to bookmark the website — **gartner.com/ap/security** — and check back for 2013 Summit updates.