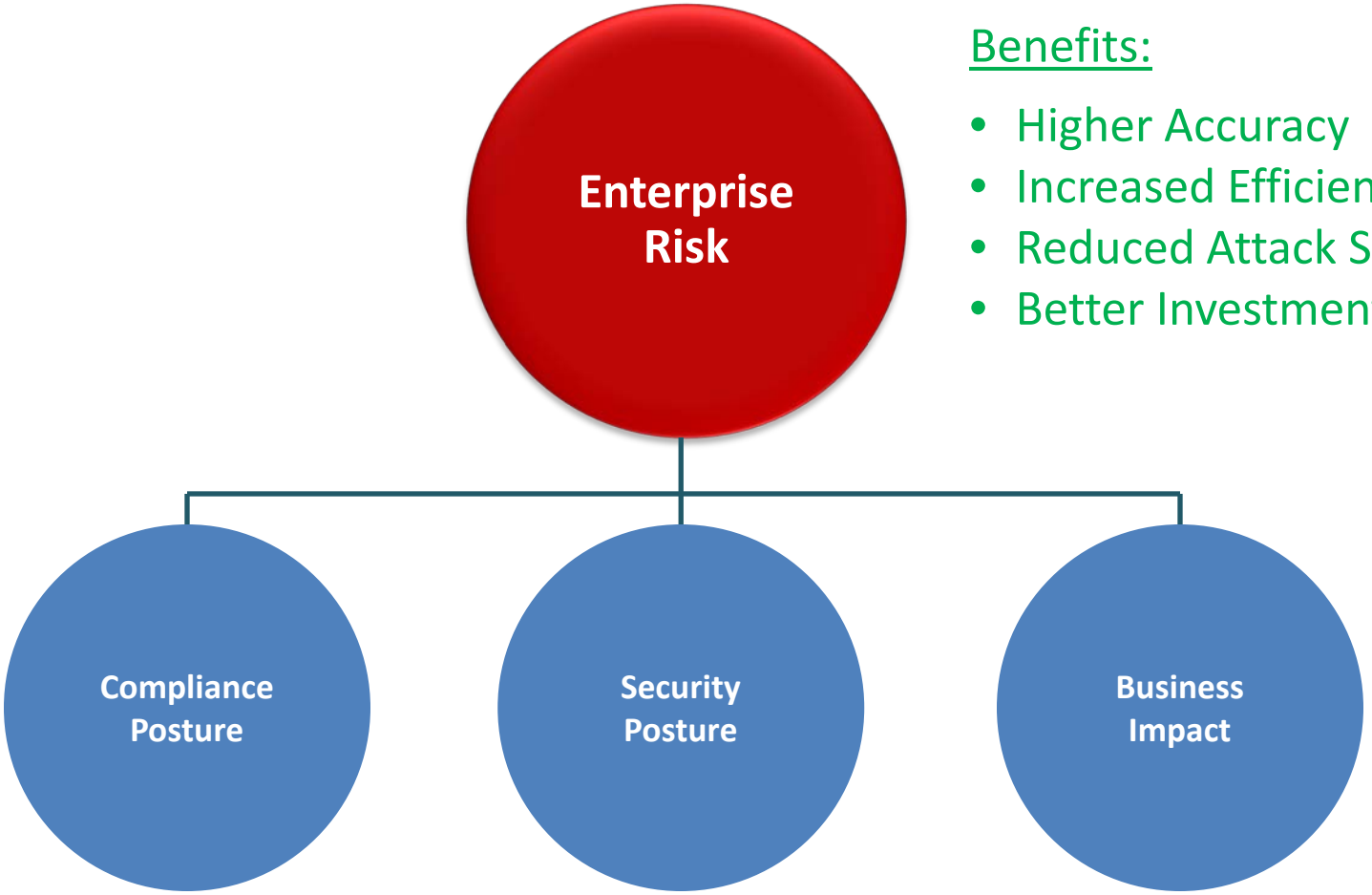
Risk: Security's New Compliance

Torsten George
VP Worldwide Marketing and Products, Agiliance
Professional Strategies - S23

Agenda

- Market Dynamics
- Organizational Challenges
- Risk: Security's New Compliance
- Elements of Risk-Based Security
  - Continuous Compliance
  - Continuous (Security) Monitoring
  - Closed-Loop, Risk-Based Remediation
- Benefits of Risk-Based Security
- Case Studies

Today's Takeaways



Benefits:

- Higher Accuracy
- Increased Efficiency
- Reduced Attack Surface
- Better Investments

Continuous Compliance

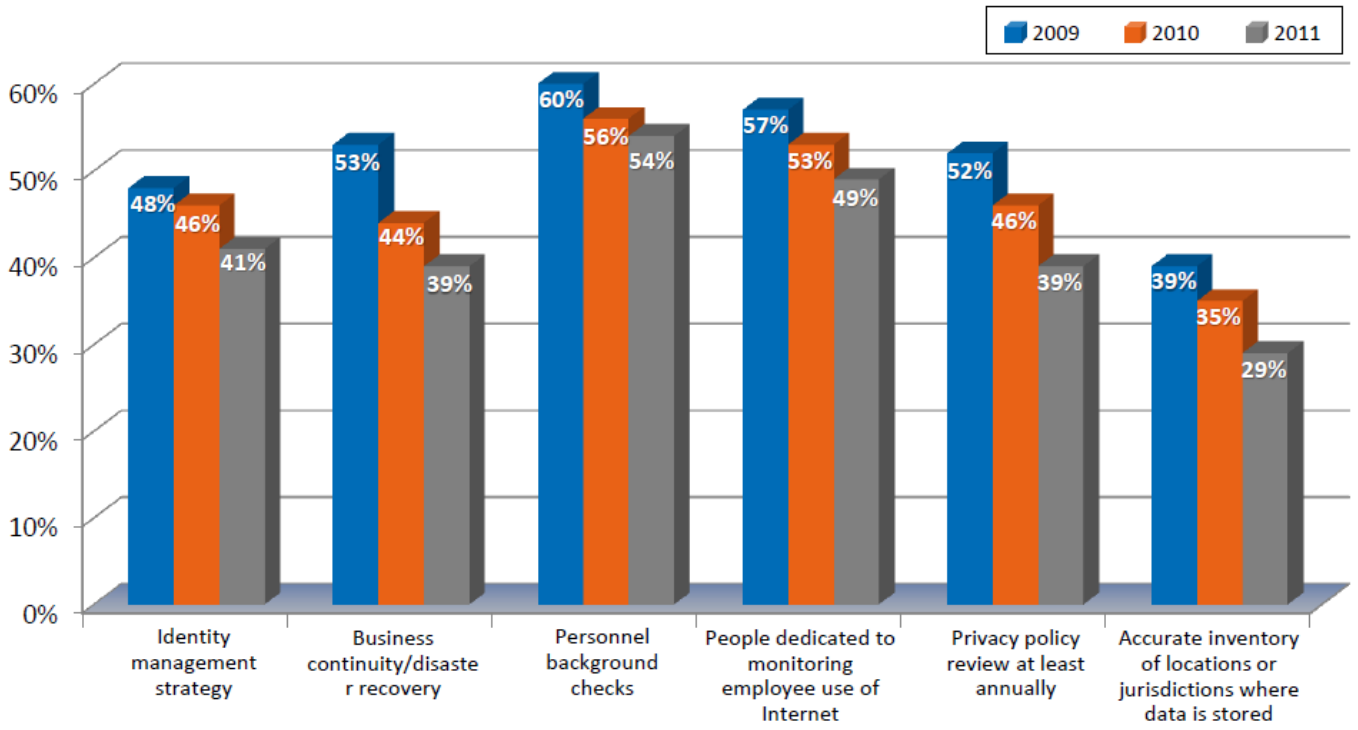
Continuous Monitoring

Risk-Based Remediation

MARKET DYNAMICS

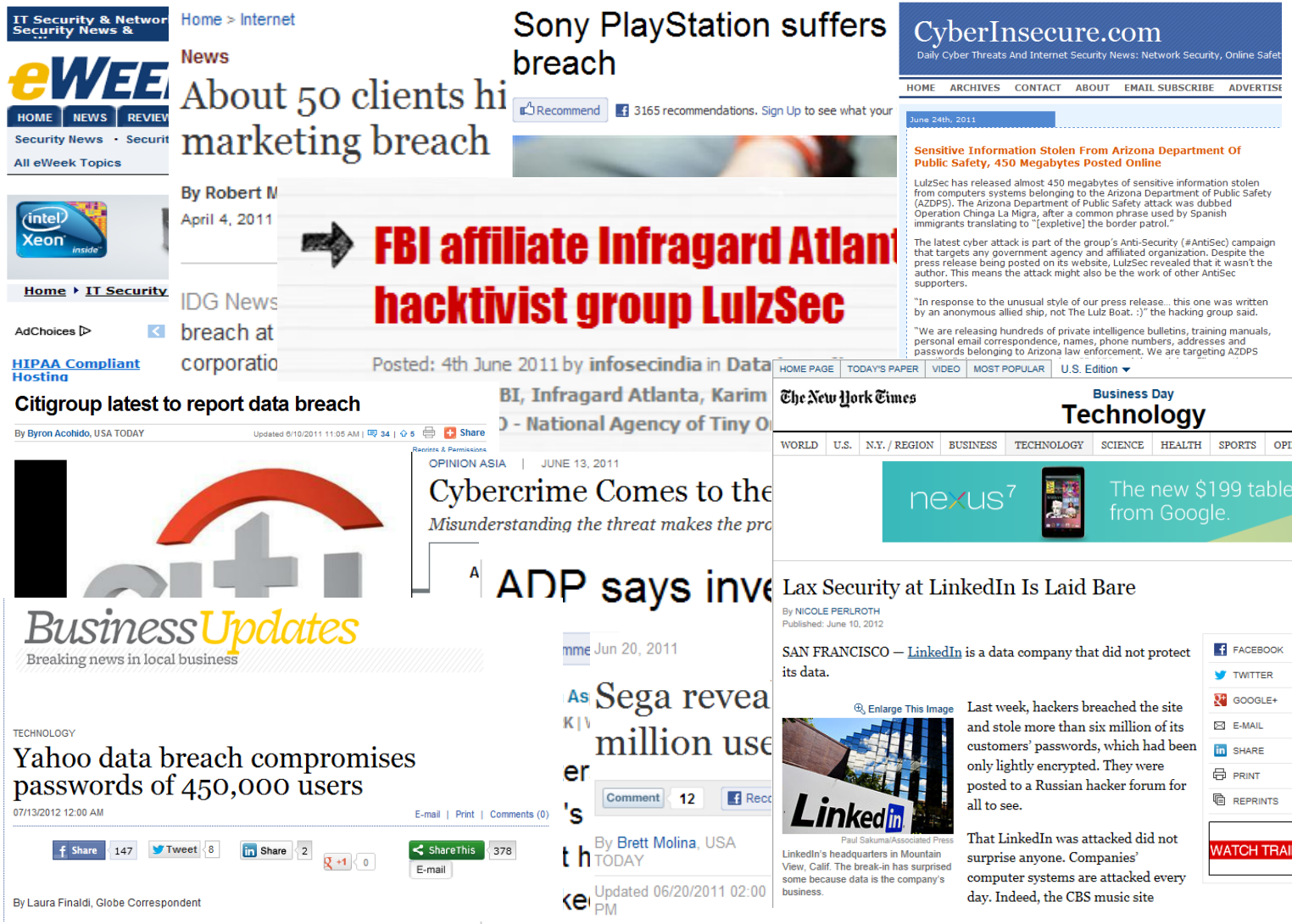
Economic Hardship

After Three Years of Budget Constraints, Degradation in Core Security Capabilities Continues



Source: 2012 Global State of Information Security Survey, PricewaterhouseCoopers, CIO Magazine, CSO Magazine, September 2011

Changes in Attack Landscape



Regulatory Pressure / Enforcement

- NIST SP 800-137
- FISMA
- FedRAMP
- SEC Cyber Guidance
- Office of the Comptroller of the Currency Regulation Enforcement
- Pending Cyber Security Act 2012
- FCC Case against Wyndham Hotel Group

ORGANIZATIONAL CHALLENGES

Organizational Challenges

Efficient Audits Amidst Escalating Regulations

- Growing complexity and variety of regulations and frameworks
- Silo-based approach with multiple owners and stakeholders
- Compliance lacks correlation to risk
- Compliance conducted periodically, not continuously

Automation of Threat / Vulnerability Remediation Actions

- Lack of continuous monitoring
- Lack of interconnectivity of existing security tools
- Lack of risk-based prioritization
- Lack of closed-loop, automated remediation

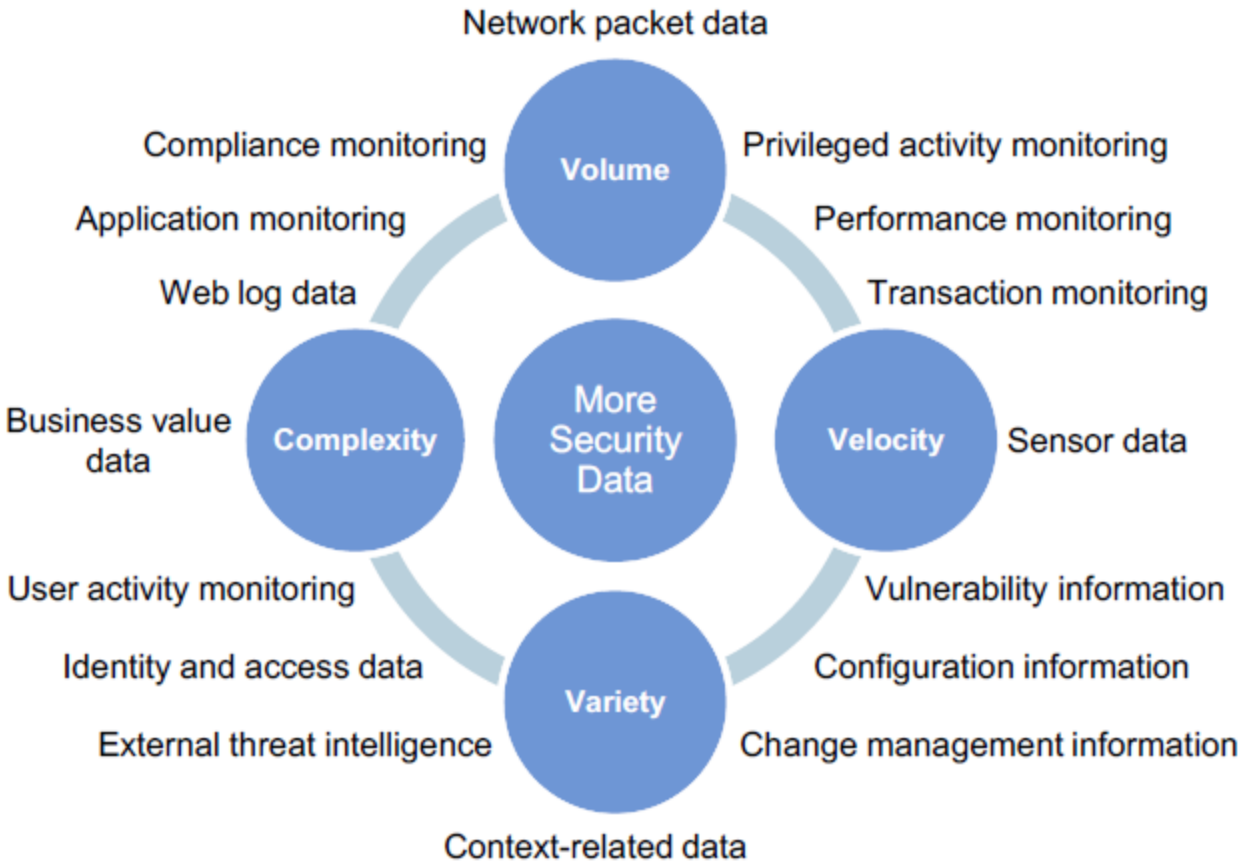
Avoiding Negligence in Incident Response

- Policies and stakeholder data live in dispersed documents
- Lack of notification alerts and automated escalation processes
- Difficulty to define prioritization without knowledge of risk and business impact
- Missing interconnectivity with remediation systems
- Lack of centralized audit trail for post-incident analysis

Effective Risk Trending for C-Suite and Board

- Lack of centralized risk register and processes to gather related data
- Point-in-time measurement leads to false sense of security and inaccurate investment decisions
- Inability to effectively involve domain experts

Common Denominator: Big Data



Gartner, "Information Security Is Becoming a Big Data Analytics Problem", by Neil MacDonald, March 2012

The Bitter Truth

You can schedule an audit, but you cannot schedule a cyber-attack.

In turn, you have to move to a more pro-active, risk-based approach to security.

RISK: SECURITY'S NEW COMPLIANCE

Risk: Security's New Compliance

Reactive Approach

- Security is seen as necessary evil
- Silo-based monitoring
- Reactive and tactical

→ Objective is to defend against threats

Compliance-Driven Approach

- Check-box mentality
- Tactical threat defense is supplemented with layered security controls

→ Objective is to achieve point-in-time compliance certification

Risk-Based Approach

- Pro-active, interconnected, and continuous monitoring and assessments
- Closed-loop, automated remediation based on risk

→ Prevention mentality

Business-Oriented Approach

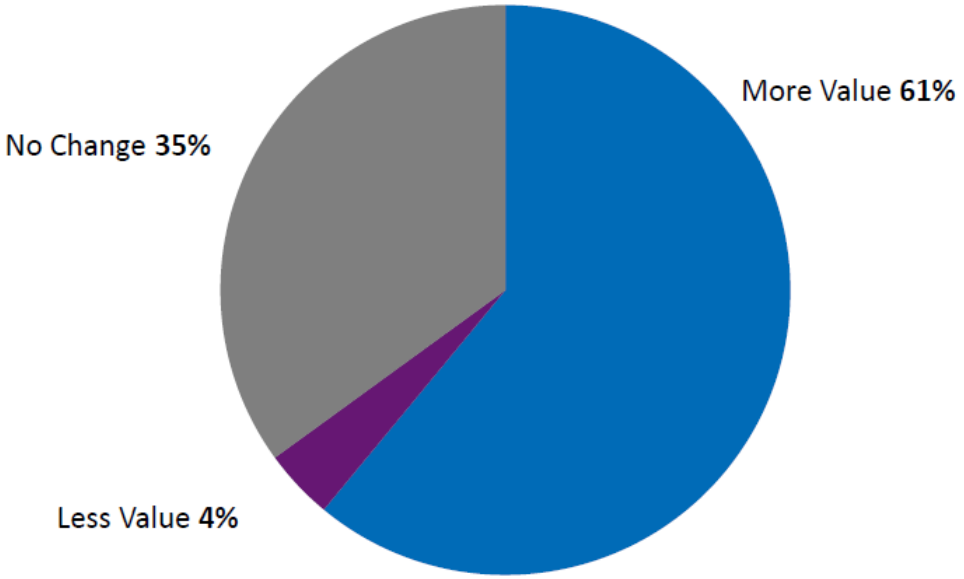
- Connected into enterprise risk processes, taking input across financial, operational, and IT risks

→ Increased operational efficiency and effective business decisions

Tactical ⟷ **Strategic**

Early Adoption

Focus on Managing Risk Not Just Security

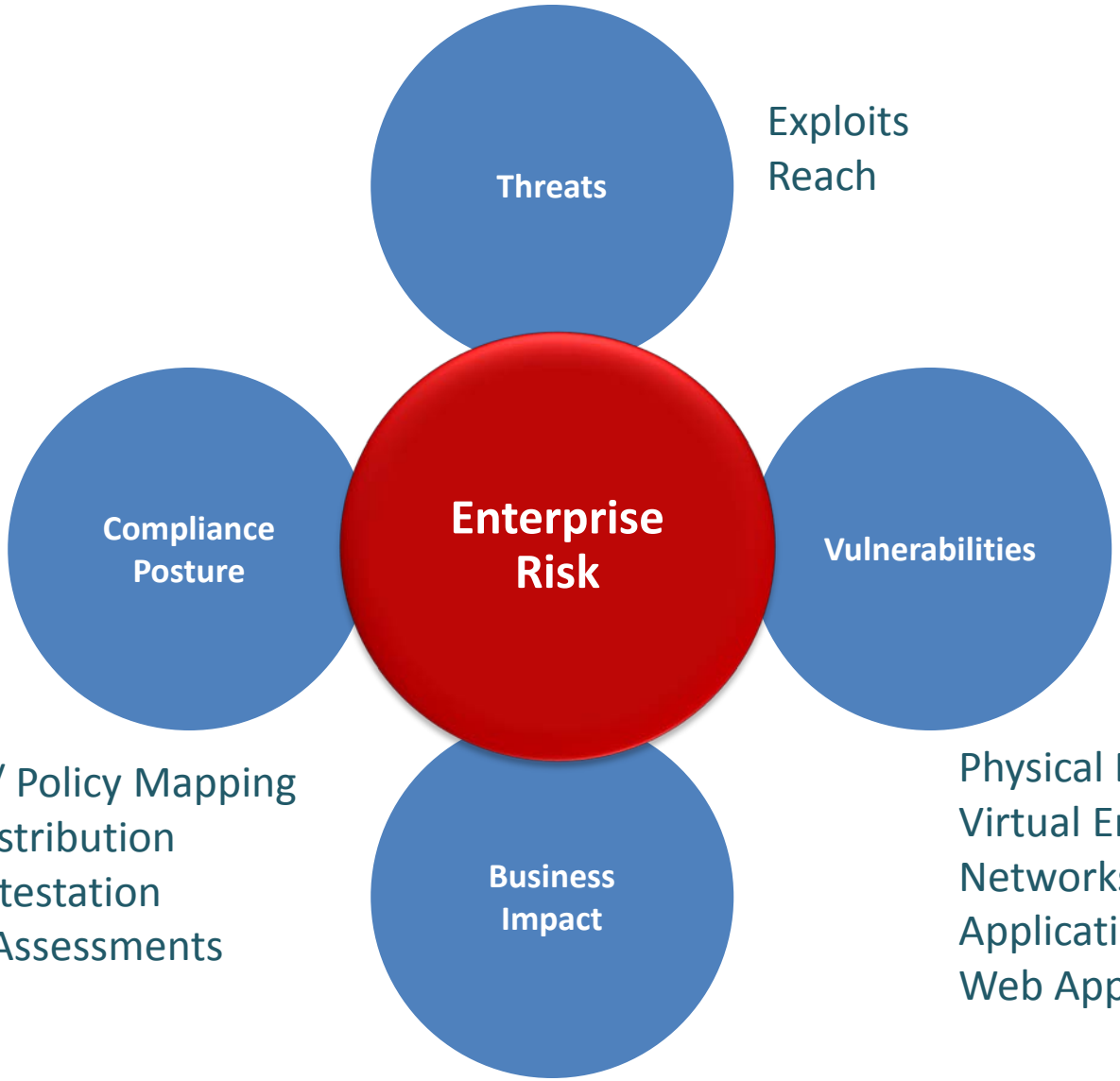


57%

of respondents' organizations use a formal Enterprise Risk Management process or methodology.

Source: The State of the CSO, CSO Magazine, 2011

A Holistic View of Risk



Exploits
Reach

Control / Policy Mapping
Policy Distribution
Policy Attestation
Control Assessments

Physical Environments
Virtual Environments
Networks
Applications
Web Applications

Improving the Odds

"The end goal is improved, risk-based information security decision making based on prioritized, actionable insight derived from the data."

"Pressure solution providers to deliver a context-aware, risk-based view of IT, combining threat intelligence, vulnerability knowledge, compliance and business impact."

– Neil MacDonald, Gartner

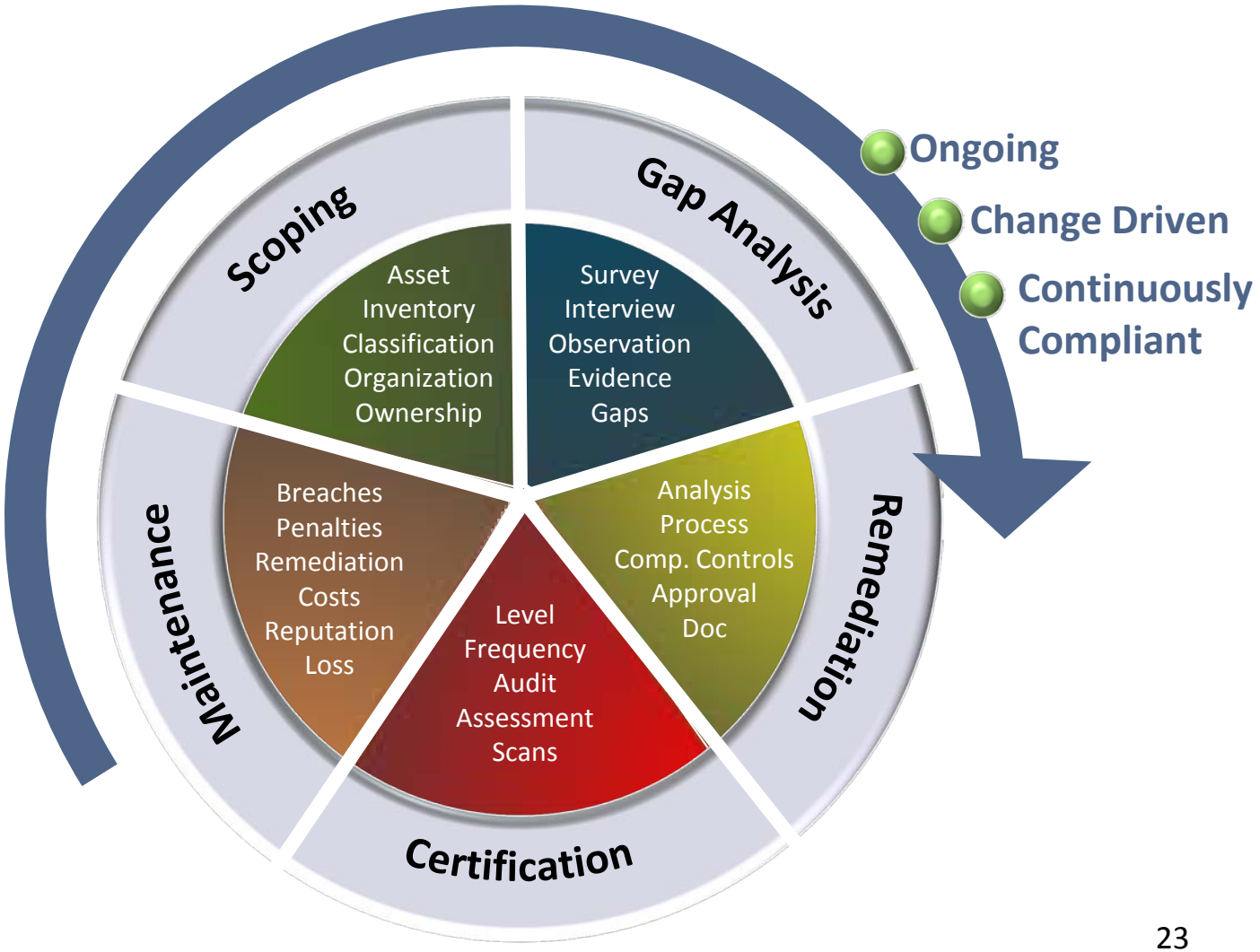
Gartner, "Information Security Is Becoming a Big Data Analytics Problem", by Neil MacDonald, March 2012

ELEMENTS OF RISK-BASED SECURITY

Elements of Risk-Based Security

- Continuous Compliance
- Continuous (Security) Monitoring
- Closed-Looped, Risk-Based Remediation

Continuous Compliance



Continuous Compliance

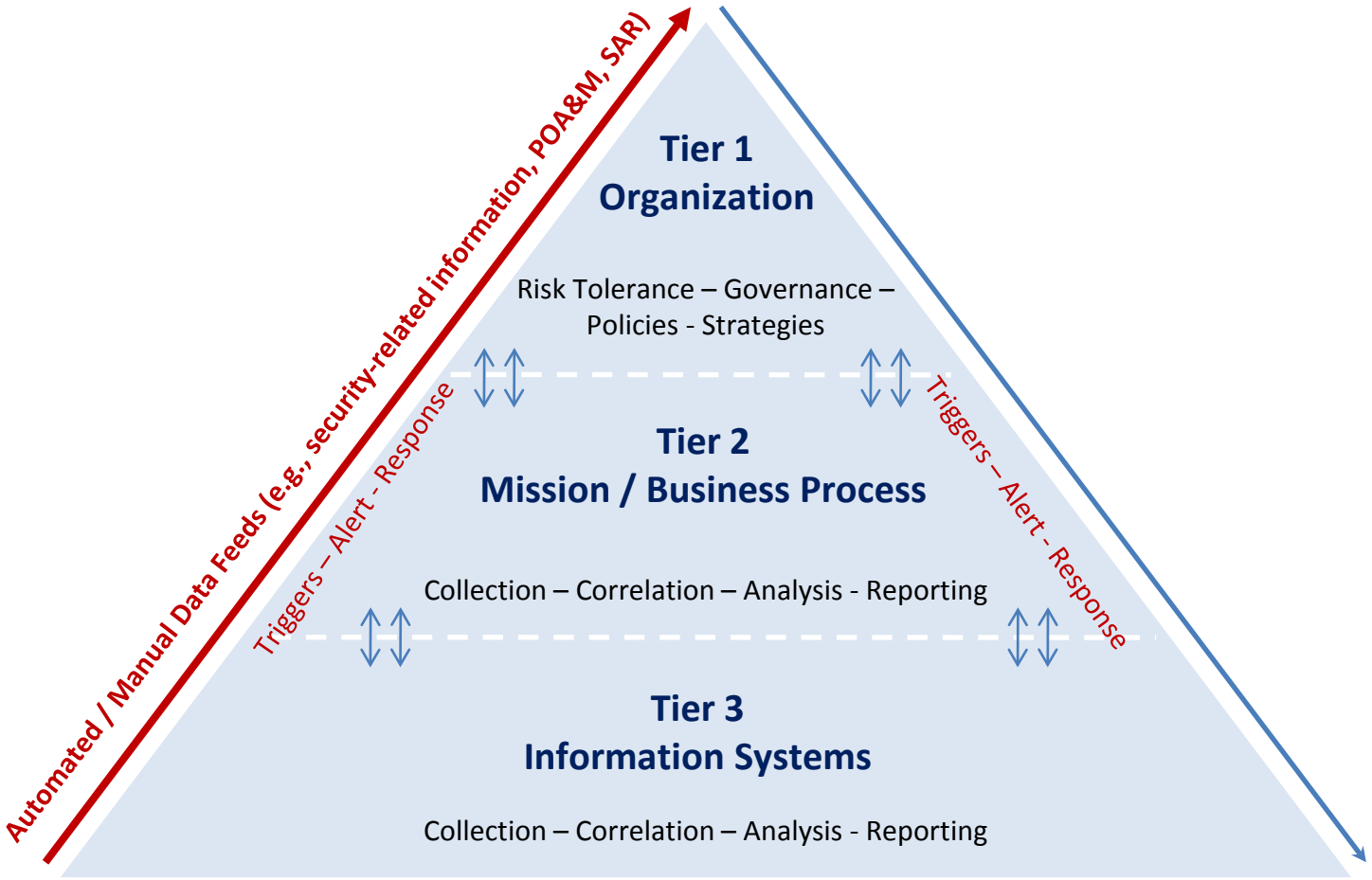
Best Practices

- Use connectors
- Reconcile assets and automate data classification
- Align technical controls
- Automate compliance testing
- Deploy assessment surveys
- Automate data consolidation

Benefits

- Reduces overlap by leveraging a common control framework
- Increases accuracy in data collection and data analysis
- Reduces redundant as well as manual, labor-intensive efforts by up to 75%

Continuous (Security) Monitoring

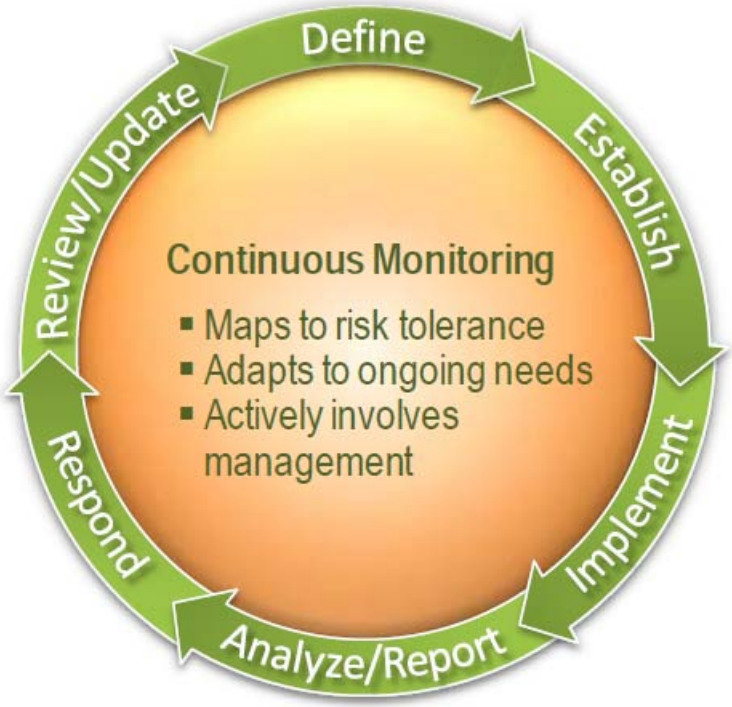


Organization-wide information security continuous monitoring for Federal information systems and organizations, NIST SP 800-137 and NIST SP 800-39

Continuous (Security) Monitoring

Security Automation / Interconnectivity

Closed-Loop Risk Management



Continuous (Security) Monitoring

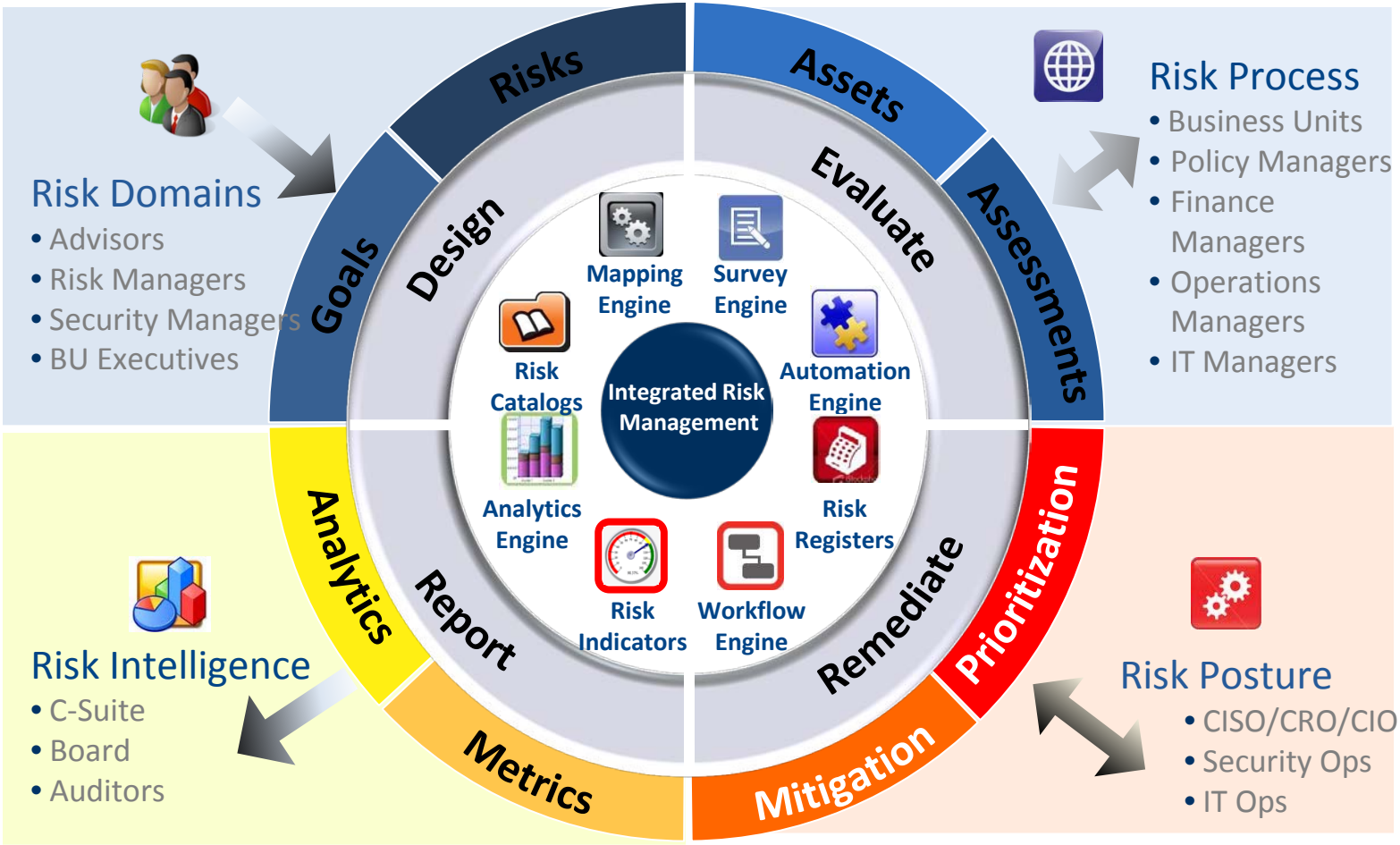
Best Practices

- Implement security automation by aggregating and normalizing data from a variety of sources such as SIEM, asset management, threat feeds, vulnerability scanners
- Increase frequency of data assessment

Benefits

- Reduces cost by unifying solutions, streamlining processes
- Creates situational awareness to expose exploits and threats in a timely manner
- Allows for historic trend data

Closed-Loop, Risk-Based Remediation



Closed-Loop, Risk-Based Remediation

Best Practices

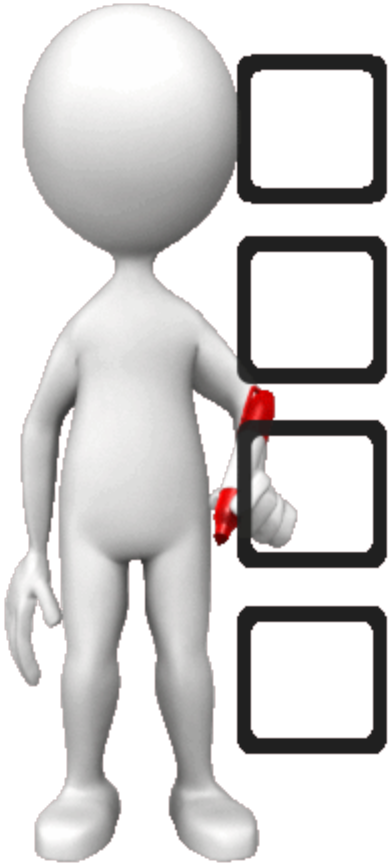
- Subject matter experts within business units define risks catalog and risk tolerance
- Asset classification define business criticality
- Continuous scoring enables prioritization
- Closed-loop tracking and measurement

Benefits

- Increases operational efficiency dramatically
- Improves collaboration between business, security, and IT operations
- Allows to measure security efforts and make it tangible

BENEFITS OF RISK-BASED SECURITY

Benefits of Risk-Based Security



- **Reduce Risk**
- **Reduce Cost**
- **Improve Response Readiness**
- **Provide Risk Posture Visibility**

CASE STUDIES

Case Studies

fiserv.

Financial Services

- Reduced time it takes to produce risk profile from 6 to 3 months , resulting in efficiency savings of up to $500k
- $1 million in overhead savings by automating risk assessment efforts
- Shortened policy controls review process from 4 to 2 months, saving up to $200k
- Increased credibility with board, management, and regulators

Case Studies

Energy

- Improved situational awareness for critical assets, allowing to fulfill NERC CIP and NEI 08-09 regulatory mandates
- Comprehensive vulnerability management program, which reduced time to shut down exploit from 190 days to less than 7 days
- Risk-centric, scalable security operations with 75% reduction in dropped remediation cases

Case Studies

Online Trading

- Consolidation of vulnerability view filtered based on user responsibility to drive resolution ownership and accountability
- Prioritized response based on highest affected assets at the highest criticality level to reduce open vulnerability count consistently over time
- Holistic view of risk, enabling to fulfill OCC mandates, resulting in freeing up funds formerly held in escrow

Thank You

Torsten George

Agiliance Inc.
VP Worldwide Marketing and Products

840 W California Avenue, Suite 240

Sunnyvale, CA 94086

USA

tgeorge@agiliance.com

Visit www.agiliance.com for upcoming webcasts, white papers, and success stories.