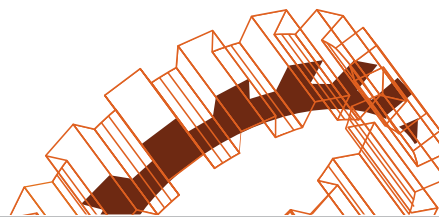# Gartner
Security & Risk Management Summit 2015

24 – 25 August | Hilton Sydney | gartner.com/ap/security

Manage Risk and Deliver Security in a Digital World

From learning how to re-evaluate and update your security and risk strategies and investments to meeting the evolving needs of the digital organization, the **Gartner Security & Risk Management Summit 2015** will cover the full spectrum of IT security and risk topics.

1 What are the leadership skills needed to be an effective CISO today?

Leaders must mind the gap between risk management necessities and business objectives, while maintaining focus on the digital business horizon, if their IT security, enterprise risk, business continuity, audit, compliance and privacy initiatives are to succeed.

- Top Trends and Takeaways for Cybersecurity   **Earl Perkins**
- People-Centric Security: Experiences and Lessons Learned **Tom Scholtz**
- Pragmatic Policy — Making Your Security Policy Useful **Rob McMillan**
- Be Agile Not Fragile — Use Threat Intelligence Services to Defend Yourself   **Rob McMillan**
- The Path to High Impact Security Awareness   **Rob McMillan**
- Protecting Your House on the Prairie: Security Strategy for the SMB Enterprise   **Rob McMillan, Tom Scholtz**
- The New CISO's Crucial First 100 Days   **Tom Scholtz**
- Dealing with the Dark Side   **Christine Nixon**

"By 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches — up from less than 10% in 2014."

2 What is needed to transform security programs to deal with the challenges of Digital Business?

Digital is not a binary thing. It's not a step that any organization can take to get from yesterday to tomorrow. Digital is a journey; it's the ongoing convergence of information technology with the physical world. Every step of that way is laden with risk.

- Top Trends and Takeaways for Cybersecurity   **Earl Perkins**
- Threat Intelligence — Whys and Hows   **Anton Chuvakin**
- Developing an Information Security and Risk Management Strategy   **Jeff Wheatman**
- Digital Business and Your New Relationship with Risk **Christian Byrnes**
- Challenging Decisions: Third Party Security Assurance Landscape   **Khushbu Pratap**
- The Availability Implications for Digital Business   **John Morency**
- The Cyber Kill Chain   **Craig Lawson**
- Gartner's Adaptive Security Architecture: New Approaches for Advanced and Insider Threats   **Craig Lawson**
- Operational Technology Security is Not Just for Industries Anymore   **Earl Perkins**
- Gartner Opening Keynote: Manage Risk and Deliver Security in a Digital World   **Gregg Kreizman, Earl Perkins, Tom Scholtz**

- Cybersecurity Scenario 2020 — The Impact of Digital Business on Security   **Christian Byrnes**
- Secure Use of AWS and Azure: Comparison and Best Practices   **Jay Heiser**
- Mind the SaaS Security Gaps   **Craig Lawson**

3 What are the approaches to empower people to drive change and transform the business, yet keep a secure environment?

People are often considered the weakest link — but they are also the most flexible one. Constraining employees with overly strict technical and procedural controls can do more harm than good. Keeping them alert and engaged for risk matters remains a challenge.

- Gartner Opening Keynote: Manage Risk and Deliver Security in a Digital World   **Gregg Kreizman, Earl Perkins, Tom Scholtz**
- People-Centric Security — Experiences and Lessons Learned   **Tom Scholtz**
- Changing User Behavior — Challenges and Best Practices **Tom Scholtz**
- Dealing with the Dark Side   **Christine Nixon**
- The Path to High Impact Security Awareness   **Rob McMillian**
- The New CISO's Crucial First 100 Days   **Tom Scholtz**
- Human Risk Management —The Key to Organizational Success   **David Turner**

"By 2020, more than 80% of enterprises will allow unrestricted access to noncritical assets (up from less than 5% today), and reduce spending on identity and access management by 25%."

4 How can I sharpen the security metrics to make them relevant and effective in the era of digital business?

One of the concerns that chief information security officers (CISOs) sometimes have when they develop security metrics for senior-level management is that they think it is too hard to do. The reality is that, in fact, it is hard to do, and our discussions with Gartner clients show that security metrics are rarely linked to organizational performance and risk posture.

- Digital Business and Your New Relationship with Risk **Christian Byrnes**
- Information Security Metrics — Building from the Business Down   **Jeffrey Wheatman**
- Information Security Metrics   **Jeffrey Wheatman**
- The Availability Implications for Digital Business   **John Morency**
- Developing an Information Security and Risk Management Strategy   **Jeffrey Wheatman**
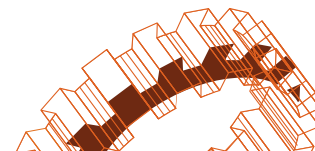
5 What are the best practices to protect your organization in a rapidly changing threat environment?

All types of attacks are continuing to penetrate organizational defenses, highlighting the fact that most enterprise security is based on yesterday's security concepts that use rules and signatures to prevent "bad" occurrences. What's needed is rapid detection and response, enabled in part through behavioral analytics.

- Top Trends and Takeaways for Cybersecurity   **Earl Perkins**
- Be Agile Not Fragile — Use Threat Intelligence Services to Defend Yourself   **Rob McMillan**
- Threat Intelligence — Whys and Hows   **Anton Chuvakin**
- Winning the Data Breach War with User Behavioral Analytics   **Jonathan Care**
- Mobile Security Threats and Trends, 2015   **Rob Smith**
- The Cyber Kill Chain   **Craig Lawson**
- Gartner's Adaptive Security Architecture — New Approaches for Advanced and Insider Threats   **Craig Lawson**
- Keynote — Cybersecurity Scenario 2020: The Impact of Digital Business on Security   **Christian Byrnes**

6 What are the benefits of cloud computing, and how do you prepare for the costs of mitigating these risks?

Failing to analyze cloud risk will result in missed opportunity and/or unacceptable risk to the business. Risk management is a mature discipline that can determine how much cloud risk is acceptable.

- Cloud-based Recovery Management — DRaaS   **John Morency**
- Roundtable: Comparing Best Practices for Cloud Risk Management   **Jay Heiser**
- Cloud Security Scenario   **Jay Heiser**
- Secure Use of AWS and Azure — Comparison and Best Practices   **Jay Heiser**

"By 2019, cloud security audits will routinely include a model that scores risk and implementation effectiveness separately."

7 What are the best practices for monitoring and mitigating vendor risks?

The world of cloud, social and mobile means that many business processes are supported by and dependent on an increasing number of external IT and business processes and extended supply chains. Many end-user organizations are still struggling with these disruptive technologies, yet we are on the cusp of new developments that will add yet more complexity.

- Use a Vendor Risk Management Framework to Mitigate Regulatory, Compliance, Security and Performance Issues   **Christopher Ambrose**
- Challenging Decisions — Third Party Security Assurance Landscape   **Khushbu Pratap**
- What Risks are Microvendors Introducing to Your Enterprise?   **Christopher Ambrose**
- The Cyber Kill Chain   **Craig Lawson**
- Third Party Security Audits — A Slippery Slope?   **Khushbu Pratap**
- Managed Services Solution Providers (MSSP) Success and Failure Tips   **Anton Chuvakin**

"Through 2016, despite being a top priority of CIOs, less than 15% of vendor management programs will leverage data analytics and business intelligence to identify and manage vendor risk."

8 What are the current best practices, latest issues and trends for Identity & Access Management (IAM)?

Many aspects of IAM are technologically mature, but nonetheless remain extremely complex and widely misunderstood. In particular, many unresolved barriers of scale and compatibility are challenging entry into mobile use cases, and there is still no clear industry direction for handling the Internet of Things.

- Roundtable: Securing Mobile Payments and Mobile Wallets   **Rob Smith**
- Leveraging Social Identities to Enable Digital Business   **Anne Elizabeth Robins**
- Future-Proofing IAM   **Gregg Kreizman**

"By year-end 2016, the Internet of Things will drive device and user relationship requirements in 20% of new identity and access management implementations."

9 How do IT organizations adapt to the rapidly changing environment and implement new policies and new technologies to mitigate the risks of the mobile workplace?

Enterprises need to drastically change their endpoint strategy to avoid the increasing disconnect between workforce enablement and security. We illustrate how enterprise approaches to protecting data evolve as mobility and consumer Internet of Things converge.

- Roundtable: Securing Mobile Payments and Mobile Wallets   **Rob Smith**
- Mobile Security Threats and Trends, 2015   **Rob Smith**
- Magic Quadrant: Enterprise Mobility Management Suites   **Rob Smith**
- How To Build A Globally Legal and Successful BYOD Program   **Rob Smith**

"By 2020, 70% of enterprises will treat the entirety of their endpoints as untrusted platforms, regardless of whether they are enterprise or privately owned, up from 20% today."

10 What are the insights into the architecture and use of security technologies to manage risk appropriately?

Enterprises are overly dependent on blocking and prevention mechanisms that are decreasingly effective against advanced attacks. Comprehensive protection requires an adaptive protection process integrating predictive, preventive, detective and response capabilities.

- Mind the SaaS Security Gaps   **Craig Lawson**
- Security Incident Response in the Age of the APT   **Anton Chuvakin**
- The Cyber Kill Chain   **Craig Lawson**
- I've Already Invested in PKI — How Can I Reuse It for Mobility and Internet of Things?   **Anne Elizabeth Robins**
- Gartner's Adaptive Security Architecture — New Approaches for Advanced and Insider Threats   **Craig Lawson**

"By 2020, 60% of enterprise information security budgets will be allocated to rapid detection and response approaches — up from less than 10% in 2014."