MetricStream

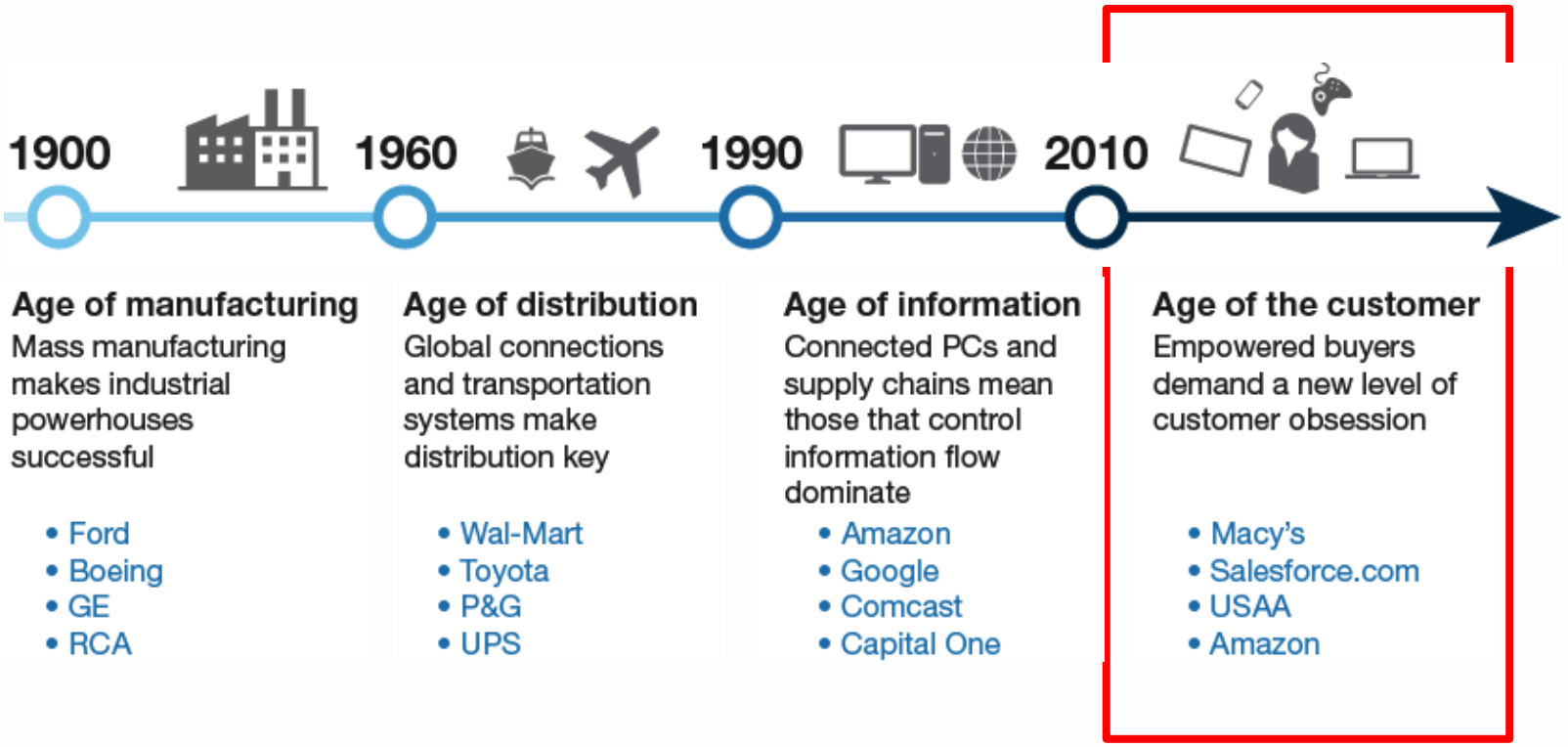
The Convergence of Enterprise, IT and Security Risk Management

Sonal Sinha, CISA, CISM, MBA
Vice President, Industry Solutions
sonalsinha@metricstream.com
MetricStream Inc.

Agenda

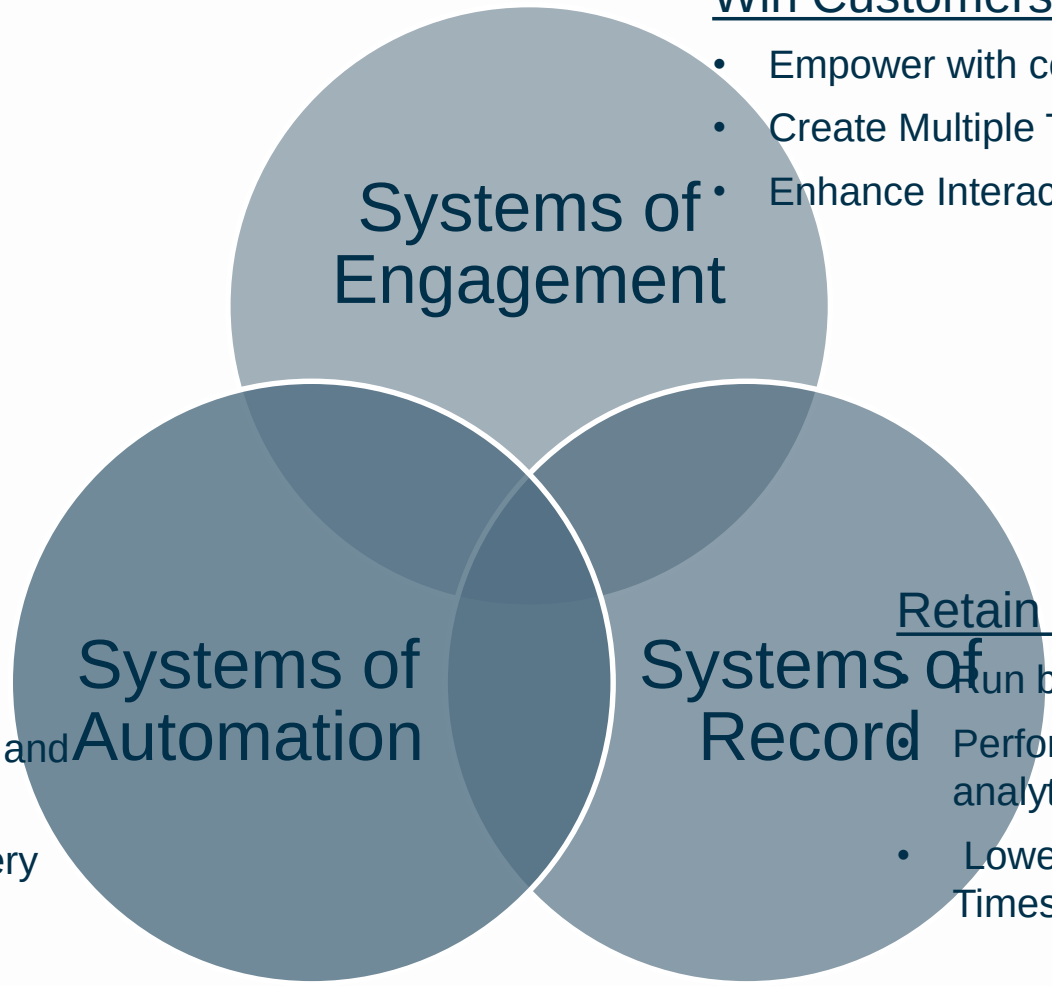
- The Age of the Customer and the New Digital Paradigm
- Why Convergence – Cyber Breaches and Business Continuity
- Trends and Tech Driving Convergence
- What Does Cyber-Business Continuity Convergence Look Like?
- Five Critical Competencies in Orchestrating Convergence
- How Can Technology Support Convergence?
- Summary - Best Practices and Benefits
- GRC Intelligence
- Audience Questions and Discussion

It's the Age of Customer and They are 'Always On'



- *Source: Forrester's October 10, 2013 "Competitive Strategy In The Age Of The Customer" report*

The New Digital Paradigm



Win Customers

- Empower with context-rich apps
- Create Multiple Touch points
- Enhance Interaction experience

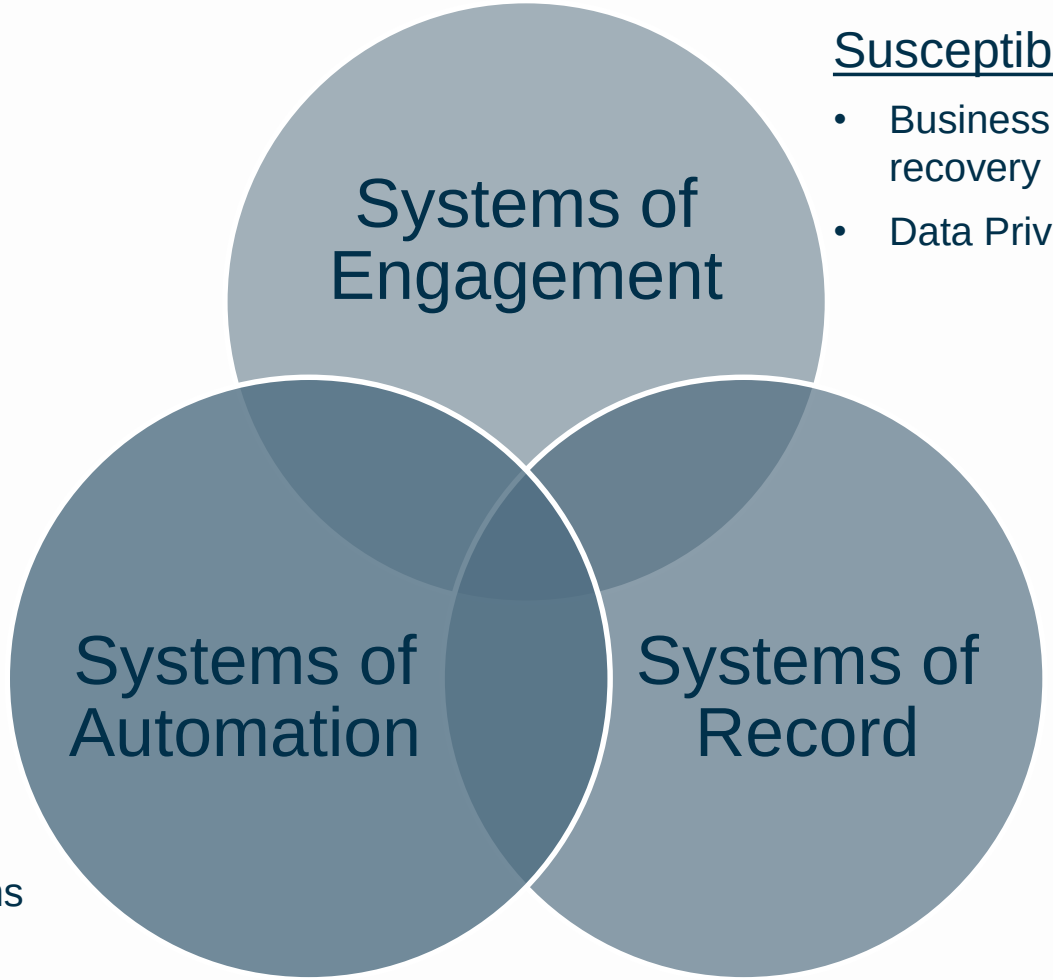
Serve Customers

- Manage physical products, networks, and infrastructure
- Ensure Value Delivery across lifecycle

Retain Customers

- Run business operations
- Perform business analytics
- Lower Value Delivery Times

Risks Across Digital Assets



Susceptible to Data breaches

- Business continuity & Disaster recovery measured in seconds
- Data Privacy & Security

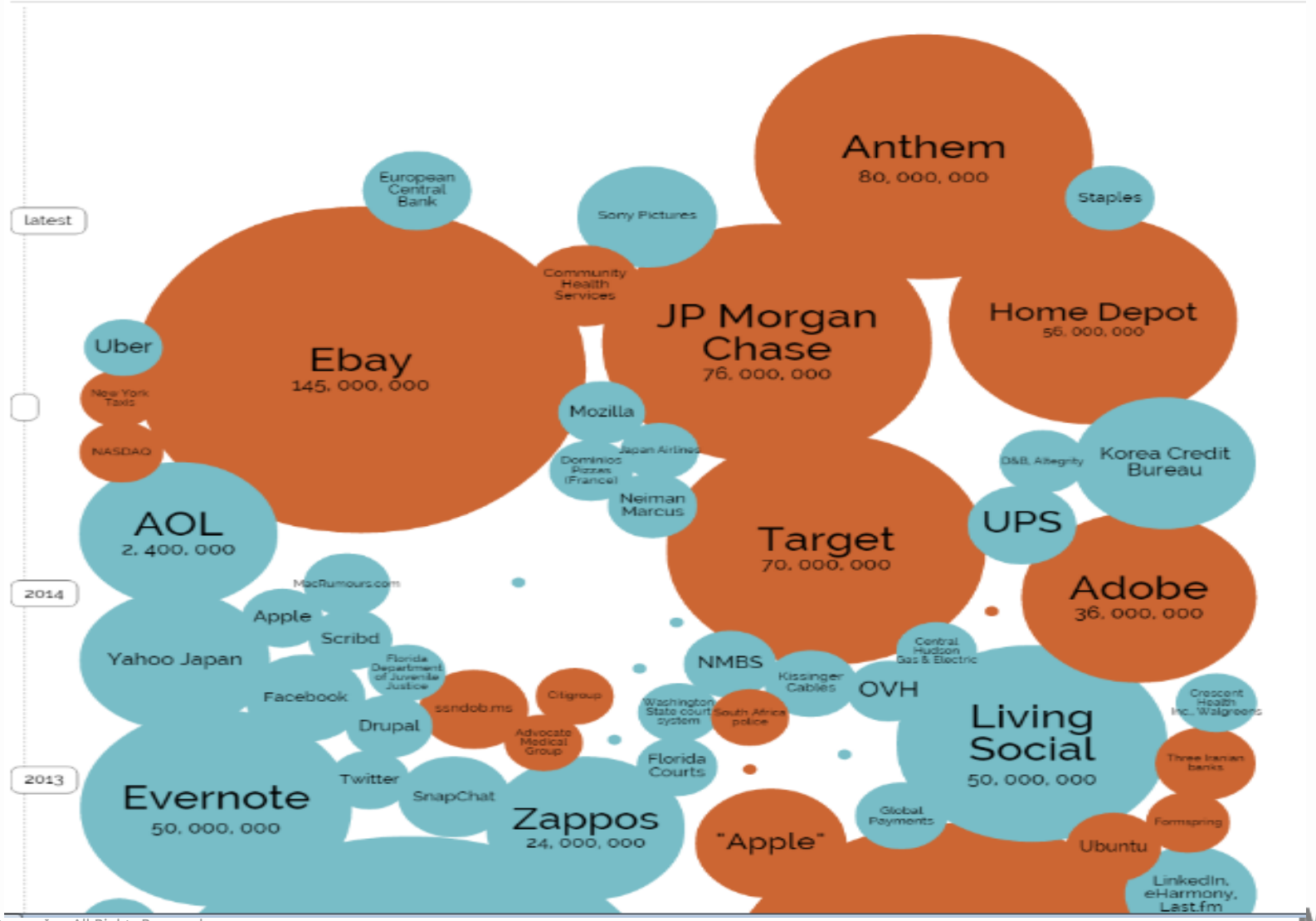
DDoS Attacks

- CSRF
- Sensitive Data Exposure
- Malware and Intrusions

Data Segregation and Access control

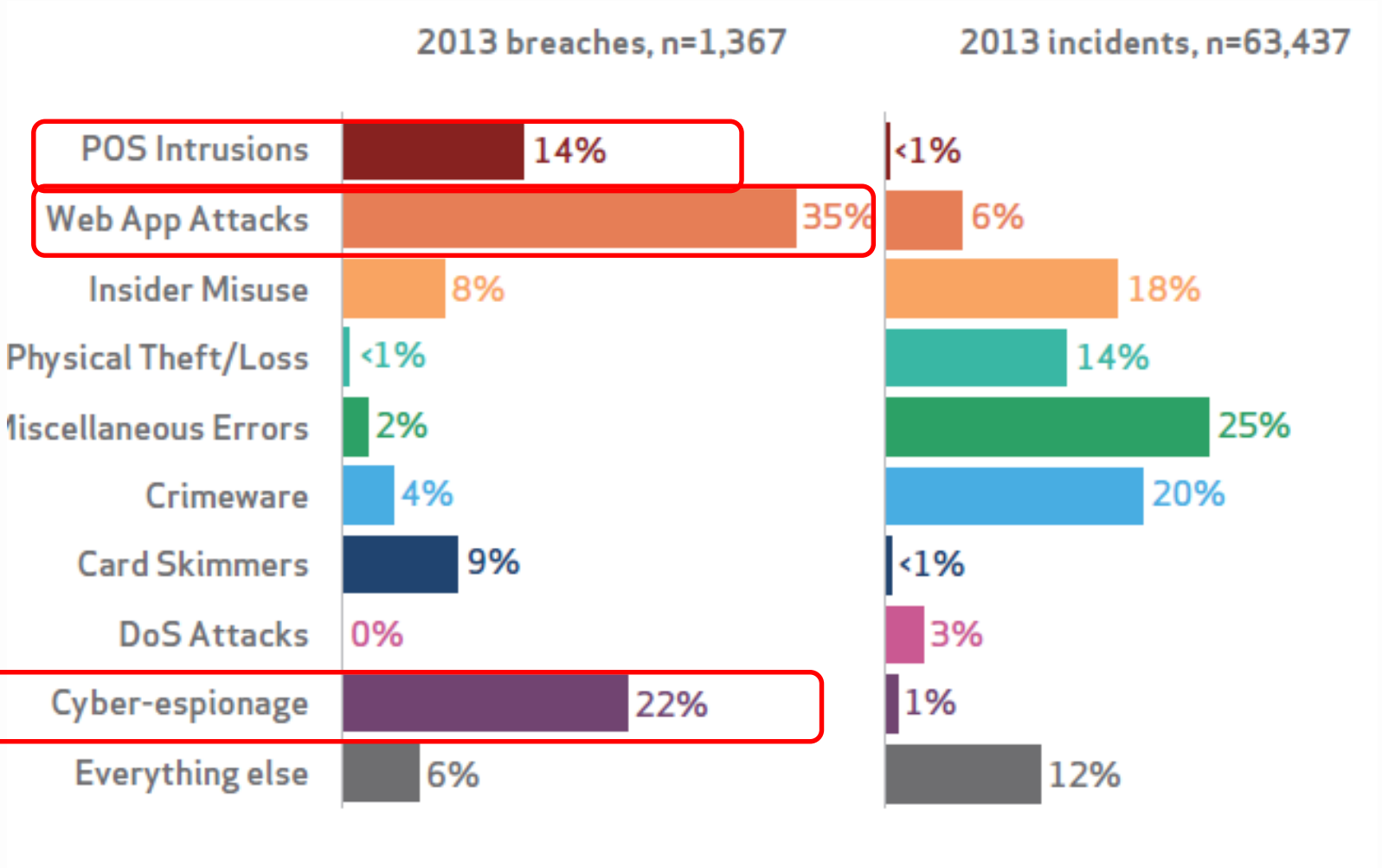
- Segregation of Duties
- Preventive and Reactive Control Monitoring

Cyber Breach Landscape – Not 'If', but 'When'



MetricStream

Top 3 Cyber-Threats disrupting the Business



- *Source: Verizon Data Breach Report 2015*

Cyber Breaches Impact Business Continuity

MetricStream

Business Impacts from Sony Cyber-Attack

Computer Systems Crippled & Network Shutdown for 1 week –

Millions of work hours and costs

Interview Movie Release canceled –

~$120 Million

33,000 documents with PII and SSN leaked–

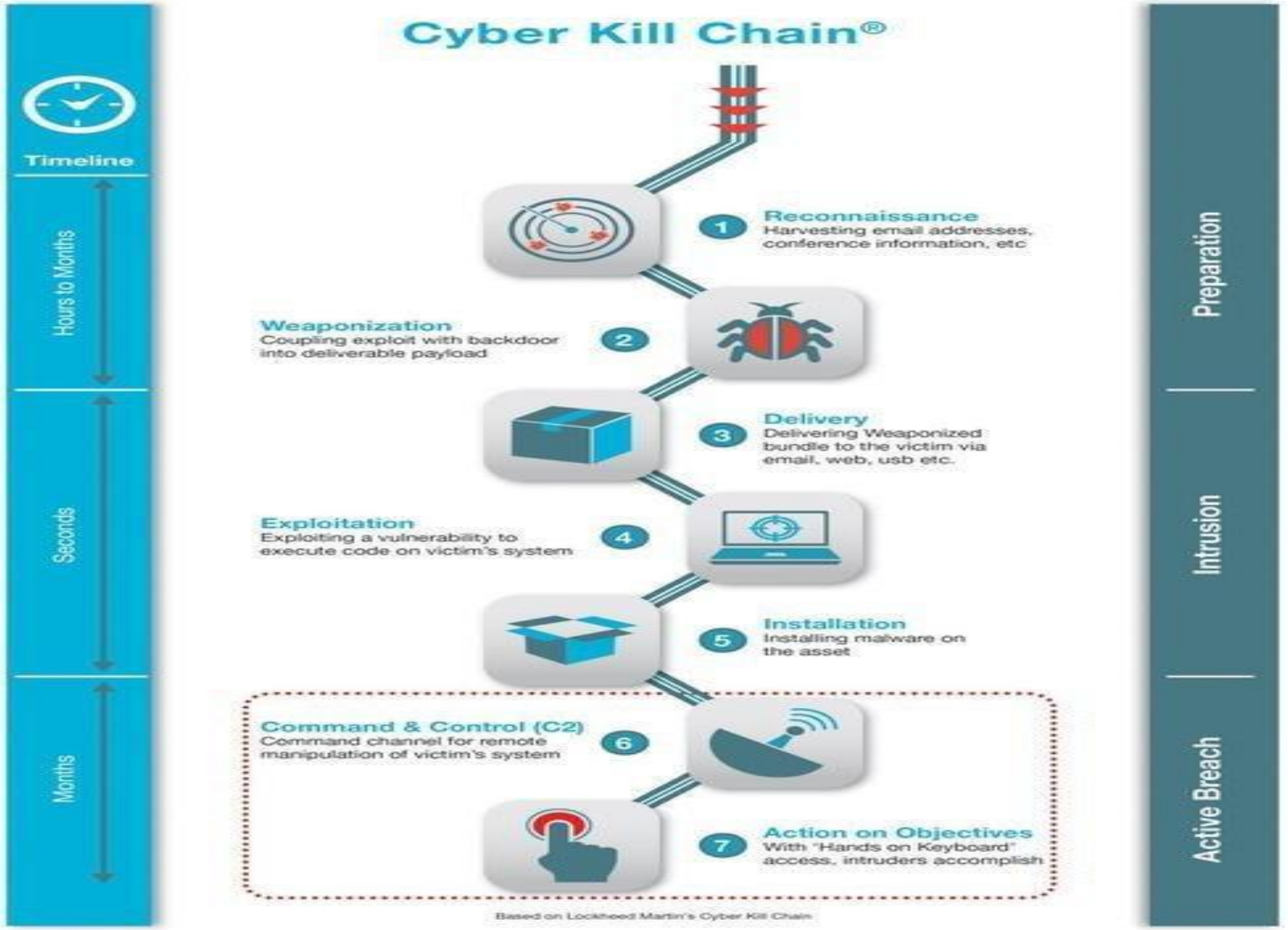
Value Still being Ascertained

Lawsuits by employees & Actors –

Yet to be assessed…

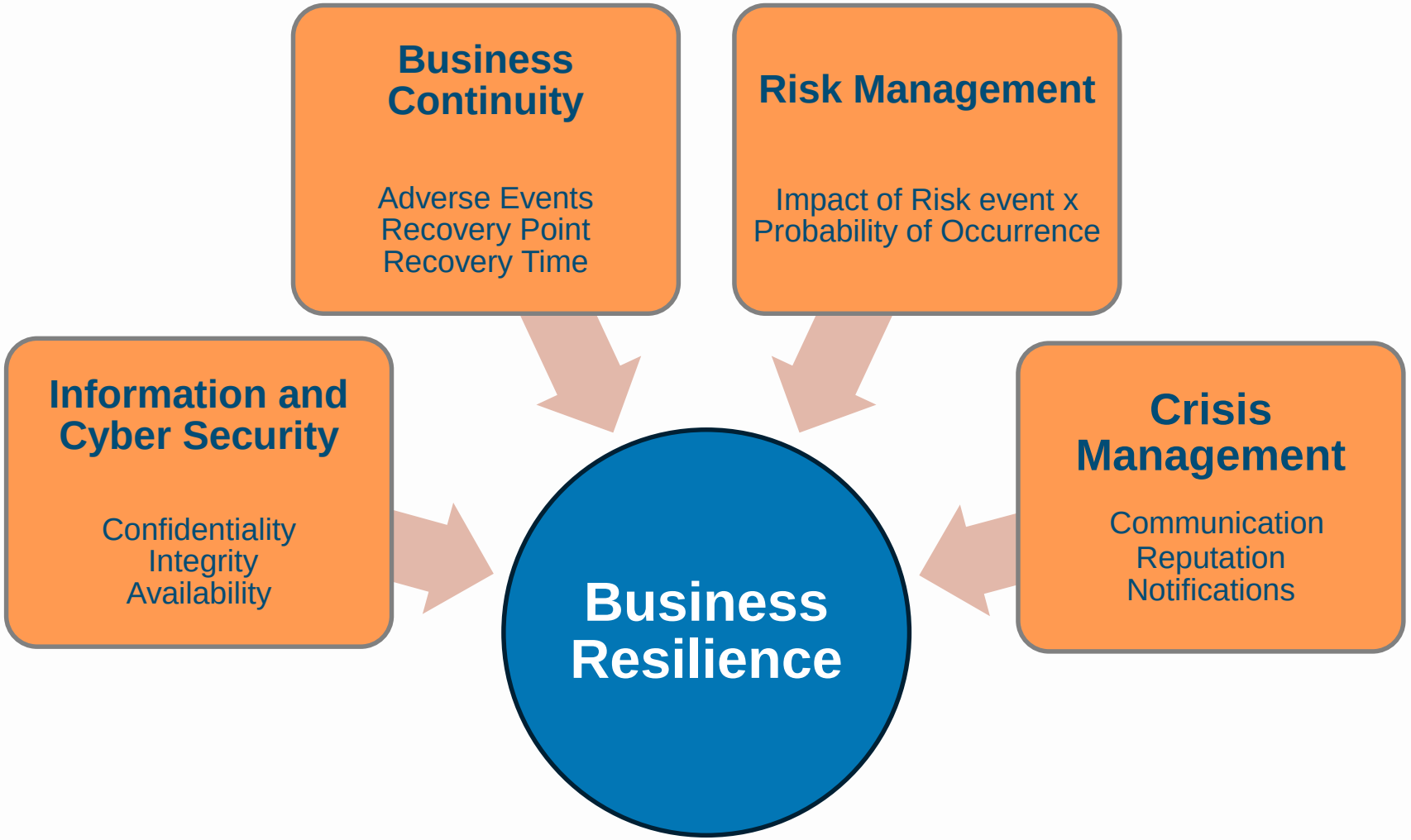
MetricStream

Cyber Security Analysts are Thinking 'Outside-In'



MetricStream

Convergence is Imperative



Trends Driving Convergence

Globalization – Explosion of data, rules, policies, and regulations and risks as organizations extend across countries

Management is demanding a 360 view of risk – size, scale and scope

Tolerance time is shrinking - from hours to minutes to nano-seconds – expectations are high

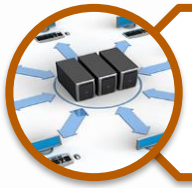
Increasing Coordination - across BC, DR, Crisis Mgmt, PR, Info Sec, Gov't Agencies…3rd Parties

Impacts occur and cascade very quickly - incident can have a ripple effect that expands rapidly

Tech Driving Convergence

Complexity of Information security threats - and the threat surface - are increasing

Hyper-Connectivity – Expansion of employee, vendor and supply chain ecosystem into a real-time collaborative network

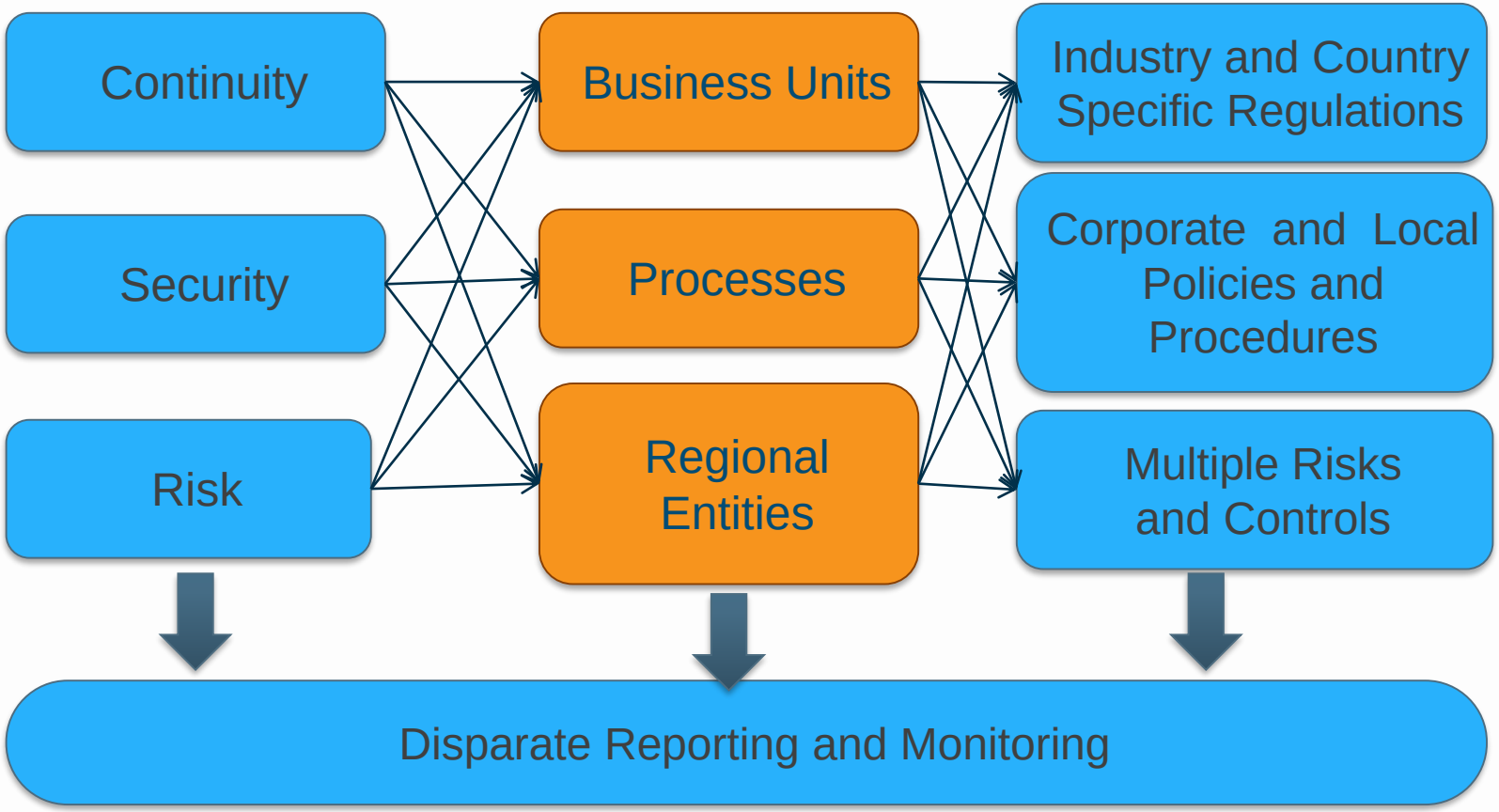


Cloud & Virtualization – Transfer of critical data on cloud for scalability and efficiency to drive the TCO of IT systems lower

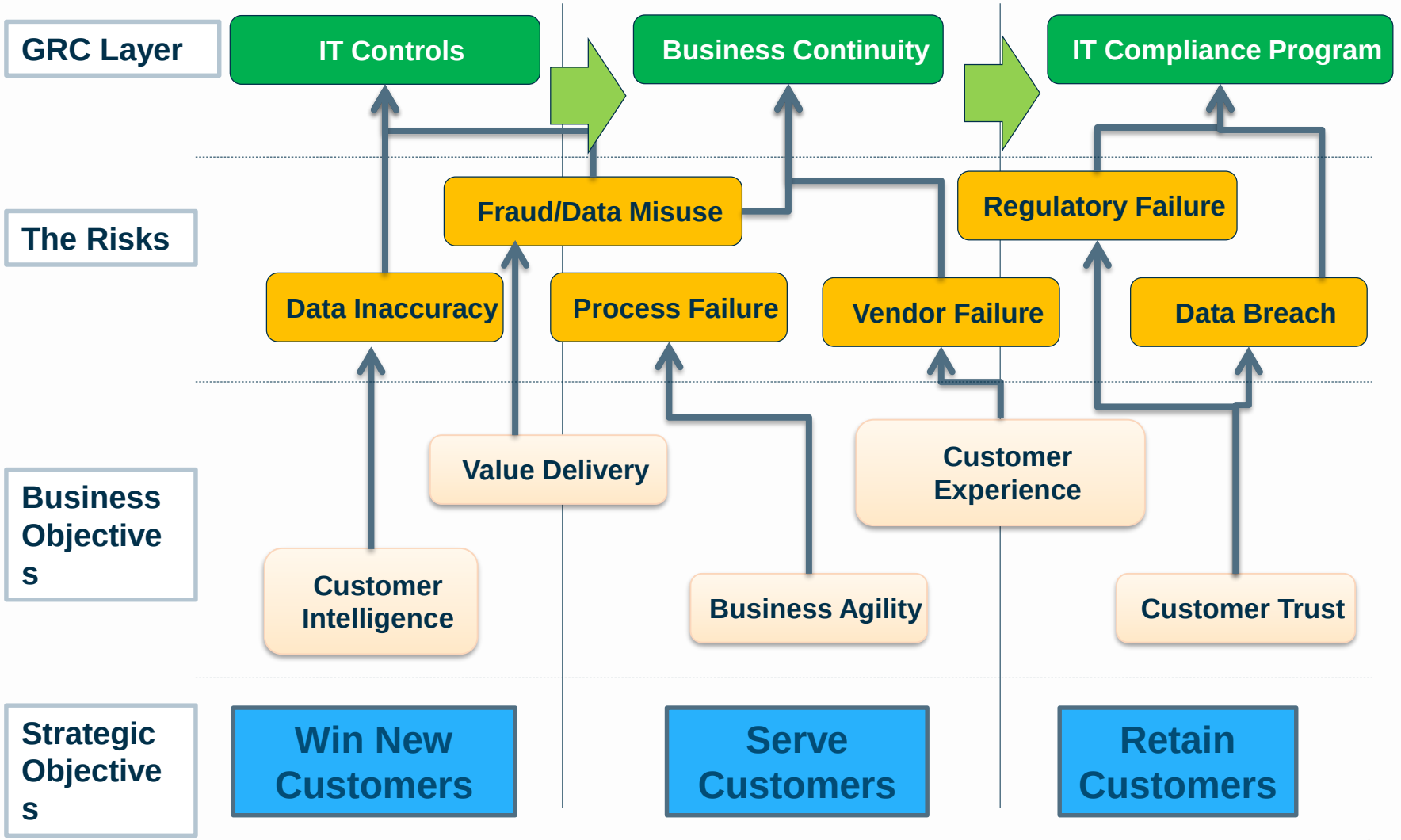
Social Media – New set of imperfect data for real time Risk intelligence, extensive sharing of data and blurring of traditional organization boundaries

Mobility – Ubiquitous access to information and data across devices for employees, customers and partners

Convergence is Challenging



Convergence Requires Competence

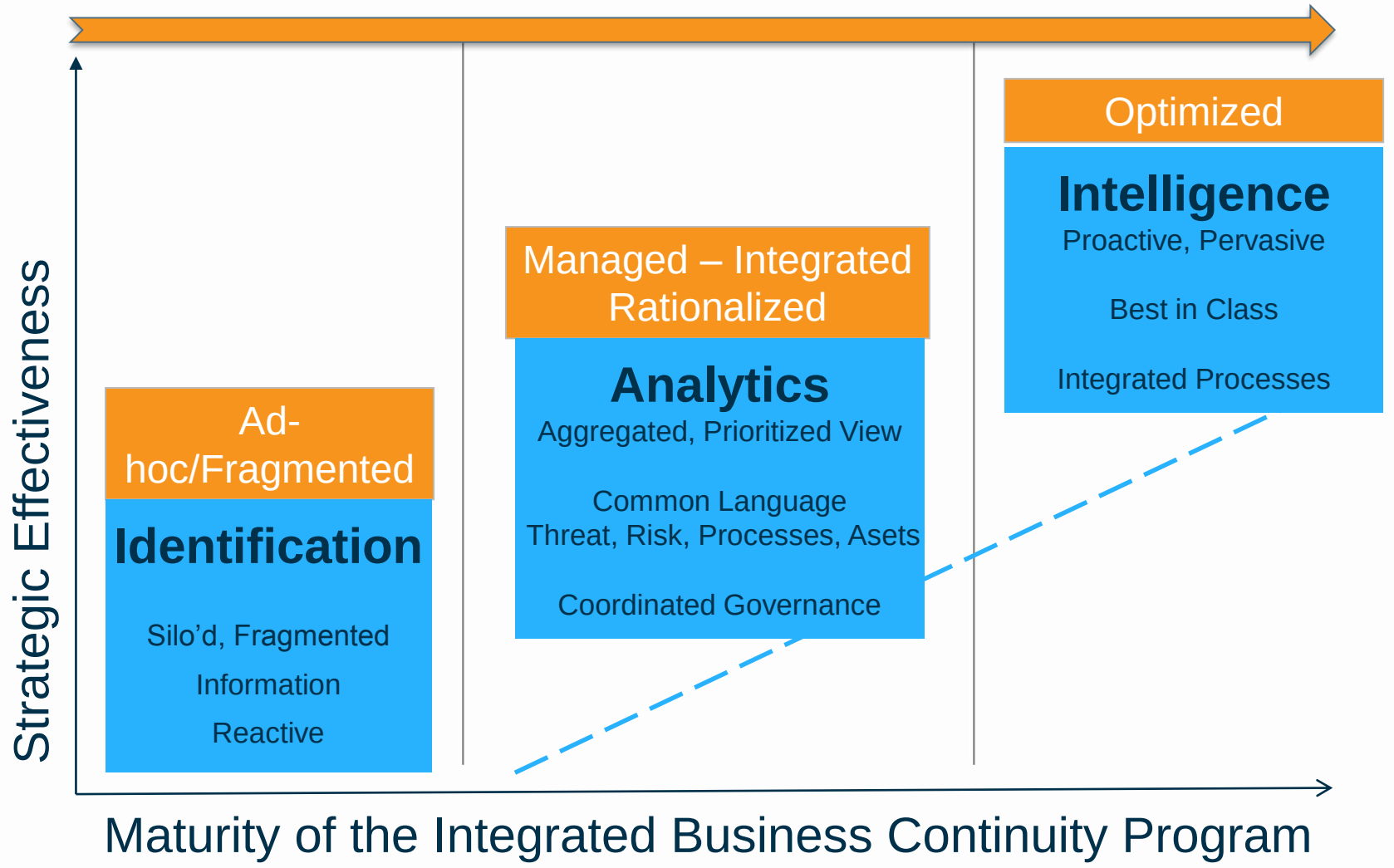


MetricStream

What Does Successful Convergence Look Like?

Discipline	Effective Convergence	Ineffective Convergence
Business Continuity and Response	Highly Responsive to Events Provide Continuity and Resilience Defend against Threats	Reactive to Events Disruption and Loss Defeated by threats
Governance Policy, Procedures Roles	Policy aligned w/desired behaviors Policy aligned with procedures Procedures aligned with roles Empowerment through role clarity	Disconnect between desired behavior and policy Confusion and conflicts Lack of empowerment and action
Risk Management across Enterprise, Operational, IT, Security, 3rd Parties	Clear appetites and thresholds Common Language Proactive view of operational and cyber risk Smart end-end remediation Streamlined controls that mitigate risk	Unclear appetites Confusion on terms Gaps in accountability Partial remediation Problems pushed down the chain Overlapping, conflicting controls
Orchestrating Change and Building Community	Constructive Change Continuous Improvement Community of Innovation Knowledge Management	Reactive to change Loss of productivity Lost opportunity

Maturing the Program – Getting to Intelligence



MetricStream

Critical Competencies in Convergence

MetricStream

Critical Competencies in Convergence

01

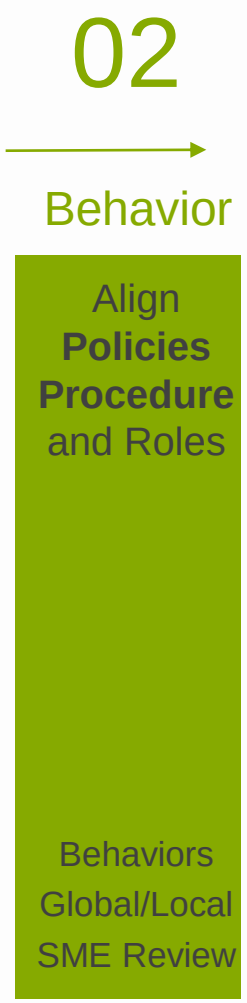
Culture

Create a **Culture of Risk** Awareness

Appetites
Thresholds
Performance

- **What**
  - **Create a risk-aware culture through a formal program: defined and communicated appetites and accountabilities, embedded processes**
  - **Build proactive decision-making across teams: Crisis Management, Business Continuity, Disaster Recovery, Risk and Security/Cyber Teams.**
- **How**
  - **Define Appetites and Tolerances through BIA**
  - **Link Decisions to Performance Goals**
  - **Support the Dialogue with Metrics and Analytics**

Critical Competencies in Convergence



- **What**
  - **Align business strategy and appetites with prescribed behavior, not only through policies, but also through procedures embedded in role descriptions – test, test, test – the empower to act in an event/crisis**
- **How**
  - **Align Policies, Procedures to Business Objectives**
  - **Resolve Global/Local Conflicts in Procedures/Roles**
  - **Engage the right owners/SMEs to create and test**

Critical Competencies in Convergence

- **What**
  - **Use a clear set of terms and federated taxonomies to define what is meant by risk**
  - **Define corresponding calculations to form the basis for meaningful discussions and thresholds/criteria for response**
- **How**
  - **Agree Taxonomies and Definitions**
  - **Provide Context for the Risk – What Process, What Assets, What location, What People**
  - **Align with Automated Monitoring across IT, Security, 3rd Parties**

MetricStream

Critical Competencies in Convergence

- **What**
  - **Create a highly streamlined, end-end incident response and crisis management processes with a 360 view, tied to risks, people, processes, assets**
- **How**
  - **Manage issues and incidents as a portfolio**
  - **Develop a proactive preventive capability**
  - **'Right-Size' Remediation investments**
  - **Use technology to coordinate across groups and 3rd Parties, Emergency Responders, Vendors, Gov't Authorities**

Critical Competencies in Convergence

05

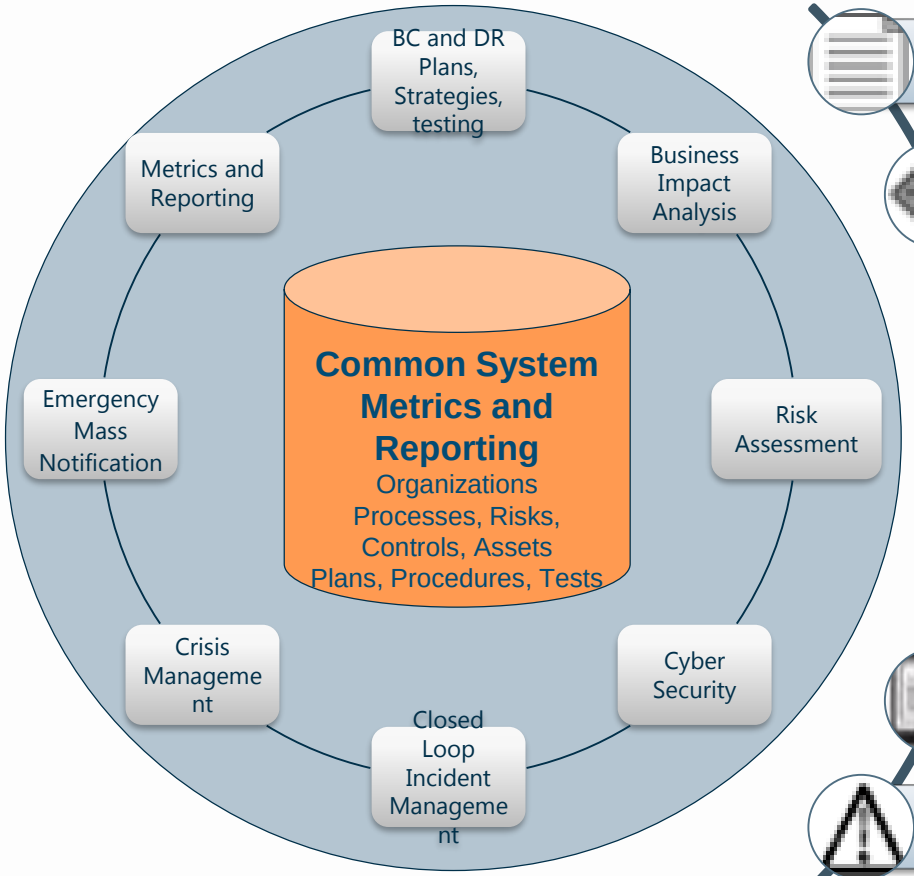
Orchestration

Orchestrate Change Across Processes

Community
Innovation
Improvement

- **What**
  - Create Convergence as a competency by orchestrating change that will create continuous value, spot opportunities for operational efficiencies, identifies synergies, funds strategic initiatives and certification programs
- **How**
  - **Build a Community dedicated to the vision of Convergence in Business Continuity, Risk Management, Cyber Security, Crisis Management**
  - **Mature the Program to Achieve 'Intelligence'**
  - **Continuously Improve**

How Can Technology Support Convergence?

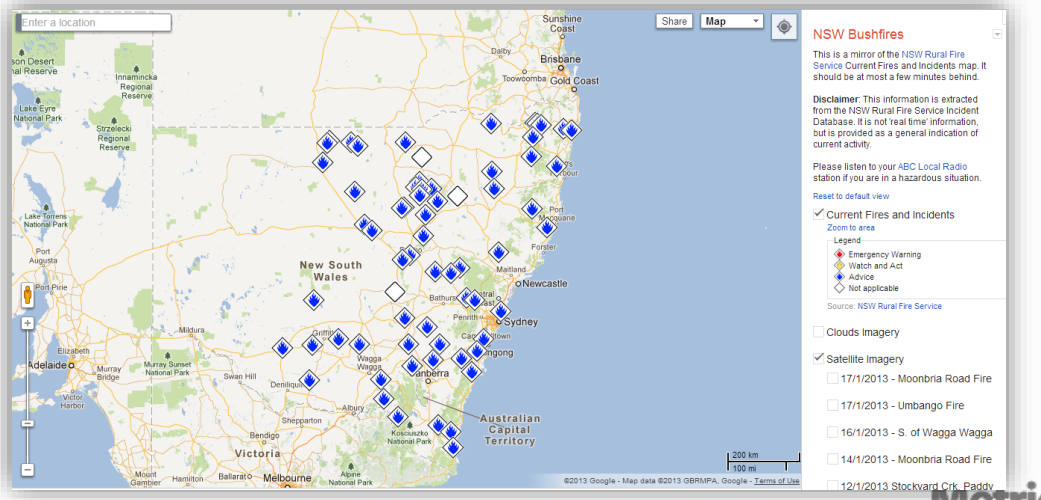


Key Features and Functions

- **BC Plans and Strategies, Testing** – BC Plans, Disaster Recovery Plans, mapped to policies, best practices
- **Business Impact Analysis** – RPO RTO MTPD, mapped to business org, process and assets
- **Risk Assessment**- Centralized library of risks, controls, assessment workflow, KRIs
- **Cyber Security** - Threat and Vulnerability
- **Closed loop Issue and Incident Management** - follow up actions, remediation & review
- **Crisis Management** – Establish authority and control, communication and coordination
- **Emergency Mass Notification** – notification through SMS, Voice Mail etc.

How Can Social Media Support Convergence?

- Track Social Media platforms like:
  - Twitter
  - Facebook
  - Pinterest
  - Google (Google +, Youtube, Crisis Map etc.)
- Correlate Information with Organizational Assets / Facilities / Risks
- Trigger / Update Incident Management Workflows & Notifications
- Real-Time Reports & Dashboards
- Leverage Social Media for Communications During Emergencies



MetricStream

How Can GRC Content Support Convergence

Knowledge Mosaic
ComplianceOnline
The Largest GRC Advisory Network
State Net
DATA.GOV
Corporate Risk Solutions
CLEAR Market Practices
Code of Federal Regulations
DOW JONES
LexisNexis
SHESHUNOFF | PRATT
INFORMATION SERVICES
SHARED ASSESSMENTS
IT UCF

Regulatory Feeds

News Feeds

Risk/Control Libraries

grc intelligence.com

Curate

- Regulatory Changes & Alerts
- Risk and control libraries updates
- Geo-political news

MetricStream
GRC Platform

Apps
- Regulatory Change Mgmt.
- Third-Party Mgmt.
- IT-GRC

Libraries
- Regulations
- Geographic Entities
- Processes
- Controls

Energy & Utilities

Hi-Tech & Manufacturing

Banking & Financial Services

Healthcare & Pharmaceutical

Retail

MetricStream

Summary – 8 Best Practices for Convergence

1. **Universe** - Consider the end-end eco-system, 3rd parties and suppliers

2. **Planning** - Be Objective and honest, look at all angles, question access and think about what you are allowing into your environment

3. **Language** - Develop a common nomenclature for scenarios, use cases and threat landscapes

4. **Community** - Collect and develop better information about attack vectors, impact achieved by adversaries, and threat agents

5. **Prepare for emerging cyber threats** - Perform a shift in Business, technology and security controls to accommodate them

6. **Test** - Integrate tests and exercises across Business Continuity, Disaster Recovery, Security and Crisis Management programs

7. **Technology** - Leverage a common Governance, Risk and Business Continuity Planning platform, with an asset inventory, and risk and control framework

Summary – 9 Benefits of Convergence

1. **Risk-Aware Culture:** evolving to proactive risk intelligence
2. **Risk:** A broader view of risk and treatment based on real appetites
3. **Common Language:** An common policy, risk, control and mitigation framework
4. **Threats:** A 360, proactive view of evolving threats and risks
5. **Eco-system:** A clearer, integrated understanding of products and services, and the processes, assets and the resources that support them
6. **Resilience**: A more proactive, resilient capability to support and protect the business
7. **Response**: Pragmatic procedures to responding on-the-ground challenges
8. **Systems:** Coordinated, integrated systems for orchestrating, monitoring and managing risk
9. **Prioritization and Investment** – effective investment in remediation

About MetricStream

Vision

Integrated Governance, Risk and Compliance for Better Business Performance

Solutions and Applications

- Risk Management
- Business Continuity Management
- IT GRC
- Compliance Management
- Audit Management
- Supplier Governance
- Quality Management
- EHS & Sustainability
- Governance & Ethics
- Content and Training

Partners

KPMG, Infosys, hp, NetIQ, IT UCF, Qualys, Deloitte., pwc, TATA CONSULTANCY SERVICES, WhiteHat SECURITY

Organization

- Over 1,500 employees
- Headquarters in Palo Alto, California with offices worldwide
- Over 350 enterprise customers
- Privately held – backed by leading global VCs, Goldman Sachs, Sageview Capital

Differentiators

- Technology - GRC Platform – 9 Patents
- Breadth of Solutions – Single Vendor for all GRC needs
- Cross-industry Best Practices and Domain Knowledge
- ComplianceOnline.com - Largest Compliance Portal on the Web

Product Leadership

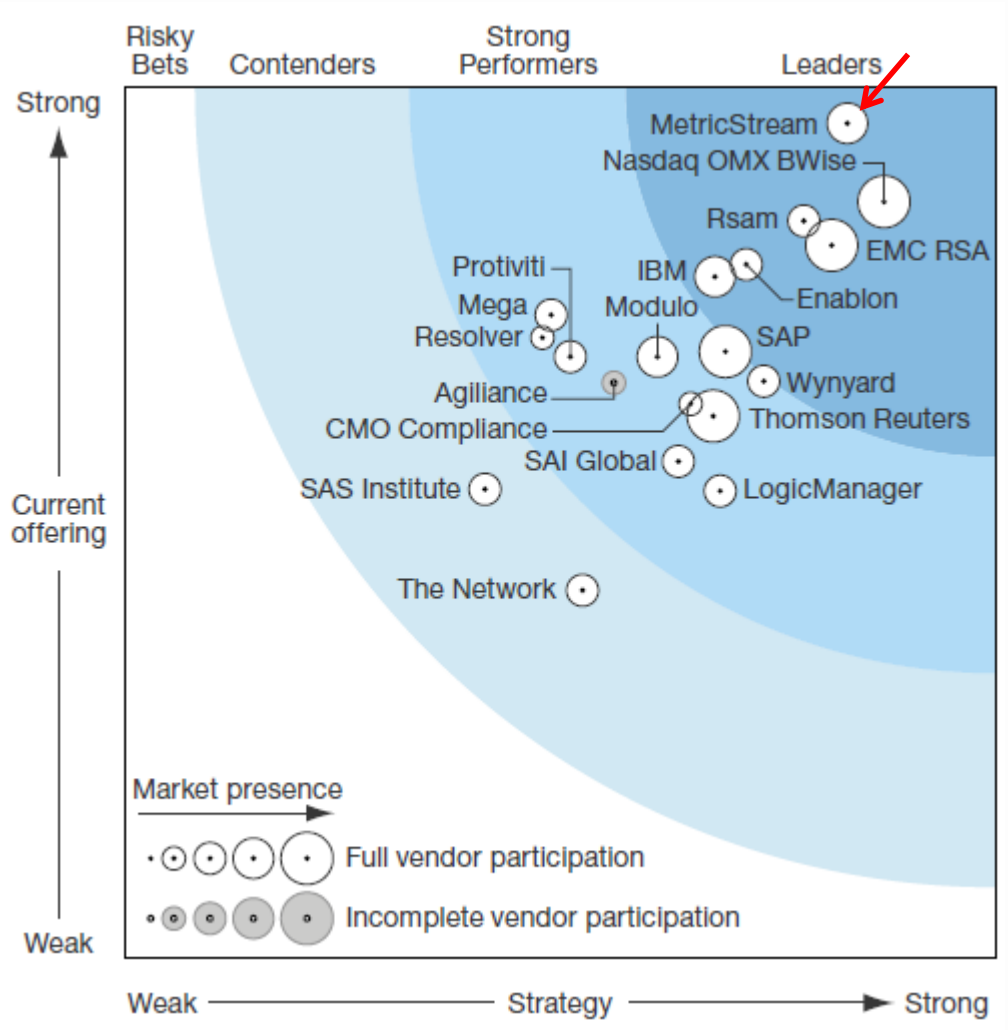
Gartner

Leader in BCM Magic Quadrant 2014

Gartner

Leader in IT Vendor Risk Management Magic Quadrant for 2014

Product Leadership – A Disruptive Force



FORRESTER®

"MetricStream's fast growth is a disruptive force in the market."

Highest score for Current Offering criteria for strength of product offering and capabilities

- Forrester Wave™: GRC Platforms, Q1 '14

Thank You
Q&A

Contact Us:

Website: www.metricstream.com | **Email:** webinar@metricstream.com

Phone: USA +1-650-620-2955 | UAE +971-5072-17139 | UK +44-203-318-8554

MetricStream