New Technology Enabled Supplier Risk Services

NDIA Systems Engineering Division Meeting
Theme: Enterprise Risk Management/Technology Enablers for Assurance
March 16, 2015
New Technology Enabled Supplier Risk Services

- Example 1: Predictive Intelligence for Supplier Risks (Global4Sight)
- Example 2: Dynamic Technology Assessment: Quantifying Risk-Cost Tradeoffs
- Example 3: Use of Ultra-sensitive RF Sensors for HW QC (Attacus)
Manufacturing trends like globalization, increasing product complexity, and more use of IT in production create new risks in supply chains.

**Conventional Supply Chain Issues**
- Price (PPV)
- Part availability
- Speed to customer
- Effective inventory control
- Efficient logistics
- Reputation/repeat customers

**Emerging Supply Chain Risks**
- Counterfeiting
- Cyber threats
- Foreign influence
- Intellectual property theft
- Diversion

Evolving To Include...
In response to emerging Supply Chain risks, we are seeing new Government Regulations mandating Supply Chain Risk Management

**Timeline of Key Regulations**

**Comprehensive National Cybersecurity Initiative (CNCI)**
- Initiative #11
  - Develop a multi-pronged approach for global supply chain management
  - Risks stemming from both the domestic and globalized supply chain must be managed over the entire lifecycle of products, systems and services.

**Intelligence Community Directive 731**
- Issued by the Director of National Intelligence on 7 Dec. 2013, and directs agencies in the Intelligence Community to consider supply chain risk in IT procurements.

**DFARS Interim Rule 2012-D050 (Section 806)**
- Authorizes the Dept. of Defense to address its procurements from the IT supply chain. As a provision of the Defense Federal Acquisition Regulations Supplement, the Interim Rule requires the DoD to evaluate supply chain risk when awarding contracts. Scope covers hardware, software

**Wolf Provision**
- (Consolidated Appropriations Act of 2014, Section 515)
  - Funding for the Departments of Justice, Commerce, NASA, and the NSF. Restricts spending on “high” or “moderate” impact IT until the agency assesses supply chain risk. Affected agencies are now creating regulations to implement this mandate

**Army Regulation 70-77**
- (ex. May 2015)
  - Requires PMs to review suppliers for potential foreign influence threats and file a mitigation plan with the Assistant Secretary of the Army for Acquisitions, Technology, and Logistics (ASAALT)

**DoD 5000.02**
- Requires all Defense acquisition program managers (PMs) to control the risk that enabling technologies will be lost to an adversary. PMs are instructed to focus on the risk that design vulnerabilities or supply chains will be exploited to destroy, modify, or exfiltrate critical data, degrade system performance, or decrease confidence in a system
At the same time there’s been a revolution in the availability and use of open source data that could be used for all sorts of intelligence purposes.

Every minute...

...570 new websites launched
...200 million e-mail messages sent
...2 million queries received by Google
...48 hours of video added to YouTube
...47,000 apps downloaded by Apple

Commercial Data Services Proliferating

Highlight on One Area: Social Media
Booz Allen’s Global4Sight Supplier Risk Offerings use this world of open source to address new risks by offering predictive intelligence on suppliers.

GLobal4Sight (G4S)

- Know more about a supplier
- Know more about an entire supply chain
- Know it sooner
- Take action as needed

New Actionable Insights into Suppliers and Supply Chains
In building new supplier risk offerings, we are guided by a few key tenets that are worth noting.

**Traditional Supplier Assessments**

- Use only supplier provided data or internal data from the buyer’s enterprise
- One-time due diligence performed when first engaging a supplier
- Assessment of direct suppliers only

**Tenets of Booz Allen Supplier Risk Offerings**

- Also use novel open source data, including broadcast media, social media, and 3rd party data aggregator services
- Ongoing 360-degree continuous monitoring of vendors
- Can address entire supply chain (i.e., supplier’s suppliers)

New G4S Supplier Risk Offerings are intended to augment, not replace, traditional supplier risk management.
Our Supplier Risk service offerings provide clients with powerful new analyses that can be tailored to their specific needs

Descriptions of Supplier Risk Services

1. **Supplier Assessments**
   An independent, in-depth assessment of a supplier using novel data sources which can quickly screen many suppliers and evaluate vulnerabilities using our proprietary assessment framework

2. **Supplier Monitoring**
   A semi-automated continuous monitoring service that uses advanced analytics and a state of the art dashboard to monitor near real-time activity across a set of suppliers, forewarning any risks (e.g., fraud, financial, etc.)

3. **Supply Chain Assessment**
   For a single supplier, map out and characterize discoverable risks associated with subsequent tiers of suppliers that they use to deliver their products and/or services
Our Supplier Assessments use a proprietary Risk and Vulnerability Assessment framework...

### Risk and Vulnerability Framework

<table>
<thead>
<tr>
<th>Attributes</th>
<th>Icon</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Location</strong> – Vulnerabilities associated with firm location based on U.S. friendly and business environment</td>
<td></td>
</tr>
<tr>
<td><strong>Ownership</strong> – Vulnerabilities associated with identities and affiliations of firm owners</td>
<td></td>
</tr>
<tr>
<td><strong>Business Relationships</strong> – Vulnerabilities based on foreign affiliation of the partner and the strength of the relationship (e.g., customer, vendor, strategic partner, JV)</td>
<td></td>
</tr>
<tr>
<td><strong>Key Personnel</strong> – Vulnerabilities associated with biographic information of key personnel (e.g., C-suite, program managers, key technical staff, etc.)</td>
<td></td>
</tr>
<tr>
<td><strong>Reputation</strong> – Vulnerabilities associated with the standing of the firm</td>
<td></td>
</tr>
<tr>
<td><strong>Security</strong> – Measures taken to protect information, products, and operations. Breaches include insider, physical and cyber, etc.</td>
<td></td>
</tr>
<tr>
<td><strong>Financial Stability</strong> – Vulnerabilities associated with the financial stability of a firm over time</td>
<td></td>
</tr>
</tbody>
</table>

### Sample Open Source Materials

- Company websites
- Company marketing literature
- Hoovers
- Multiple integrated circuit trade journals
- Defense.gov
- Justice.gov
- SEC.gov
- Darpa.mil
- Nasdaq.com
- Lexis-Nexis
- Interviews with subject matter experts
- Investor communications
- Annual and quarterly financial filings
- Various business publications
- Tax documents
- Google Earth
- Law 360
- Manta
- Linkedin.com
...that yields comprehensive and actionable evaluations of the risk inherent in specific suppliers

- We are currently performing Supplier Assessments on firms involved in R&D of emerging technologies of interest to a military intelligence client.

- We use a bespoke risk assessment methodology that we developed to assess the susceptibility of suppliers to various sorts of foreign influence.

- Using our proprietary open source tradecraft, we've evaluated large numbers of suppliers and prioritized which firms the client should assess more deeply using their special rights and authorities (but scarce resources).
Our Supplier Monitoring capability allows buyers to stay current on Suppliers with the latest relevant news

- The Supplier Monitoring Dashboard allows analysts to quickly sort through large number of open source results and find most relevant information
- Provides “Trending” information by displaying frequency of key terms
- Enables production of monthly reports, updating vulnerability assessments with latest news

Sample Monthly Continuous Monitor Reports
We can also do deep look into an entire supply chain evaluating the risk to products from lower tier suppliers

- We recently performed a Supply Chain Assessment for a Fortune 500 IT company
- Our analysis leveraged automated open source collection and advanced simulation tools that allowed our client to understand the intent, capability, sophistication, and motive of threats to their supply chain
- Clients use insights from our efforts to determine the best way forward in building out programs to manage cyber security supply chain and business risks to product assurance, integrity, confidentiality, and availability
New Technology Enabled Supplier Risk Services

- Example 1: Predictive Intelligence for Supplier Risks (Global4Sight)
- Example 2: Dynamic Technology Assessment: Quantifying Risk-Cost Tradeoffs
- Example 3: Use of Ultra-sensitive RF Sensors for HW QC (Attacus)
Counterfeit electronic components remain a persistent threat, particularly to systems facing obsolescence and offshoring issues.

### Drivers of Counterfeit Part Production
- **Old, Obsolete Designs** – as a part becomes obsolete, it disappears from stock, replaced by a another, better-designed part
- **Life Cycle** – not enough inventory to last a military product’s entire 30-year lifespan
- **Procurement Process**
  - Purchased from an untrusted source to meet cost & schedule demands
  - Poor traceability / authentication
- **Suspicious Part Sales / Threat Actors** – profit motive and malicious intent can incentivize poor quality assurance and sales practices
- **Gov’t Regulations** – Environmental regulations, such as lead-free requirements can drive parts reclamation
- **Quality Assurance** – inadequate test & inspection procedures
- **Lack of Enforcement** – not enough resources to track down the counterfeiters

### Consequences of Encountering Counterfeit Parts

<table>
<thead>
<tr>
<th>Schedule Slips</th>
<th>Finding unverified parts and then testing them to ensure they are reliable takes time</th>
</tr>
</thead>
<tbody>
<tr>
<td>Higher Cost</td>
<td>For example, 100% testing of every bit state in a memory chip can take weeks full-time</td>
</tr>
<tr>
<td>Lower Performance</td>
<td>A cheap, low-speed part sold as a higher-speed part will cause slow-running apps</td>
</tr>
<tr>
<td>Poor Reliability</td>
<td>The process of harvesting counterfeit parts stresses them, lowering their reliability</td>
</tr>
<tr>
<td>Product Failure</td>
<td>Counterfeits may work as well as new parts or fail sooner – without screening, it’s a gamble</td>
</tr>
</tbody>
</table>
Dynamic Technology Assessment quantifies the risk-cost of suspect electronics by incorporating technical and supply chain data.

Dynamic Technology Assessment Software – How It Works

Criticality Assessment | Gather Supply Chain and Technical Data | Score Vulnerability Categories and Assess Technology | Run Software and Analyze Results

Supply Chain Vulnerabilities
- Supplier Interviews
- Open Source Data (GIDEP, ERAI, etc)
- Supply Chain Info
- Classified Reports

Technical Vulnerabilities
- Test Data
- Engineering Specs
- Technical Interviews
- Engineering Judgment

Supply Chain Categories
- Supplier Historical Data
- Locations of Suppliers
- Security Processes
- Ownership
- Pricing Information

Technical Categories
- Part Functional Specs
- Part Usage & Application
- Design Data & Methods
- Manufacturing Processes
- Assess Test Impact

The Chance of Getting a Faulty or Suspect Component
- 50% Average
- 75% High

SMEs provide a risk score and confidence distribution to quantify uncertainty

DTA Seeks To Maximize the Effectiveness of Risk Mitigation Actions

Do More Testing | Work with Suppliers
We prototyped the risk software on a defense UAV system, specifically the radar image processing unit microprocessors.

### Flight Control & Radar Components in UAV system

![Diagram of Radar Components]

### Actual card from Radar Image Processor

![Actual card from Radar Image Processor]

### Purchasing Information for Chips on the Radar Image Processing Card

<table>
<thead>
<tr>
<th>Part</th>
<th>Microprocessor</th>
<th>1GB DDR SDRAM Memory</th>
<th>Mercury RapidIO CN ASIC</th>
<th>8MB Flash EEPROM</th>
</tr>
</thead>
<tbody>
<tr>
<td>Vendor</td>
<td>OEM (Fab) A</td>
<td>OEM (Fab) B</td>
<td>OEM (Fab) A</td>
<td>OEM (Fab) B</td>
</tr>
<tr>
<td>Number of parts on board</td>
<td>160</td>
<td>320</td>
<td>160</td>
<td>320</td>
</tr>
<tr>
<td>Fab Selling Price</td>
<td>$284.82 each</td>
<td>Obsolete</td>
<td>Custom-made part</td>
<td>Obsolete</td>
</tr>
<tr>
<td>Distributor Selling Price</td>
<td>$187.05 each</td>
<td></td>
<td></td>
<td>$2.39</td>
</tr>
</tbody>
</table>

- The microprocessor is a high-value component
- It’s available for purchase directly from the foundry as well as through distributors

Source: COTS Journal Nov. 2005
The DTA tool quantifies the up-front versus long-term risks, in dollars, for each procurement & test alternative using Monte Carlo analysis.

<table>
<thead>
<tr>
<th>Parts Source</th>
<th>Up Front Cost</th>
<th>Residual (long term) Risk</th>
<th>Distribution of Cost vs. Risk</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributor A</td>
<td>$90,463</td>
<td>$112,524 (17.9%)</td>
<td></td>
</tr>
<tr>
<td>Distributor B</td>
<td>$90,463</td>
<td>$102,025 (16.2%)</td>
<td></td>
</tr>
<tr>
<td>Foundry Supplier</td>
<td>$95,571**</td>
<td>$89,982 (13.9%)</td>
<td></td>
</tr>
</tbody>
</table>

Note: **Cost per 160 parts, must buy 1000 parts
Comparing the various procurement alternatives, this table provides the relationship between up-front cost and accepted risk.

<table>
<thead>
<tr>
<th>Risk-Adjusted Cost Comparison for a Complex IC</th>
<th>Initial Purchase Cost</th>
<th>Failure Costs</th>
<th>Likelihood of Failure</th>
<th>Test Cost</th>
<th>Test Chance of Detection</th>
<th>Risk-Adjusted Cost</th>
<th>Up-front Costs (Purchase + Test)</th>
<th>Risk Return on Test Investment</th>
<th>Residual Risk Cost</th>
<th>Residual Risk Percentage</th>
</tr>
</thead>
<tbody>
<tr>
<td>Distributor A</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase price</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>60%</td>
<td>$-</td>
<td>0%</td>
<td>$405,010.13</td>
<td>$29,928.00</td>
<td>-</td>
<td>$375,082.13</td>
<td>59.5%</td>
</tr>
<tr>
<td>Purchase price + optical, X-ray, decap</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>60%</td>
<td>$46,535.00</td>
<td>30%</td>
<td>$339,020.49</td>
<td>$76,463.00</td>
<td>42%</td>
<td>$262,557.49</td>
<td>41.7%</td>
</tr>
<tr>
<td>Purchase price + full optical &amp; DC tests</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>60%</td>
<td>$60,535.00</td>
<td>70%</td>
<td>$202,987.64</td>
<td>$90,463.00</td>
<td>234%</td>
<td>$112,524.64</td>
<td>17.9%</td>
</tr>
<tr>
<td>Purchase price + full DC &amp; AC tests</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>60%</td>
<td>$99,535.00</td>
<td>99%</td>
<td>$133,213.82</td>
<td>$129,463.00</td>
<td>173%</td>
<td>$3,750.82</td>
<td>0.6%</td>
</tr>
<tr>
<td>Distributor B</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase price</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>54%</td>
<td>$-</td>
<td>0%</td>
<td>$370,014.13</td>
<td>$29,928.00</td>
<td>-</td>
<td>$340,086.13</td>
<td>54.0%</td>
</tr>
<tr>
<td>Purchase price + optical, X-ray, decap</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>54%</td>
<td>$46,535.00</td>
<td>30%</td>
<td>$314,523.29</td>
<td>$76,463.00</td>
<td>19%</td>
<td>$238,060.29</td>
<td>37.8%</td>
</tr>
<tr>
<td>Purchase price + full optical &amp; DC tests</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>54%</td>
<td>$60,535.00</td>
<td>70%</td>
<td>$192,488.84</td>
<td>$90,463.00</td>
<td>193%</td>
<td>$102,025.84</td>
<td>16.2%</td>
</tr>
<tr>
<td>Purchase price + full DC &amp; AC tests</td>
<td>$29,928.00</td>
<td>$629,928.00</td>
<td>54%</td>
<td>$99,535.00</td>
<td>99%</td>
<td>$132,863.86</td>
<td>$129,463.00</td>
<td>138%</td>
<td>$3,400.86</td>
<td>0.5%</td>
</tr>
<tr>
<td>Foundry</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Purchase price</td>
<td>$95,571.20</td>
<td>$645,571.20</td>
<td>14%</td>
<td>$-</td>
<td>0%</td>
<td>$185,554.09</td>
<td>$95,571.20</td>
<td>-</td>
<td>$89,982.89</td>
<td>13.9%</td>
</tr>
<tr>
<td>Purchase price + optical, X-ray, decap</td>
<td>$95,571.20</td>
<td>$645,571.20</td>
<td>14%</td>
<td>$46,535.00</td>
<td>30%</td>
<td>$205,094.22</td>
<td>$142,106.20</td>
<td>-142%</td>
<td>$62,988.02</td>
<td>9.8%</td>
</tr>
<tr>
<td>Purchase price + full optical &amp; DC tests</td>
<td>$95,571.20</td>
<td>$645,571.20</td>
<td>14%</td>
<td>$60,535.00</td>
<td>70%</td>
<td>$183,101.07</td>
<td>$156,106.20</td>
<td>-96%</td>
<td>$26,994.87</td>
<td>4.2%</td>
</tr>
<tr>
<td>Purchase price + full DC &amp; AC tests</td>
<td>$95,571.20</td>
<td>$645,571.20</td>
<td>14%</td>
<td>$99,535.00</td>
<td>99%</td>
<td>$196,006.03</td>
<td>$195,106.20</td>
<td>-111%</td>
<td>$899.83</td>
<td>0.1%</td>
</tr>
</tbody>
</table>

- Residual risk describes the remaining risk of part failure not covered in the selected tests.
- A trade off exists between risk and up-front cost.
New Technology Enabled Supplier Risk Services

- Example 1: Predictive Intelligence for Supplier Risks (Global4Sight)
- Example 2: Dynamic Technology Assessment: Quantifying Risk-Cost Tradeoffs
- Example 3: Use of Ultra-sensitive RF Sensors for Quality Control (Attacus)
Attacus is a new Solution for Component Authentication

- Attacus is based on BRIMSTONE, Booz Allen’s proprietary SW defined ultra-sensitive radio frequency (RF) detector that picks up very weak-signal RF microfluctuations.

- BRIMSTONE has detection capabilities at the attowatt level, the equivalent of the wing flap of a mosquito from up to 30 miles away.

- BRIMSTONE can capture bandwidths up to 1.8 GHz to aid in signature discovery.

- Attacus applies BRIMSTONE’s advanced capture and signal processing capabilities to detect whether a specific component complies with the known electromagnetic emissions of an authentic part.

- Attacus determines whether a chipset and circuit board is authentic by determining its electromagnetic signature. Defective or counterfeit components won’t match the operating point of an authentic component.
Multifaceted Benefits

Faster Verification

• Conventional verification methods, such as X-ray, optical, or thermal techniques, are time-consuming, expensive, and may be invasive. Attacus gives organizations the ability to quickly differentiate between legitimate and counterfeit components with a non-invasive process.

It Works When It’s Noisy

• Attacus can operate in an ambient (noisy) production environment. It detects weak radio frequency signals regardless of surroundings. This means an operator can check component authenticity in the same space where your business assembles complex systems.

Low Cost Solution

• In developing Attacus, we applied engineering and weak signals expertise to maximize the use of commercial-off-the-shelf technologies for reduced end-user costs. Its flexible software-based architecture allows for rapid development cycles.

A Wide Range of Applications

• Attacus is a flexible platform that manufacturers can use in different ways. As it examines chipsets or circuit boards at the electromagnetic level, the system can also determine if parts are defective or of subpar quality, as well as whether there is malicious functionality at the hardware or software level.
Example 1: Predictive Intelligence for Supplier Risks (Global4Sight)

Example 2: Dynamic Technology Assessment: Quantifying Risk-Cost Tradeoffs

Example 3: Use of Ultra-sensitive RF Sensors for Quality Control (Attacus)