Business Intelligence for Supply Chain Risk Management

October 2016

Agenda

INTEROS

- 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

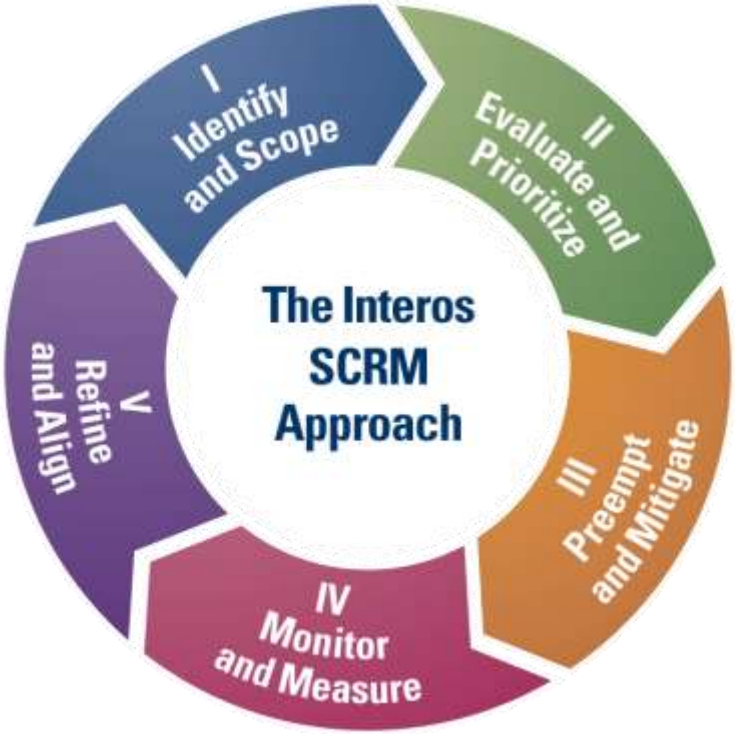
Interos Snapshot

INTEROS

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.

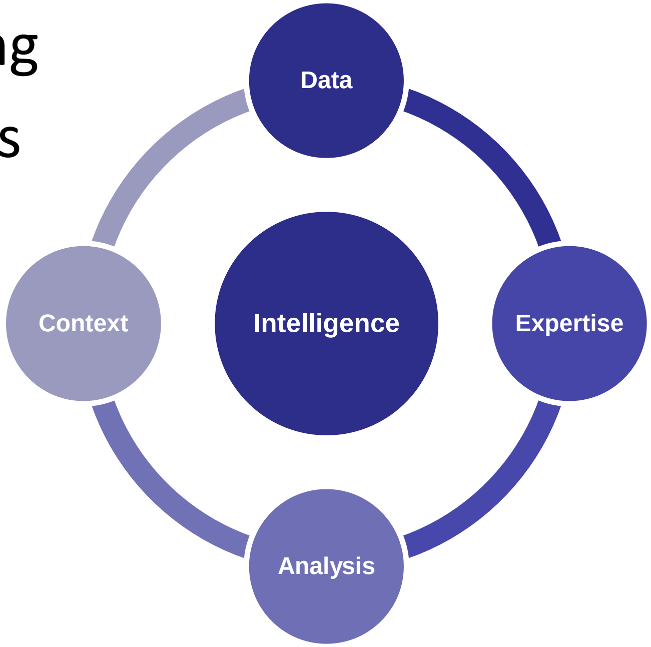
Cyber/SCRM Leadership Roles:

- 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.

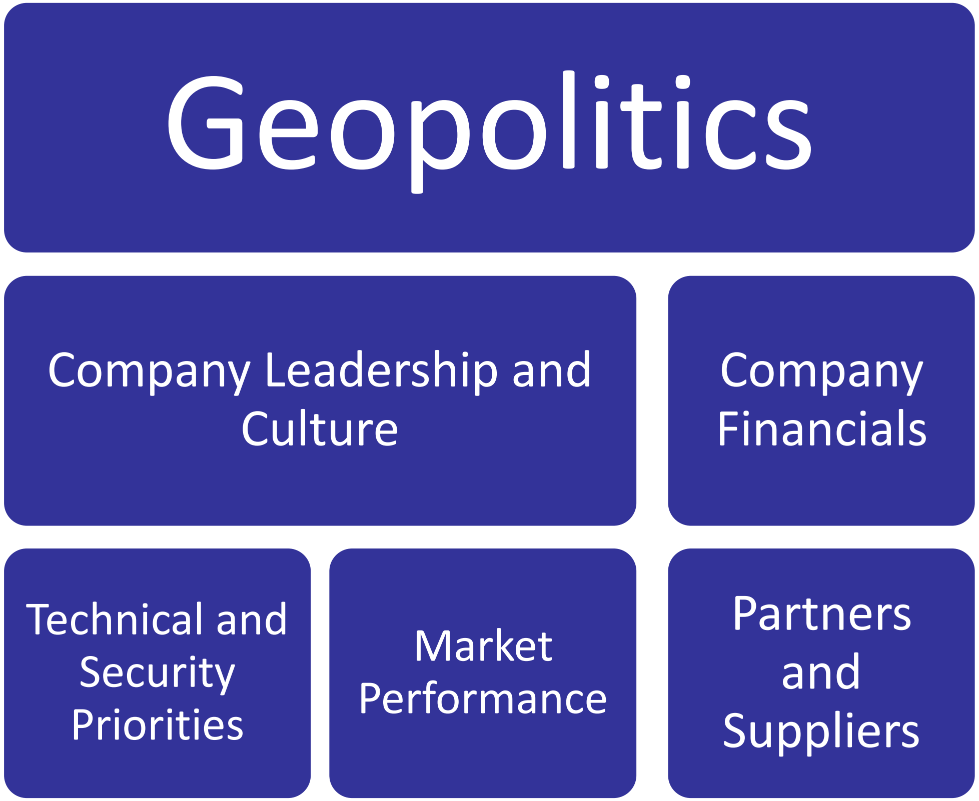
Key Risk Factors

Integrity	• Protection against counterfeit and non-conforming parts.
Resiliency	• Capacity to recover from supply chain disruptions.
Security	• Cybersecurity, Financial Security, Physical Security, etc.
Quality	• The form and function of finished goods.

Business Intelligence & Supply Chain Risk Management

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



Geopolitics

Company Leadership and Culture

Company Financials

Technical and Security Priorities

Market Performance

Partners and Suppliers

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 maintains manufacturing sites in sensitive countries:

- Technical threat: counterfeit parts
- Leadership threat: political influence
- Socioeconomic threat: political destabilization, supply chain disruption

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 poor access controls:

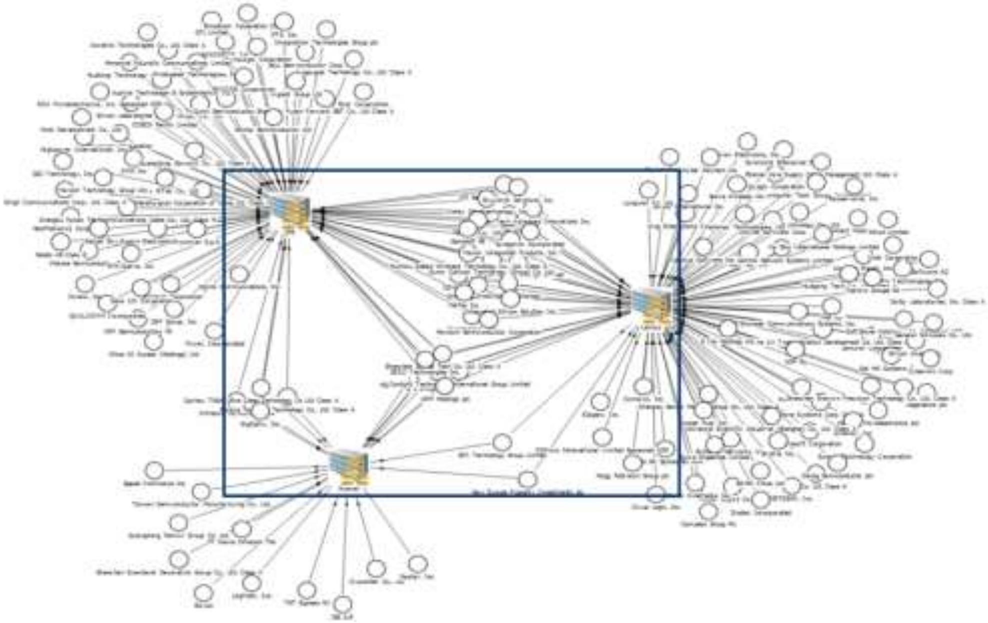
- Cybersecurity threat: infiltration
- Technical threat: grey market parts
- Physical threat: employment of bad actors

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



Knowing What We Know

INTEROS

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

Knowing What We Know

INTEROS

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

Knowing What We Know

INTEROS

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

Interos’ Findings

Federal SCRM Contracts

Department of Energy	National Nuclear Security Administration	Intelligence Community	National Aeronautics and Space Administration	Defense Intelligence Agency	Defense Security Service
Enterprise SCRM Program; Focal Point; Business Due Diligence Assessments	SCRM Program, Federal; Departmental Policy	Training, Outreach & Awareness; KPI Development; Supplier Audits; Mitigation Playbook; ICD 731 SME.	SCRM Program; Business Due Diligence Assessments	SCRM Program Training, Outreach & Awareness	Major Defense Acquisition Program Supply Chain Analysis; Business Due Diligence

Interos' Findings

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.

Interos' Findings

INTEROS

ROI Statements for Business Due Diligence

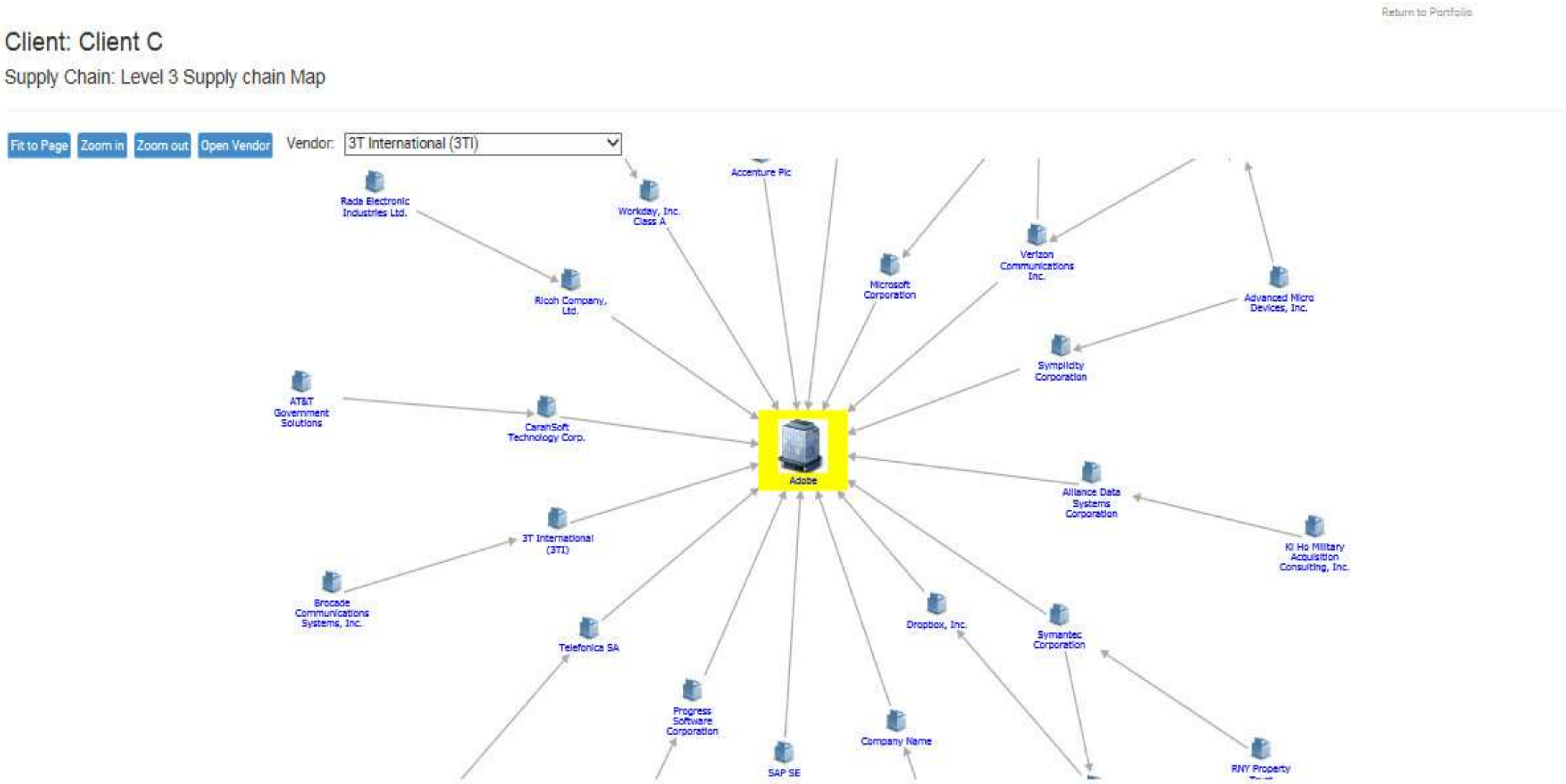
SCRM Business Due Diligence was completed:

- 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?



Client: Client C

Supply Chain: Level 3 Supply chain Map

Vendor: 3T International (3TI)

Return to Portfolio
Fit to Page
Zoom in
Zoom out
Open Vendor
Accenture Plc
Rada Electronic Industries Ltd.
Workday, Inc. Class A
Verizon Communications Inc.
Microsoft Corporation
Advanced Micro Devices, Inc.
Ricoh Company, Ltd.
Symplicity Corporation
AT&T Government Solutions
CarahSoft Technology Corp.
Adobe
Alliance Data Systems Corporation
Ki Ho Military Acquisition Consulting, Inc.
3T International (3TI)
Brocade Communications Systems, Inc.
Telefonica SA
Dropbox, Inc.
Symantec Corporation
Progress Software Corporation
Company Name
SAP SE
RNY Property

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

INTEROS