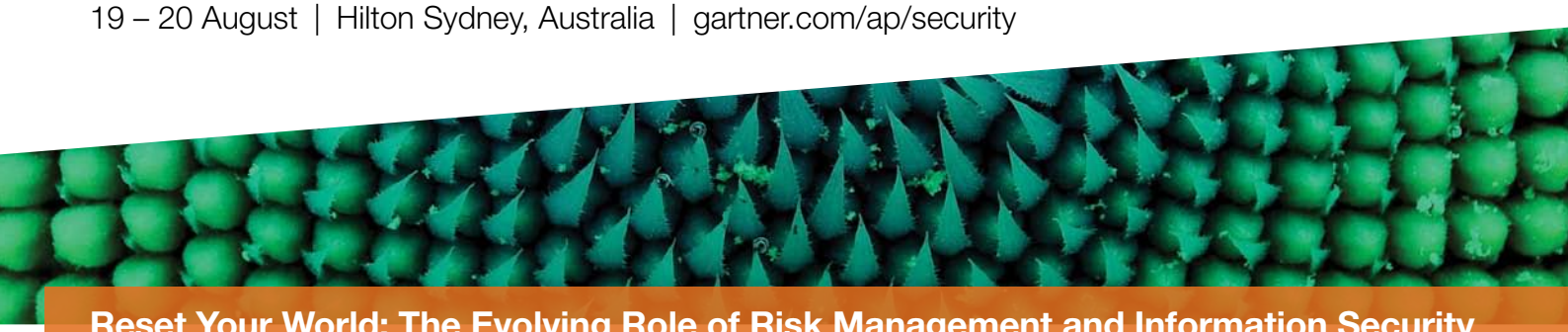
Gartner Security & Risk Management Summit 2013

19 – 20 August | Hilton Sydney, Australia | gartner.com/ap/security



Reset Your World: The Evolving Role of Risk Management and Information Security

TRIP REPORT

The Gartner Security & Risk Management Summit 2013 was held on 19 – 20 August 2013, at the Hilton Hotel, Sydney, Australia. This report summarizes and provides highlights from the event.

Overview

At this annual Gartner Security & Risk Management Summit, attendees sought ways to reset their IT security and risk strategy for success; stay relevant as IT security and risk are redefined; implement BCM best practices for threat resilience; mitigate the risks of new social collaboration tools; craft strategy for emerging BYOD and mobile threats; learn new regulatory compliance requirements; and more.

This year's summit attendees participated in on-site benefits: hearing the latest presentations from the Gartner research community on today's most pressing topics, attending workshops 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 in the Solution Showcase.

SAVE THE DATE

The **Gartner Security & Risk Management Summit 2014** will take place 25 – 26 August 2014, at the Hilton Hotel in Sydney. Be sure to bookmark the website, **gartner.com/ap/security**, and check back for 2014 conference updates.

TABLE OF CONTENTS

Gartner Keynote Sessions

Opening Global Keynote: Reset

F. Christian Byrnes, Paul E. Proctor, Rob McMillan and John A. Wheeler

In this well-attended opening keynote, Gartner analysts parodied "A Christmas Carol" to show that now is the time to break the inertia that blocks progress in security and risk management. They explained that the evolution of risk and security officer roles shows the way to reset your approach to security and risk management, and create and sustain significant security and risk benefits to your organization.

- Help stakeholders balance the need to protect the organization against the need to operate the business
- Engage all the controls at our disposal, including behavior change, process, and technology controls
- Assess and prioritize risks to support conscious decisions to address threats
- Understand the impact of IT risk on business outcomes
- Formalize programs with repeatable, survivable, and measurable processes
- Use the power of risk management and security to influence business decision making

The Gartner Five-Year Security and Risk Scenario

F. Christian Byrnes

In this keynote, Gartner analysts F. Christian Byrnes presented a five-year projection of the state of security and risk developed by the Gartner security and risk research community, which provided a base for your long-term strategic planning. Gartner analysts shared their new insights, and then turned to the audience for an open discussion.

- Analyze the impact of the four quadrants on your organization
- Outline your response to each of the four quadrants using the strategy tool
- Monitor the environment for milestones as they occur
- Shift your controls strategy as change happens

F. Christian Byrnes
Managing Vice President

Paul E. Proctor
Vice President and
Distinguished Analyst

Rob McMillan
Research Director

John A. Wheeler
Research Director

"First Gartner Event — enjoyed and found very informative. Plan to attend regularly."

Senior Security Centre Solutions Architect, NEC

Take-Aways from Gartner Security & Risk Management Summit 2013

Here are key recommendations from this year's most popular Gartner analyst sessions — especially useful for your 2014 planning and strategy considerations.

Big Data Discovery Using Content-Aware Data Loss Prevention (DLP) Solutions

Rob McMillan
Research Director

Content-aware DLP discovery leaders should …

Monday Morning

- Review take-aways and insights.
- Draft a high-level strategy for data discovery initiatives.

Next 90 Days

- Workshop the opportunities for data discovery internally.
- Identify business drivers for data discovery and map them to projects, compliance requirements, and value dimensions.
- Map key cloud encryption solutions into business key performance/risk indicators and use this to engage the CIO, CISO, CRO, finance, HR, and other business units in discussions.

Next 12 Months

- Assess deployment progress and refine your approach.

How to Create Emergency Messages That Won't Be Ignored — Best and Worst Practices

Roberta J. Witty
Research VP

- Announce the service:
  - With corporate messaging and FAQs
  - Ensure accurate data
- Keep the message simple.
- Mention your company name in each communication.
- Decide "polling" versus "information".
- Don't replace your email system; enhance it as necessary.
- Avoid "opt-out" for corporate safety emergency notifications.
- Have a "follow up"/backup plan when 100% response is required.

Top Security Trends and Takeaways for 2013 and 2014

John A. Wheeler
Research Director

Action Plan for Security and Risk Leaders

Monday Morning

- Assess how well the strategic vision of your security and risk program addresses the Nexus of Forces and specific trends.

Next 90 Days

- Educate your IT delivery and executive stakeholders on the challenges and opportunities of the Nexus of Forces.
- Assess the maturity of the major elements of your risk and security program, and decompose gaps into projects.
- Map key risk indicators into business key performance indicators, and use this to engage the business in risk discussions.

Next 12 Months

- Develop a long-term strategy for continuous improvement.
- Develop and deliver an executive reporting scheme that addresses the needs of a business audience.

Cloud Risk Management

Jay Heiser
Research VP

- Base purchases on business requirements.
- Use standards for external party risk assessments.
- Protect highly sensitive data with control technology as it becomes practical/available.
- Always have a contingency plan for supplier failure.
- Seek business ownership for the business' use of information and technology.

Strategic Road Map for Financial Services Enterprise Risk Management

John A. Wheeler
Research Director

Action Plan for CIOs, CROs and CISOs

- Engage all the controls at your disposal.
- Prioritize risks and make conscious choices.
- Develop a true understanding of your business.
- Formalize your program.
- Upgrade to modern technologies like next-gen FW.
- Stop being compliance-driven.
- Stop treating DLP like a data firewall.
- Stop reporting operational metrics to executives.

Transform Your Security Program — From Control-Centric to People-Centric

Tom Scholtz
VP Distinguished Analyst

A Proposed Strategy for the Brave

- Get stakeholder buy-in to pilot the new approach:
  - CEO, compliance, audit, legal, HR
- Modify your charter (or implement a temporary alternative charter):
  - Add principles, rights, and responsibilities
- Select a domain:
  - New application, potentially in mobile/BYOD domain, with clearly definable user group
- Define the trust space — identify the applicable policies and controls (avoid developing new ones, except for monitoring and response).
- Develop and roll out targeted education program to users.
- Monitor and be prepared for challenges.

The Information Security Maturity Pathway

Jay Heiser
Research VP

Level 1 (Initial) to Level 2 (Developing)

- At Level 1, you have no program.
- What you need to do:
  - Seek commitment from senior management for a formal program
  - Conduct an independent review to complement your maturity assessment
  - Assess the extent of information security activity in the organization. There will probably be some activity
  - Appoint a de facto CISO and give that person a mandate and budget to start a program

Level 2 (Developing) to Level 3 (Defined)

- At Level 2, you have a rudimentary program.
  - Probably still talking about "IT security," not "information" security
- What you need to do:
  - Establish a cross-functional governance regime with a clear charter
  - Define the "security vision" — use industry standards
  - Formalize the CISO role and establish the security team
  - Develop the security process catalog
  - Progress the security program so that it builds momentum

Level 3 (Defined) to Level 4 (Managed)

- At Level 3, you have a working program.
  - Whether it's good enough is in the details
- What you need to do:
  - Make your governance effective
  - Finalize and confirm accountabilities
  - Formalize security cornerstones such as policies, processes and security architecture
  - Complete the remedial security program
  - Begin measuring security
  - Tailor training programs to target different staff needs

Level 4 (Managed) to Level 5 (Optimizing)

- At Level 4, you have a good program.
  - Many organizations could stop here
- What you might consider to get to Level 5:
  - Implement a program to assess and enforce compliance to policy. Enable controlled exceptions
  - Strengthen security metrics to show relevance to business objectives and risks
  - Begin regular reporting to the board
  - Work to rolling 3- or 5-year security strategies to ensure continuous improvement
  - Link executive performance to security management

That Frightening Phrase: "The Standard of Due Care"

Rob McMillan
Research Director

Action Plan for CISO — and Others

Monday Morning

- Have a coffee and a long chat with your legal counsel. Understand each other's world.
- Establish, care, and feed your risk register.

Next 90 Days

- Catalog your "due care burden" and your position against it.
- Assess whether there are any aspects to your security posture that would fail the "reasonable steps" test.

Next 12 Months

- Fix any problems that would lead to a failure of the "reasonable steps" test.
- Practice your response to a security incident.

Organizing for Success — Developing Process-Centric Security Teams

Tom Scholtz
VP Distinguished Analyst

Action Plan for Security Executives

Monday Morning

- Review your security process status.
- Assess your security program maturity.

Next 90 Days

- Formalize your security process catalog.
- Assess your security organization.

Next 12 Months

- Change your organization structure if required.

Using Outside Resources — Security Consultants and Threat Intelligence Services

Rob McMillan
Research Director

- Allow 12% of the security budget for external consulting, but have specific tasks in mind.
- Pick the right type of consultant for the context of the task. This means understanding your political, timing, and quality requirements.
- Make your preferred consultant prove their worthiness. Like everything in life, caveat emptor.
- Use threat intelligence services to plan for the right threats. It can take up to two years, or more, to be ready for an emerging threat.

Action Plan for CISOs

Monday Morning

- Read "How to Evaluate a Security Consulting Firm".
- Review your existing works in progress to ensure that the requirements, pricing, and deliverables are right.

Next 90 Days

- Read "How to Select a Security Threat Intelligence Service".
- Develop, in cooperation with your procurement office, a set of security requirements mandatory for consulting engagements.

Next 12 Months

- Decide whether you need to use threat intelligence services to help inform your strategic planning cycle.
- Engage a threat intelligence service provider if you need to use threat intelligence services.

The Risk Management Maturity Pathway

Rob McMillan
Research Director

Level 1 (Initial) to Level 2 (Developing)

- At Level 1, you have no program.
- What you need to do:
  - Assess the culture and gather evidence to support a business case. Set expectations with senior management
  - Assess the extent of risk management already in the organization and how it works, if at all
  - Define a model for risk management roles and responsibilities
  - Define the scope for a program

Level 2 (Developing) to Level 3 (Defined)

- At Level 2 you have a rudimentary program.
- What you need to do:
  - Formalize the activities and structures of risk management governance committees
  - Create a risk register
  - Implement a common language
  - Define a common risk assessment process
  - Establish business asset owner accountabilities
  - Formalize program measurements and reporting

Level 3 (Defined) to Level 4 (Managed)

- At Level 3, you have a working risk program:
  - It meets your need but isn't state-of-the-art
- What you need to do:
  - Broaden the established enterprise governance committee approach across the entire organization
  - Map KRIs to business performance KPIs in order to engage business unit leaders
  - Assign accountable owners to any remaining, identified gaps in risk controls
  - Develop and implement an enterprise risk communication and awareness program

Level 4 (Managed) to Level 5 (Optimizing)

- At Level 4 you have a strong program:
  - It is a strategic asset
  - It facilitates informed, long-term risk decisions across the enterprise
- Level 5 is not for the faint-hearted:
  - This level is really about improving the quality and usefulness of information
  - Consider linking risk-related KPIs to executive performance management and remuneration

Top 10 Security Myths

Jay Heiser
Research VP

- Incorporate human factors into your security program.
- Understand how people react to ambiguous and risk situations.
- Base your security program around what the business needs.
- Create mechanisms that can help business managers conceptualize their security risks.

Why ERM and GRC Depend on Each Other to Succeed

John A. Wheeler
Research Director

- Develop an ERM framework that focuses on risk appetite, risk aggregation, risk assessment, and risk analytics.
- Implement a GRC infrastructure that includes the right technology applications, the necessary architecture, and the appropriate level of assurance.
- Promote risk accountability that drives the right actions that lead to the achievement of desired business outcomes.

Action Plan for Risk Managers

Monday Morning

- Evaluate current risk management and compliance program against the ERM/GRC blueprint.
- Develop list of key stakeholders and program areas to include in integration effort.

Next 90 Days

- Identify gaps and/or integration opportunities using the 10 As.
- Engage board members, senior management, and business operations management to answer key questions.

Next 12 Months

- Define ERM framework and GRC infrastructure build requirements.
- Begin ERM/GRC integration effort.

CyberInsurance — Evolution or Revolution?

Paul E. Proctor
VP Distinguished Analyst

John A. Wheeler
Research Director

- The cyberinsurance market is characterized at present by aggressive selling behavior from brokers and a low knowledge level among buyers.
- These are complicated products with a short track record, so organizations must proceed cautiously to take advantage of the offered benefits.
- Cyber and related liability policies are not a substitute for sound, proactive management of cyber liability risk.
- Adhering to the cyberinsurance screening processes will allow organizations to adopt best practices in risk management.
- Cyberinsurance could play a role in the risk transfer of large and uncertain costs of cyber attacks (black swan events).

Managing Global Recovery and Continuity Risk

Roberta J. Witty
Research VP

Today

- Review your project life cycle process and add BCM at least into the change control process.
- Identify all risks to business operations, not just those related to traditional BCM thinking.
- Identify your key performance and risk indicators for your organization's business processes.
- Access your current crisis management preparedness planning.
- Assess your current state of supply chain resilience.
- Identify a framework to follow.

Near Future (6 to 12 Months)

- Develop an enterprise operational risk view of business operations, including a risk register.
- Assess your current state of resilience against multiple scenarios/risk exploits.
- Work with your supply chain to meet its recovery requirements.
- Map performance and risk, and then educate management on the importance of business resilience.
- Understand the cost-benefit position of multiple levels of resilience.
- Build recovery and resilience planning into the performance review process.
- Build resilience and recovery planning into the project life cycle.

Long Term (Beyond 12 Months)

- Review all the above on an annual basis for business applicability.

Linking Risk to Business Decision Making — Creating KRIs That Matter

Paul E. Proctor
VP Distinguished Analyst

Action Plan for CIOs, CROs and CISOs

- Review all of your dashboards and metrics.
- Define the audience they address.
- Determine the decisions for the audience that are influenced by the metrics.
- Determine the causal relationships each metric has to a business dependency.
- Revise your metrics to be leading indicators.
- Reposition IT operational metrics away from business decision makers.

Practicing Safe SaaS

Jay Heiser
Research VP

Recommendations

- Base purchases on business requirements.
- Use standards for external party risk assessments.
- Protect highly sensitive data with control technology as it becomes practical/ available.
- Always have a contingency plan for supplier failure.
- Seek business ownership for the business' use of information and technology.

Predictions — Your Network Security in 2018

Mark Nicolett
Managing VP

In 2018, Your Netsec Will ...

- Be expensive and mostly point solutions.
- Use out-of-band inspection — still mainstream for WAN/LAN and very-high-speed links.
- Need to secure your SDN and virtualization, as they won't be self-defending.
- Have more hybrid aspects.
- Still be deployed in depth.
- Not be fully virtualized, but accommodate virtualization.

Call to action: 2018 is less than one firewall refresh away

CyberSecurity! (The Biggest Scam since The Ponzi Scheme)

John Girard
VP Distinguished Analyst

- Enterprises: Ignore all things cyber; focus on vulnerability remediation and improvements in security monitoring and shielding.
- Enterprises: Collaborate with government efforts, but within reasonable limits.
- Governments: Don't let the confusion of "cyber" deflect your attention from state-sponsored threats.
- Unique Entity: Use cybersecurity as a synonym, but don't let it take strategy where you don't want it to go.
- Critical infrastructure: You are a unique entity, but your defenses won't change much.

Cost, Consequence and Value — The Economics of IAM

Gregg Kreizman
Research VP

- Identify the type of IAM justification required by your enterprise and the sponsor(s).
- Develop IAM cost estimates based on formulas of function required by the business.
- Calculate the current costs of services delivered by IAM within your enterprise
- Create pragmatic metrics for measuring IAM project and program success.
- Evaluate new means of IT consumption and delivery to incorporate changes within current IAM programs.

Action Plan

Monday Morning

- Identify the players, processes, and products currently involved in IAM at your enterprise.
- Determine if there are any current initiatives involving or requiring IAM currently under way.

Next 90 Days

- Calculate current costs of delivering IAM process in your enterprise.
- Evaluate current technology and service options for IAM delivery in the market.

Next 12 Months

- Document requirements and process changes required for best-practice IAM.

Security Monitoring for Early Breach Detection

Mark Nicolett
Managing VP

Your Action Plan

CISOs and security managers should …

Monday Morning

- Integrate threat intelligence feeds supported by your SIEM vendor.
- Begin deployment of anomaly detection functions for high priority use cases.

The Next 90 Days

- Evaluate opportunities to integrate your SIEM with Active Directory and other IAM sources to gain user context.

The Next 12 Months

- Evaluate readiness for lean-forward tools.
- Evaluate opportunities to improve security analytics, subject to staffing and project support constraints.

Securing the OT Environment

F. Christian Byrnes
Managing VP

Action Plan for CIO or CISO

Monday Morning

- Find out who is in charge of OT security. If it is more than one person, find them all.
- Ask for a meeting with your management to discuss your role in this effort.

Next 90 Days

- Establish communications with your OT counterparts in a series of meetings to establish requirements and identify processes.
- Hire an outside consultant to assist in assessment and planning — someone who isn't political or too close to the issues.

Next 12 Months

- Use the IT/OT security assessment results to make a multiyear plan.
- Set up training and awareness programs, and define consolidated security roles.

Your Cloud and Mobile Devices Broke My IAM

Gregg Kreizman
Research VP

Develop an IAM Strategy That Includes Cloud, Mobile, and Social Needs

- Partner with business leaders to include security/IAM, mobile, and social requirements as part of the planning process when procuring and developing business applications and services.
- Understand your costs for providing internal IAM functions, and your ability to obtain and retain staff as a prelude to comparative shopping for IDaaS.
- Plan for mobile user use cases that will include employee- or consumer-owned devices and direct access to SaaS.
- Incorporate social identities using a graded access approach to mitigating risk.
- Obtain vendor road maps for supporting cloud, mobile, and social.

Endpoint Security — When the Consumer Is King

Song Chuang
Research Director

- For enterprise PCs, focus on application control.
- Implement MDM, containerization, and NAC to protect corporate mobile devices.
- Consider using cloud SWG to provide acceptable usage.
- For BYOD, focus on real threats to data and transaction systems, and select solutions appropriately.

Workshop: Information Security Architecture 101

Tom Scholtz
VP Distinguished Analyst

- Position security as a principal enabler to achieving the requirements of business.
- Get buy-in and support from business — "No more Dr. No."
- It is about planning for the future.

Workshop: Cloud Contracts — Develop Your Own Security and Risk Exhibits

Gayla Sullivan
Research Director

Recommendations

- Forge relationships with sourcing, procurement and/or vendor management, and discuss concerns.
- Engage and educate stakeholders in security and risk management of cloud providers.
- Develop a checklist of RFP/precontract requirements — list deal breakers that would prevent service provider use.
- Develop contract exhibits for use as standard language in cloud agreements.
- Be ready for crises, and ensure that everyone knows his or her role.

Workshop: Build an Effective Security and Risk Program

Tom Scholtz
VP Distinguished Analyst

Your Action Plan

Monday Morning

- Review the maturity of your security and risk program, if you have one.
- Initiate a program if you do not have one.

Next 90 Days

- Obtain executive support for your program.
- Establish the required governance forums.
- Develop a strategy plan.

Next 12 Months

- Refresh your program if it is not delivering what you need.

Workshop: Supplier Contingency Planning: What You Need to Know for Supplier Recovery

Gayla Sullivan
Research Director

- Develop a supplier contingency framework within your existing risk management framework.
- Categorize vendors by the potential risk impacts.
- Evaluate current supplier contingency contract clauses.
- Develop BCM key performance indicators and service-level agreements.
- Make vendor risk management and supplier contingency a business imperative.

Workshop: Security Monitoring of Cloud Workloads

Mark Nicolett
Managing VP

Keep a process check on the following:

- What's in the cloud now?
- What's being monitored now?
- What workloads are planned for the cloud?
- Cultural, security, and compliance issues.
- How will you monitor?

Workshop: ITScore for Privacy

John A. Wheeler
Research Director

- Establish the maturity of your enterprise's privacy program, and address the areas identified as requiring improvement.
- Set a maturity objective for your organization. Invest in reaching that level only if there is a business case.
- Analyze emerging technologies for its privacy impact (e.g., location-based services, cloud computing and social media).
- Take a risk-based approach to privacy.
- Make sure you have the basics covered: privacy officer, privacy policy and usage policies.

Guest Keynotes

Closing the Gap — Security → Privacy

Malcolm Crompton, Managing Director,
Information Integration Solutions Pty Ltd

Regulation may be the only way to improve website privacy policies according to former Australian Privacy Commissioner, Malcolm Crompton. Speaking at the Gartner Security & Risk Management Summit in Sydney, Crompton was responding to the results of a privacy sweep by current Commissioner, Timothy Pilgrim, which found that nearly 50 per cent of website privacy policies were difficult to read. On average, policies were over 2600 words long.

The sites were also rated against the Australian Privacy Principles (APPs) which come into law on 12 March 2014. To comply with APP1, which covers the open and transparent management of personal information, organisations must have an up-to-date privacy policy.

Crompton told media that companies should "start again" if their policy is not easy to read. He added that global regulators may need to step in if website privacy policies are going to improve in the future. According to Crompton, companies should create a layered privacy notice where the policy's key points are contained on one page. The user can then access a longer privacy notice where more detail is set out. He added that a policy should set out all the possible uses of customer information and how it is collected.

Gartner Australia research director Rob McMillan said an easy to read privacy policy would signal to consumers that the company has nothing to hide. McMillan said that 80 per cent of the website policies he has read are "very long" while the remaining 20 per cent used plain language.

Courtesy of Computerworld

How a Security Program Encourages User Engagement and Grows Business

Craig Davies, CISO,
Cochlear

Australian hearing aid implant manufacturer Cochlear has improved employee security awareness since embarking on a re-education program two years ago. Craig Davies told delegates that his security team runs an "observe and monitor" program.

"I believe the vast majority of people want to do the right thing, but the trouble is we don't tell them what the right thing is," he said. "They're always worried that they are going to breach some rule. What we have tried to do is drive all the housekeeping stuff out of our environment. We want the basics done right."

The company also has an acceptable Internet use policy which is deployed worldwide. It blocks some sites such as Australian dating service RSVP and music streaming site Pandora. Davies added that it is non-negotiable about piracy. It uses a rating system for these types of security incidents ranging from accidental access up to high ranking. Davies said it was important that staff were engaged with security awareness programs. According to Davies, he used to get one to two security incidents a week before doing the re-education program. He has not had a security incident for the past three months.

Courtesy of CIO.com

The Mobile Banking Balancing Act — Balancing Risk and Security with User Experience

Johnathan Sharratt, Solution Architect, ING Direct

Complaints about its mobile banking app led ING Direct Australia to develop a new version which offered improved features with good security. Johnathan Sharratt told delegates that its old app had a limited set of features. "It forced our users back to the website because they couldn't do what they wanted to via mobile," he said. "As a result, we had a bad rating on Apple's App Store and anonymous comments from unhappy customers."

A new app was released for iOS and Android devices on 25 June 2013. Once a customer is registered, they can check their balance without entering a PIN. "Having to enter a PIN just takes too long," Sharratt said. "The key with PIN-less transactions is focusing on low risk areas such as balance checks." All high risk transactions no longer require SMS messages to be sent. ING Direct got rid of the SMS service partly due to an increase in malware and the cost of sending messages to customers. Transactions are kept secure through two-factor authentication and a security certificate.

According to Sharrat, ING Direct's app is now one of the most popular banking apps in Australia. "We had 180,000 downloads within five weeks of release. Of those downloads, 74,000 registered the app," he said. Of the people who registered the app, half of them login to their account every day.

Courtesy of techworld.com.au

Achieving Value & Relevance

Eric Cowperthwaite, Chief Information Security Officer, Providence Health & Services

Providence Health & Services has more than 63,000 people, operating 32 hospitals in 5 states on the west coast of the USA. At the Gartner Opening Keynote, they were cited as a great example of how to build an appropriate risk and security program. In response to a series of security-related issues early in 2006, Providence went on a multi-year journey to create a mature security and risk management program. In 2006, they had a program with only five employees who were focused almost entirely on technical issues. Providence spent approximately 18 months in a "reactive" mode, addressing the most urgent problems and high-risk issues it had identified … and they hired a Chief Information Security Officer Eric Cowperthwaite.

Hiring new employees took considerable time, but Providence went from 5 to 32 employees in the security organization. They developed proactive risk and security processes that are transparent, measurable and support accountability. Today their program has higher maturity than most healthcare delivery organizations in the US. Providence's CISO, Eric Cowperthwaite has identified four critical factors in the success of its security program:

- Executive sponsorship
- Business unit support
- Planning
- Governance

Eric Cowperthwaite delivered the End-User Keynote at the Summit highlighting areas to focus on and ask the relevant questions: How does your organization view cloud, mobile, social media as opportunities, places to make money, new customers, capture markets? How many cloud apps and infrastructure is your company running? BYOD? Do you have a mobility strategy? Are you 5 steps behind already?

Eric ended his presentation with the following recommendations from a practical perspective to add value and relevance to your organization:

- Find out what your boss' objectives are
- Help your boss and other leaders earn their performance compensation
- Show that your activity supports the strategy
- Ride the elevator as a good citizen
- Have a beer with the CFO
- AND ask how to make your activity strategic

Thank you to our Sponsors

Premier

airwatch — We Simplify Enterprise Mobility™
CISCO
hp

Platinum

Good
PIREAN
RSA
SOURCEfire
Symantec
TrustSphere

Silver

ARBOR NETWORKS
BLUE COAT
CipherCloud — Trust in the Cloud™
Decipher Works — SECURING YOUR ENTERPRISE
DELL Software
FireEye
FIRST POINT GLOBAL
Netbox BLUE
NetIQ
Ping Identity
SHELDE
splunk>
websense
zscaler — Secure. Everywhere.

> "The quality of the attendees was high-knowledgeable people with interesting business problems."
>
> Regional Solutions Architect — APAC, Ping Identity

Post Event Resources

Customizable post-event worksheet

Take a moment to complete your own post-event trip report, a valuable resource for future reference and a great way to share with colleagues what you learned.

Learn more with relevant research

Want to learn more about the topics that interest you most? Turn to the end of each session presentation for a list of related Gartner research notes. Select Gartner research is available on demand at **gartner.com**.

CONNECT WITH GARTNER SRM

Connect with Gartner Security & Risk Management Summit on Twitter and LinkedIn.

#GartnerSEC

Gartner SECURITY Xchange

> "I have had a great experience at the Security & Risk Summit and will take with me some very valuable insights and resources. I look forward to the next summit and gaining more insights and knowledge in the realm of security and risk."
>
> RACQ Group

28 – 31 October
Gold Coast, Australia
gartner.com/au/symposium

Gartner®
SYMPOSIUM ITXPO® 2013

The World's Most Important Gathering of CIOs and Senior IT Executives

Leading in a Digital World

Accelerating growth. Creating new connections. Driving greater agility. A powerful convergence of forces — mobile, social, cloud and information — is rapidly reshaping how business gets done now and in the future. CIOs and senior IT executives are at the center of this transformation, leading the creation of the digital enterprise. At Gartner Symposium/ITxpo 2013, attendees will discover how to seize new opportunities, forge strategic partnerships to drive change, and evolve to become indispensable leaders in the digital world.

Audience highlights

500 CIOs

70 solution providers

1400 total attendees

200+ sessions

50+ Gartner analysts