• Interos Snapshot
• What is Business Intelligence?
• What is Supply Chain Risk Management?
• Business Intelligence & Supply Chain Risk Management
• Knowing What We Know
• Interos’ Findings
• Your Role in SCRM
Award-winning, certified WOSB. Eleven+ year old enterprise-oriented management services company with core capabilities in Supply Chain Risk Management and Cybersecurity focused on multiple critical infrastructure sectors including Information Technology, Energy, Food and Ag, Healthcare, Transportation, Manufacturing and the Defense Industrial Base.

**Cyber/SCRM Leadership Roles:**
- Virginia Governor’s Cybersecurity Commission
- Top 100 CEO Leader in STEM
- Chairperson NDIA Cyber Division Co-chair (previous)
- DHS SSCA WG1 Co-chair (previous)
- International Cyber Dialogue: Executive Committee
- DHS IT-SCC Member
- Open Group Member
What is Business Intelligence?

• Information vs. Intelligence
  – Data vs. Context, Expertise, and Analysis
  – Intelligence turns facts into connections, choices, and impacts

• Business Intelligence (BI)
  – Using data analysis to support industry decision-making
  – Context: information to understanding
  – Expertise: understanding to strategies
  – Analysis: strategies to action
What is Supply Chain Risk Management?

**Supply Chain Risk Management (SCRM):** The systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities and threats throughout the supply chain and developing mitigation strategies to combat those threats.

### Key Risk Factors

<table>
<thead>
<tr>
<th>Integrity</th>
<th>• Protection against counterfeit and non-conforming parts.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Resiliency</td>
<td>• Capacity to recover from supply chain disruptions.</td>
</tr>
<tr>
<td>Security</td>
<td>• Cybersecurity, Financial Security, Physical Security, etc.</td>
</tr>
<tr>
<td>Quality</td>
<td>• The form and function of finished goods.</td>
</tr>
</tbody>
</table>
BI enables SCRM through comprehensive modeling:

- Investigates technical, business enterprise, market, and security risk
- Illuminates multiple supplier tiers
- Identifies comingling and resiliency risks
- Enables assessment of supplier criticality and prioritization
Example Risk Concerns

A supplier fails to make payroll:
• Legal threat: legal suit and conviction
• Insider threat: theft, sabotage, protest
• Technical threat: lost expertise
• Financial threat: instability

A supplier prioritizes growth of customer base:
• Technical threat: cutting corners
• Leadership threat: less focus on individual customers
• Insider threat: workforce spread thin

A supplier maintains manufacturing sites in sensitive countries:
• Technical threat: counterfeit parts
• Leadership threat: political influence
• Socioeconomic threat: political destabilization, supply chain disruption

A supplier maintains poor access controls:
• Cybersecurity threat: infiltration
• Technical threat: grey market parts
• Physical threat: employment of bad actors
Business Intelligence & Supply Chain
Risk Management

Business Intelligence builds trust in suppliers by placing them in context.

*A man is known by the company he keeps.*

- Aesop’s Fables
Interos leverages a wide range of sources to analyze data through an established methodological framework.

**Confidence in Content**

**Acquire**
- Government and court records
- Scholarly and trade publications
- Company reports and filings
- Regulatory alerts and reports
- Well-regarded media
- Internet sites and social media
- Information services ("Big Data")

**Rate**
- Independence
- Substantiation
- Credibility
- Accuracy
- Consistency

**Analyze**
- What was found
- What wasn’t
- What both mean
## The Analytical Framework

<table>
<thead>
<tr>
<th>Analytical Category</th>
<th>Analytical Factor</th>
<th>Examples</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Technical</strong></td>
<td>Quality Assurance</td>
<td>Quality standard registration</td>
</tr>
<tr>
<td></td>
<td>Production &amp; Manufacturing</td>
<td>Counterfeits; manufacturing strategy</td>
</tr>
<tr>
<td></td>
<td>R&amp;D Innovation</td>
<td>Advancement investment plans</td>
</tr>
<tr>
<td><strong>Business</strong></td>
<td>Leadership &amp; Organization</td>
<td>Current and prior political affiliations</td>
</tr>
<tr>
<td></td>
<td>Supplier Management</td>
<td>Requirement flow-down</td>
</tr>
<tr>
<td></td>
<td>Business Alliances</td>
<td>Joint ventures; sharing agreements</td>
</tr>
<tr>
<td><strong>Market</strong></td>
<td>Industry Market Position</td>
<td>Performance relative to competitors</td>
</tr>
<tr>
<td></td>
<td>Revenue &amp; Financial</td>
<td>Sources and stability of revenue</td>
</tr>
<tr>
<td></td>
<td>Regulatory &amp; Legal</td>
<td>Regulatory compliance; award protests</td>
</tr>
<tr>
<td><strong>Security</strong></td>
<td>Socioeconomic Environment</td>
<td>Geopolitical environment; crime rates</td>
</tr>
<tr>
<td></td>
<td>Cybersecurity</td>
<td>History of attack; noted vulnerabilities</td>
</tr>
<tr>
<td></td>
<td>Physical Security</td>
<td>Access controls; labor issues</td>
</tr>
</tbody>
</table>
Knowing What We Know

1. Discuss risk priorities and supply chain failure consequences with risk owner
2. Research and acquire data through a multitude of data sources and providers
3. Determine its confidence in the data
4. View high-confidence data through its holistic analytical framework
5. Analyze the data’s impact on risk vulnerability and in context of risk owner’s priorities
6. Form impact statements: “Given X, Y.”
7. Propose mitigation strategies
## Federal SCRM Contracts

<table>
<thead>
<tr>
<th>Department of Energy</th>
<th>National Nuclear Security Administration</th>
<th>Intelligence Community</th>
<th>National Aeronautics and Space Administration</th>
<th>Defense Intelligence Agency</th>
<th>Defense Security Service</th>
</tr>
</thead>
<tbody>
<tr>
<td>Enterprise SCRM Program; Focal Point; Business Due Diligence Assessments</td>
<td>SCRM Program, Federal; Departmental Policy</td>
<td>Training, Outreach &amp; Awareness; KPI Development; Supplier Audits; Mitigation Playbook; ICD 731 SME.</td>
<td>SCRM Program; Business Due Diligence Assessments</td>
<td>SCRM Program Training, Outreach &amp; Awareness</td>
<td>Major Defense Acquisition Program Supply Chain Analysis; Business Due Diligence</td>
</tr>
</tbody>
</table>
From Interos Reports:

- An ICT vendor supplying a federal agency used non-authorized manufacturers and resellers with a robust history of selling counterfeit cellular equipment.
- An ICT vendor adhered to a strategy of growing their customer base and off-loaded quality assurance and service costs onto their customer.
- An RFT company had been involved in the illegal sale of technology to a foreign government.
- An EMS company was found guilty of committing over 60 I-9 (Employment Eligibility Verification) violations and forced to pay a civil penalty. ICE alleged that over half of its employees were unauthorized aliens.
- An instrumentation fabricator lacked a clear succession plan and was disrupted by the loss of a key leader.
- An apparel vendor relied on third-party manufacturing in sensitive countries that experienced ethnically-targeted violence against factories.
- An instrumentation fabricator supplying a federal agency bore expired QA certifications and was found to have neither registered or be a discoverable assignee to new patents in nearly 20 years.
SCRM Business Due Diligence was completed:

• Resulted in the Agency changing their IT procurement strategy, leading to an approximate $80 million cost-avoidance and reduced risk by purchasing from a less risky vendor.

• Resulted in the Agency changing their procurement strategy based on the Interos report and subsequent admissions by tech company of “backdoors” within their products, leading to an approximate $15 million cost-avoidance and reduced risk from purchasing from another vendor.

• Resulted in $3 million in cost-avoidance and reduced risk by complying with TAA.

No SCRM analysis: As a result of the Agency’s procured computers being taken offline and being replaced, a $5 million cost was incurred, diminishing any potential returns on investments. If an appropriate supply chain risk analysis and review had been completed, it would have been concluded that the computers did not meet specified standards, and these costs would have been avoided.
Your Role in SCRM

How can you identify who is lurking in your supply chain?
Your Role in SCRM

What are the Sources of Knowledge that you can go back to your office and use today? How about your Source’s Sources?
Interos Headquarters
1725 Duke Street, Suite 510
Alexandria, VA 22315
(703) 677-3135

Jennifer Bisceglie
CEO
jbisceglie@interos.net
703-927-3929