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’

1900 1960 1990 2010

Age of manufacturing
Mass manufacturing makes industrial powerhouses successful
- Ford
- Boeing
- GE
- RCA

Age of distribution
Global connections and transportation systems make distribution key
- Wal-Mart
- Toyota
- P&G
- UPS

Age of information
Connected PCs and supply chains mean those that control information flow dominate
- Amazon
- Google
- Comcast
- Capital One

Age of the customer
Empowered buyers demand a new level of customer obsession
- Macy's
- Salesforce.com
- USAA
- Amazon

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 Touchpoints
  - Enhance Interaction experience

- **Systems of Engagement**
- **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

- **Systems of Record**
- **Systems of Automation**
Risks Across Digital Assets

Systems of Engagement

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

Data Segregation and Access control
- Segregation of Duties
- Preventive and Reactive Control Monitoring

DDoS Attacks
- CSRF
- Sensitive Data Exposure
- Malware and Intrusions

Systems of Automation

Systems of Record
Cyber Breach Landscape – Not ‘If’, but ‘When’
Top 3 Cyber-Threats disrupting the Business

- **POS Intrusions**: 14%
- **Web App Attacks**: 35%
- **Insider Misuse**: 8%
- **Physical Theft/Loss**: <1%
- **Miscellaneous Errors**: 2%
- **Crimeware**: 4%
- **Card Skimmers**: 9%
- **DoS Attacks**: 0%
- **Cyber-espionage**: 22%
- **Everything else**: 6%

**Source:** Verizon Data Breach Report 2015
Cyber Breaches Impact Business Continuity

GoDaddy takes down half the Internet

US markets crippled by Nasdaq outage

What The Sony Hack Can Teach About Cyber Security

Health Insurer Anthem Struck By Massive Data Breach
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…
Cyber Security Analysts are Thinking ‘Outside-In’

Cyber Kill Chain®

1. Reconnaissance: Harvesting email addresses, conference information, etc.
2. Weaponization: Coupling exploit with backdoor into deliverable payload
3. Delivery: Delivering Weaponized bundle to the victim via email, web, usb etc.
4. Exploitation: Exploiting a vulnerability to execute code on victim’s system
5. Installation: Installing malware on the asset
6. Command & Control (C2): Command channel for remote manipulation of victim’s system
7. Action on Objectives: With “Hands on Keyboard” access, intruders accomplish

Timeline

Intrusion

Preparation

Active Breach

Based on Lockheed Martin's Cyber Kill Chain
Convergence is Imperative

- **Business Continuity**
  - Adverse Events
  - Recovery Point
  - Recovery Time

- **Risk Management**
  - Impact of Risk event \( x \)
  - Probability of Occurrence

- **Information and Cyber Security**
  - Confidentiality
  - Integrity
  - Availability

- **Crisis Management**
  - Communication
  - Reputation
  - Notifications

**Business Resilience**
**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

- Continuity
- Security
- Risk
- Business Units
- Processes
- Regional Entities
- Industry and Country Specific Regulations
- Corporate and Local Policies and Procedures
- Multiple Risks and Controls

Disparate Reporting and Monitoring
## What Does Successful Convergence Look Like?

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

**Maturity of the Integrated Business Continuity Program**

- **Ad-hoc/Fragmented Identification**
  - Silo’d, Fragmented Information
  - Reactive

- **Managed – Integrated Rationalized Analytics**
  - Aggregated, Prioritized View
  - Common Language
  - Threat, Risk, Processes, Assets
  - Coordinated Governance

- **Optimized Intelligence**
  - Proactive, Pervasive
  - Best in Class
  - Integrated Processes

**Strategic Effectiveness**
Critical Competencies in Convergence

01 Core Competencies

Culture

Create a Culture of Risk Awareness
Appetites, Thresholds, Performance

02 Behavior

Align Policies, Procedure, and Roles
Behaviors, Global/Local SME Review

03 Language

Speak a Common Language
Taxonomies, Context, Monitoring

04 Incidents

Gain an Extended Enterprise View
360 View, Preventive Remediation

05 Innovation

Orchestrate Change Across Processes
Community, Innovation Improvement
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

02

Behavior

- 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

03

Language

• 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
  • Align with Automated Monitoring across IT, Security, 3rd Parties
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

• **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, KRIIs
- **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.

Common System Metrics and Reporting
Organizations, Processes, Risks, Controls, Assets, Plans, Procedures, Tests
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
How Can GRC Content Support Convergence

MetricStream GRC Platform

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

Libraries
- Regulations
- Geographic Entities
- Processes
- Controls

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

News Feeds

Risk/Control Libraries

Energy & Utilities
Hi-Tech & Manufacturing
Banking & Financial Services
Healthcare & Pharmaceutical
Retail
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
![Partners Logos]

## 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

Leader in IT Vendor Risk Management Magic Quadrant for 2014
“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