

# Academic Engagement In Supply Chain Best Practice Development

Dr. Sandor Boyson, Director, Supply Chain Management Center

- Key Academic Engagement Processes:
  - **Capturing Consensus Best Practices** through survey research, expert interviews and specialist focus groups.
  - **Transferring Best Practice Sets** into MBA/MS curriculum, software and teaching tools.

# 1. Capturing Supply Chain Best Practices

- Business & technology practices are continuously adapting to operational volatility.
- Standards are becoming more elusive... like trying to catch bullets in flight.
- Academia can help accelerate/crystalize community consensuses around supply chain best practice sets.
- Academia can help update practice sets frequently based on data from ongoing effectiveness studies.

# **The Cyber Supply Chain Risk Management Portal**

Crystalizing consensus best practices

- **Cyber- SCRM (CSCRM) combines enterprise risk management, supply chain management and cyber security into a fusion discipline.**
- **This discipline is aimed at gaining visibility and control over the end to end operations (facilities, people and processes) that integrate hardware, software and network connectivity into systems.**

# Why Is Cyber Supply Chain Risk Management Best Practices Development So Urgent?

- Symantec's 2013 Internet Security Threat Report, based on its network monitoring across 157 countries, found that the supply chain is the latest threat vector:

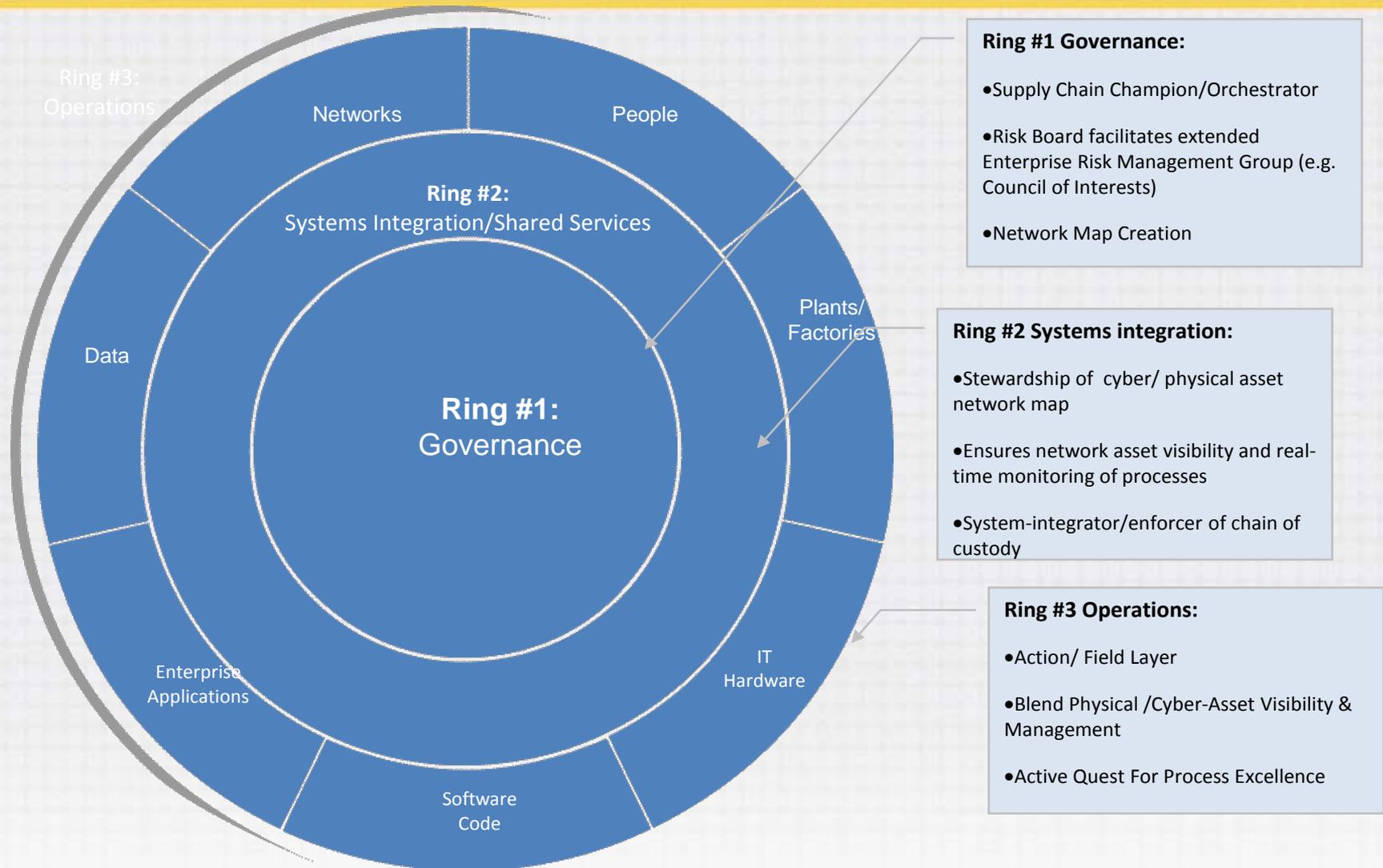
**“Manufacturing Sector and Knowledge Workers Become Primary Targets:** Shifting from governments, manufacturing has moved to the top of the list of industries targeted for attacks in 2012. Symantec believes this is attributed to an increase in attacks targeting the supply chain – cybercriminals find these contractors and subcontractors susceptible to attacks and they are often in possession of valuable intellectual property. Often by going after manufacturing companies in the supply chain, attackers gain access to sensitive information of a larger company” [12].

- The composite losses from attacks on the IT supply chain are staggering. The Chairman Of The U.S. House of representatives Intelligence Committee, Mike Rogers, a former FBI agent, revealed that *the combined losses from cyber attacks on U.S. enterprises was an estimated trillion dollars in lost revenue and 10,000 jobs lost in 2013*
- In response to these losses, the Security & Exchange Commission (SEC) has given guidance that publically traded companies need to disclose cyber risks in their SEC filings that are “material” e.g. threaten 10% or more of revenue. Over 2,000 disclosures have been made.

# Crystallizing CSCRm Best Practices: Our Research History

- The Supply Chain Management Center of the R.H. Smith School Of Business has been engaged in a multi-phase research project for the Information Technology Lab of NIST focusing on helping identify and define the emerging practices & standards of supply chain risk management for information systems.
- Currently in its fifth phase, the project has previously surveyed over 200 IT vendors of the federal government; interviewed over 100 experts; mapped over 60 public and private standards & practice initiatives; and created a set of portal-based enterprise assessment tools for organizations that have been field tested by 180 companies.
- To bring users into the design process, we created a portal advisory group that included NIST, DHS, the Open Group, TM Forum (an association of over 800 telcom vendors) and the National Electronics Manufacturing Association (NEMA).

# Cyber-SCRM: A Holistic Model



# Our CSCRMM Portal's Mission

-Our Cyber SCRM portal has been sponsored by the National Institute Of Standards & Technology and directly incorporates the latest NIST standards and practices.

-This portal is highly secure and enables an organization to **anonymously** share data.

-An organization can assess its capabilities in IT Security and Supply Chain Risk Management against a dynamic set of benchmark standards and practices.

-The portal enables comparing an organization against its industry peers to gain practical insights into improving CSCRMM capability/maturity levels.

The screenshot shows the CyberChain portal homepage. At the top, there are fields for Username and Password, and a LOGIN button. The CyberChain logo is prominently displayed. Below the logo, there are navigation links for Home, Register, and Cyber Alerts & News. The main content area features a section titled "Our Value To You" with three paragraphs describing the portal's benefits for Federal Agencies, IT Vendors, and U.S. publicly traded companies. To the right of this text is a large image of a US dollar bill. Below the "Our Value To You" section, there is a red button labeled "TAKE THE ASSESSMENT". Underneath this button, there are three interactive cards: 1) A map of the United States with a network overlay, titled "Evaluate your readiness with scenario based mapping tools." 2) A card with a blue background and a white line graph, titled "How prepared is your organization? Take part in our risk assessments tools." 3) A card with a blue background and a white line graph, titled "Calculate your risk maturity capability." At the bottom of the page, there is a section titled "Cyber News & Alerts" with a list of recent security updates from Google, Apple, and Adobe. A "More" link is located at the bottom right of the page.

# The Portal's Business Value

- **If you are a federal agency:** our assessment tools enable rapid diagnosis of IT supply chain “trouble spots” and areas for improvement based on NIST guidelines
- **If you are an IT vendor to the federal sector:** our tools enable you to document the scope of your IT supply chain management activities based on NIST guidelines to include in responses to Agency RFPs.
- **If you are a publically traded company:** our tools might help you obtain broader or cheaper cyber security insurance coverage by documenting information security controls, an historical record of performance and active management of your cyber risk profile

# Our Tool Kit

## Risk Scoring Your IT Supply Chain

- If you complete our enterprise assessment, your organization will receive an Aggregate Risk Score that factors in governance, network design, systems management and cyber-risk disclosure/ insurance data.
- This Score rates your IT Supply Chain’s riskiness : its exposures and susceptibility to attacks along the chain and your operating distance from current best practice.
- Our Risk Scoring is based on the latest NIST standards/ practices (as contained in the President’s Executive IT Risk Framework & Supply Chain Risk Management Special Publications), as well as consensus community practices.

FUNCTION		Your points earned	Total possible points	% of extent of coverage of attributes
IDENTIFY	Asset Management Business Environment Governance Risk Assessment Risk Management	56	60	93.3%
PROTECT	Access Control Awareness and Training Data Security Info Protection Processes Protective Technology	68	98	69.4%
DETECT	Anomalies and Events Security Continuous Monitoring Detection Processes	19	22	86.4%
RESPOND	Communications Analysis Mitigation	14	16	87.5%
RECOVER	Improvements Communications	14	14	100%

### Executive IT Risk Intelligence Score

You earned 74% or less of possible total points in each Function. Your company has received a Grade C and does not meet the performance threshold. To improve your score, consider building these core capabilities and strategies as described in the table below.

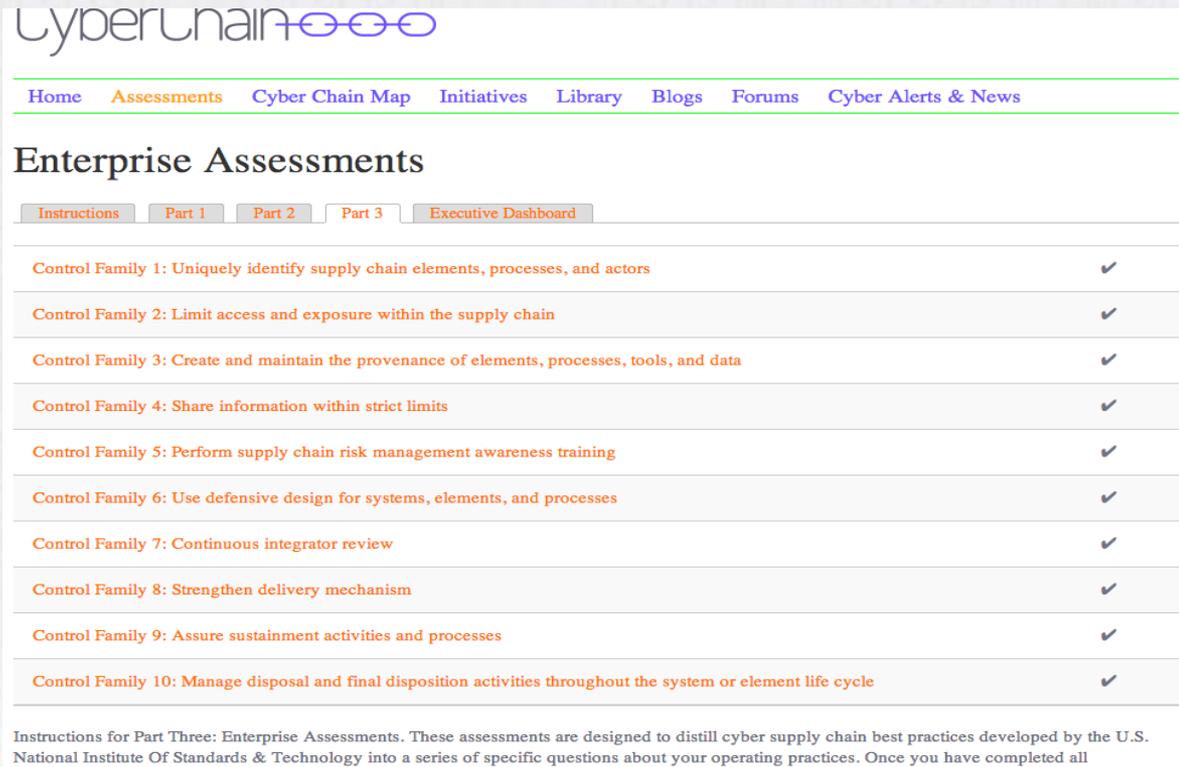
### Building Core Capabilities & Strategic Improvements

Function	Build these Core Capabilities	Consider these Strategic Improvements
PROTECT	Hardening Defensive IT Processes/Procedures	1) Tighten credential management for devices and users 2) Enforce physical access control for critical IT infrastructure 3) Toughen configuration change controls for organizational systems 4) Protect wired and wireless networks through better security planning
DETECT	Conducting Real Time, Continuous IT Systems' Monitoring	1) Establish baseline of "normal" organizational behaviors and expected data flows 2) Utilize network traffic analysis and malicious code detection mechanisms to identify and characterize anomalies and events 3) Perform periodic vulnerability scanning, penetration testing and access control log audits to check for possible breaches
RESPOND	Analyzing Breaches/Incidents & Allocating Resources To Mitigate Their Impacts	1) Formalize policy, procedures, practice and coordination to implement agreed upon mitigation actions in response to cyber security events 2) Conduct forensics in order to classify the incident and uncover root causes

# NIST Control Families (CFs)

Control families represent the basic units of operational assessment.

Each control family is an organizing principal under which a specific set of cyber security and supply chain interventions are grouped. Each of the ten control families has an associated set of assessment questions



The screenshot shows the CyberChain website interface. At the top, the logo "CyberChain" is displayed with a chain-link icon. Below the logo is a navigation menu with links: Home, Assessments, Cyber Chain Map, Initiatives, Library, Blogs, Forums, and Cyber Alerts & News. The main heading is "Enterprise Assessments". Below this heading is a sub-navigation bar with tabs: Instructions, Part 1, Part 2, Part 3 (selected), and Executive Dashboard. The main content area lists ten control families, each with a description and a checkmark in the right margin, indicating completion. The descriptions are: Control Family 1: Uniquely identify supply chain elements, processes, and actors; Control Family 2: Limit access and exposure within the supply chain; Control Family 3: Create and maintain the provenance of elements, processes, tools, and data; Control Family 4: Share information within strict limits; Control Family 5: Perform supply chain risk management awareness training; Control Family 6: Use defensive design for systems, elements, and processes; Control Family 7: Continuous integrator review; Control Family 8: Strengthen delivery mechanism; Control Family 9: Assure sustainment activities and processes; Control Family 10: Manage disposal and final disposition activities throughout the system or element life cycle. At the bottom, there is a note: "Instructions for Part Three: Enterprise Assessments. These assessments are designed to distill cyber supply chain best practices developed by the U.S. National Institute Of Standards & Technology into a series of specific questions about your operating practices. Once you have completed all

# Our Tool Kit

## Mapping Your IT Supply Chain's Key Hubs & Nodes

-Our **First Of Its Kind Mapping Tool** can determine the vulnerability of key hubs and nodes in your IT supply chain

-It is based on industry-leading **CVSS standards** and enables your team to make expert judgments on the criticality and fragility of your hubs & nodes.

-The mapping tool ensures privacy with a strong emphasis on stripping away geo-locational identifiers to anonymize user data.

### Supply Chain Map

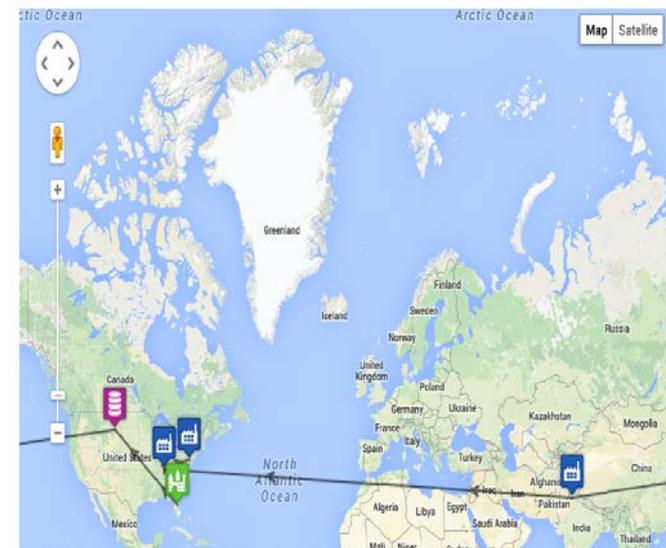
Total # of Transactions: 4  
Total Possible Risk: 40  
Actual Risk Score: 1.7

Total # of Nodes: 5  
Total Possible Risk: 50  
Actual Risk Score: 1.5

Supply Chain Risk Score: 6.2

[What does this score mean?](#)

[+ Back to Dashboard](#)



# Our Tool Kit

- **Cyber Risk Insurability Analysis**

- Our partner, Beecher Carlson, is one of the largest insurance brokers in the world and a pioneer in analyzing the Security & Exchange Commission's database of corporate cyber security risk disclosures,

- In-built calculators will determine your organization's extent of cyber risk exposures as compared to industry peers.

# Challenges In Best CSCRМ Practices Development

- Long maturation period for identification of consensus practices.
- Need multiple data points to track emergence/diffusion of practices( surveys, field work, etc).
- Still no clear evidence- despite claims-on actual effectiveness of best practices in achieving business or IT security goals.
- Despite difficulties, academia can play a key role in negotiating consensus on best practice sets and in advocating for effectiveness studies.

## II. Transferring SCRM Best Practices Into Graduate Education

- Transferring best practices into graduate education requires partnering with industry to expose students to the most advanced tech platforms and managerial processes.
- Universities must commit to adapt/customize industry databases and training programs to succeed in an educational environment.
- See Resilinc example that follow

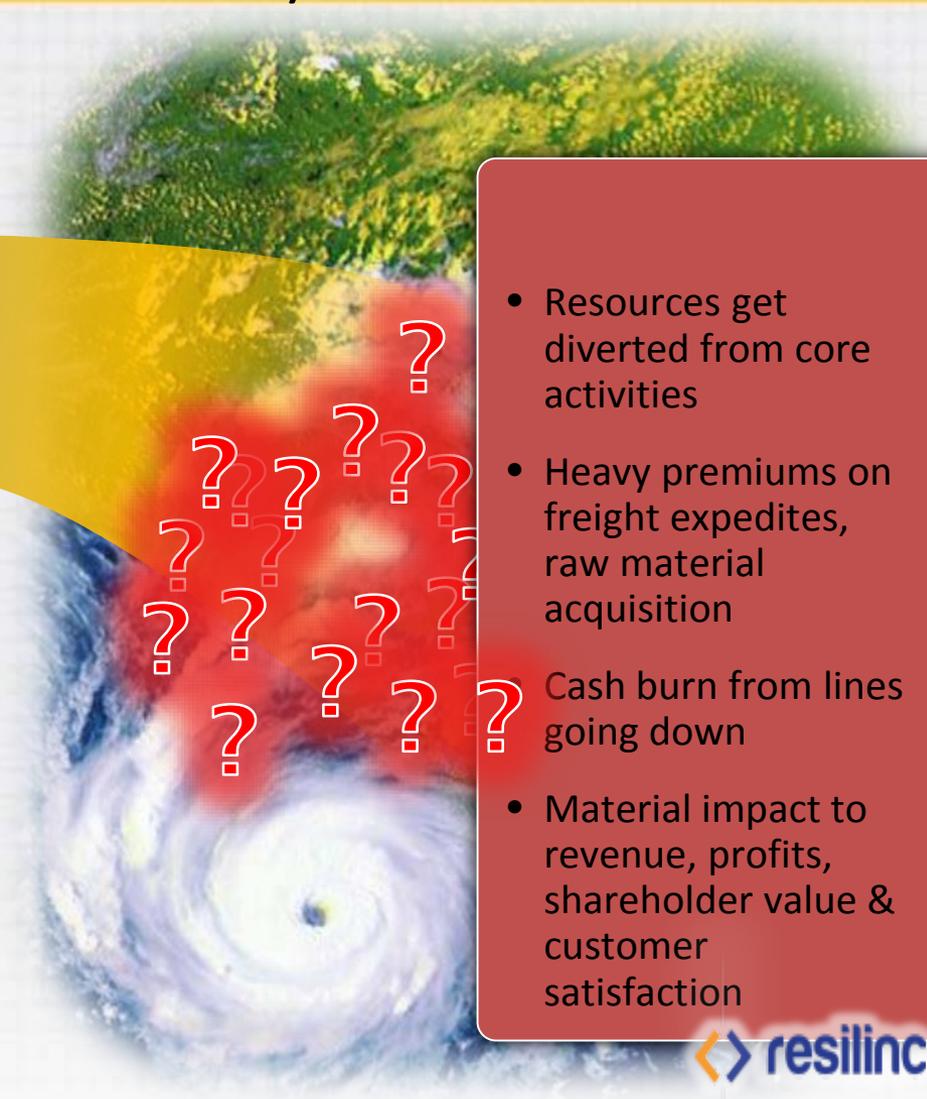
**Resilinc:**  
Transferring Best Risk Practices  
Into Graduate Education

Accelerating the training of next generation leaders

# Limited Visibility Into Supply Base & Slow Reaction to Disruptions = Need for Supply Chain Resiliency



Order ID	Order Type	Status	Date	Location
0123	Order	Shipped	10/12/12	01545
0124	Order	Shipped	10/12/12	01545
0125	Order	Shipped	10/12/12	01545
0126	Order	Shipped	10/12/12	01545
0127	Order	Shipped	10/12/12	01545
0128	Order	Shipped	10/12/12	01545
0129	Order	Shipped	10/12/12	01545
0130	Order	Shipped	10/12/12	01545
0131	Order	Shipped	10/12/12	01545
0132	Order	Shipped	10/12/12	01545
0133	Order	Shipped	10/12/12	01545
0134	Order	Shipped	10/12/12	01545
0135	Order	Shipped	10/12/12	01545
0136	Order	Shipped	10/12/12	01545
0137	Order	Shipped	10/12/12	01545
0138	Order	Shipped	10/12/12	01545
0139	Order	Shipped	10/12/12	01545
0140	Order	Shipped	10/12/12	01545



- Resources get diverted from core activities
- Heavy premiums on freight expedites, raw material acquisition
- Cash burn from lines going down
- Material impact to revenue, profits, shareholder value & customer satisfaction

# Investments in Supply Chain Resiliency Drive Proactive and Efficient Response



## resilinc



- Resources continue to focus on core activities
- Reduced instances of RM premiums & freight expedites
- Reduced lines down situations
- Prevent negative impact to financials, brand & customer satisfaction

# About Resilinc

The world's biggest repository of supplier, site, part and multi-tier intelligence...

Centralized Data  
Repository

SalesForce.com  
Solution

Supplier  
Onboarding



Supply Chain Risk Management



Supply Chain Event Monitoring



Conflict Minerals



Corporate Social Responsibility



Business Continuity Planning



# Resilinc's Approach To Enabling Resilient Supply Chains

## Plan

- **MAP** Suppliers and Parts across Multiple Tiers
- **QUANTIFY** Single Points of Failure
- **PRIORITIZE** Resources & Budget for Mitigation

## Protect

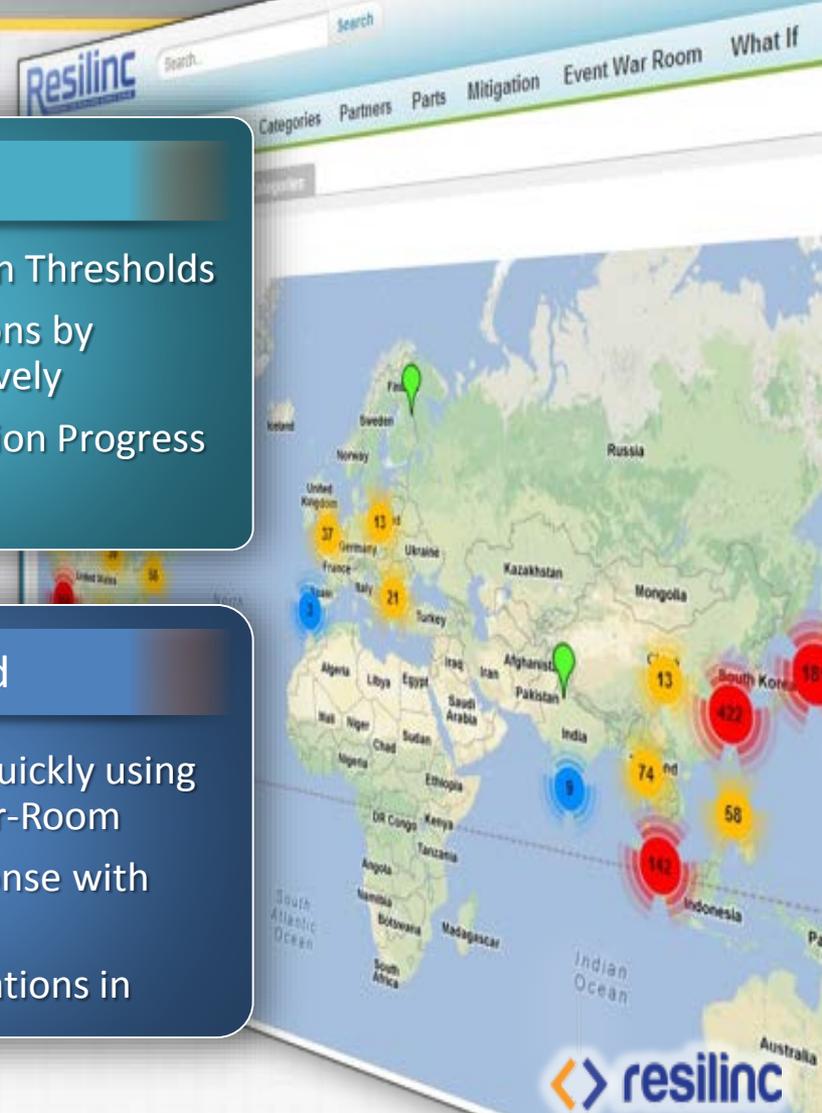
- **ACCEPT** Risk within Thresholds
- **MANAGE** Exceptions by Mitigating Proactively
- **MEASURE** Mitigation Progress over Time

## Sense

- **MONITOR** Global Events 24x7
- **RESEARCH** event to determine scale and size
- **NOTIFY** customers based on Impact

## Respond

- **ASSESS** Impact Quickly using Virtual Event War-Room
- **ORGANIZE** Response with Preset Triggers
- **LEVERAGE** Mitigations in Progress



# Training Tomorrow's Business Leaders in Supply Chain Resiliency Concepts

- Resilinc SupplyIntel integrated into Smith's MBA & MS curriculums to educate future leaders on supply chain risk management best practices
- First university to integrate this Salesforce.com application into course curriculum
- In Spring 2014, 120 Masters Degree students learned that risk quantification and visibility improve business results.
- Today, over 200 students have taken software training.



# Challenges In Best Practices Transfer

- Negotiating Software Licensing and other startup costs.
- Re-purposing corporate training materials into useful aids to student learning and critical thinking.
- Staffing/ supporting usage of technology by large size classes.

# Conclusions

- Supply chain standards are elusive and we should rather emphasize evolving consensus on best practice sets.
- Collaboration between academia, industry and the government is crucial to accelerate the identification, development and diffusion of best practices across industry and into graduate education.
- The Supply Chain Risk Management field- and especially cyber supply chain risk- requires effectiveness studies to determine the Return On Investment of specific practices.
- Other areas that seem ripe for academic engagement in best practices development include: Single Window Trading Systems; Urban Logistics/Distribution; and the Internet Of Things.