What BC Managers Need to Know About Vendor Risk Management

Bud Telchin, CBCP

btelchin@att.net 917-566-4513

NYC ACP Meeting
July 21, 2016

Introduction

- Business Continuity = Continuity of Operations
- Where do Vendors Fit In ?
- Risk-Based View
- Engagement Focus, rather than Vendor Focus

Agenda

- 1. Introduction
- 2. Vendor Risk vs Supply Chain Risk
- 3. Which Vendors to Worry About
- 4. Stages in the Vendor Relationship Life Cycle
- 5. TAKEAWAYS:
  - Vendor Risks You Need to be Prepared For
  - Two Sheets of Paper: Risk Filter and Exit Strategy
- 6. How to Set up a Vendor Risk Management Program
- 7. How to Do a Vendor Risk Assessment
- 8 Q&A

EVERYTHING IS FINE…..ISN'T IT?

- Reliable Service and Results
- Excellent Support
- Impeccable References
- Solid Audit Results

- But you never know when or how a Vendor will shut you down

WHAT CAN GO WRONG?

- Ericsson vs. Nokia
- Target Corp Data Breach
- California Child Welfare System:
  IBM, Iron Mountain, FedEx

WHY SHOULD YOU CARE?

- Regulators
  - HIPAA, GLBA, PCI, SOX, OCC
  - Mandate that corporate controls extend to ‘third party’ providers
  - Require organizations to perform regular and ongoing vendor risk assessment as part of the compliance process
- BC Touchpoints: You already deal with Vendors
- Business Continuity = Continuity of Operations

BC TOUCHPOINTS

- Annual Risk Assessment:
  - Natural Risks, Accidental, Intentional, **Supply Chain**
- BIA:
  - Processes: Inputs from Vendors
  - Dependencies on Vendors
- Business Continuity Plan
  - Critical Vendor Contacts, Escalation Steps
- BC Testing:
  - To include key vendors in yours; be part of Vendor's testing

What Risks Does Your Organization Face?

.

- Economic
- Credit
- Interest
- Market
- Geo-Political
- **Operational Risks**

Operational Risks

- Natural Events: Flood, Earthquake, Forest Fires
  - Volcanos; Tsunamis
- Accidental Events: Fires, HVAC, Power

OPERATIONAL RISKS (Con'td)

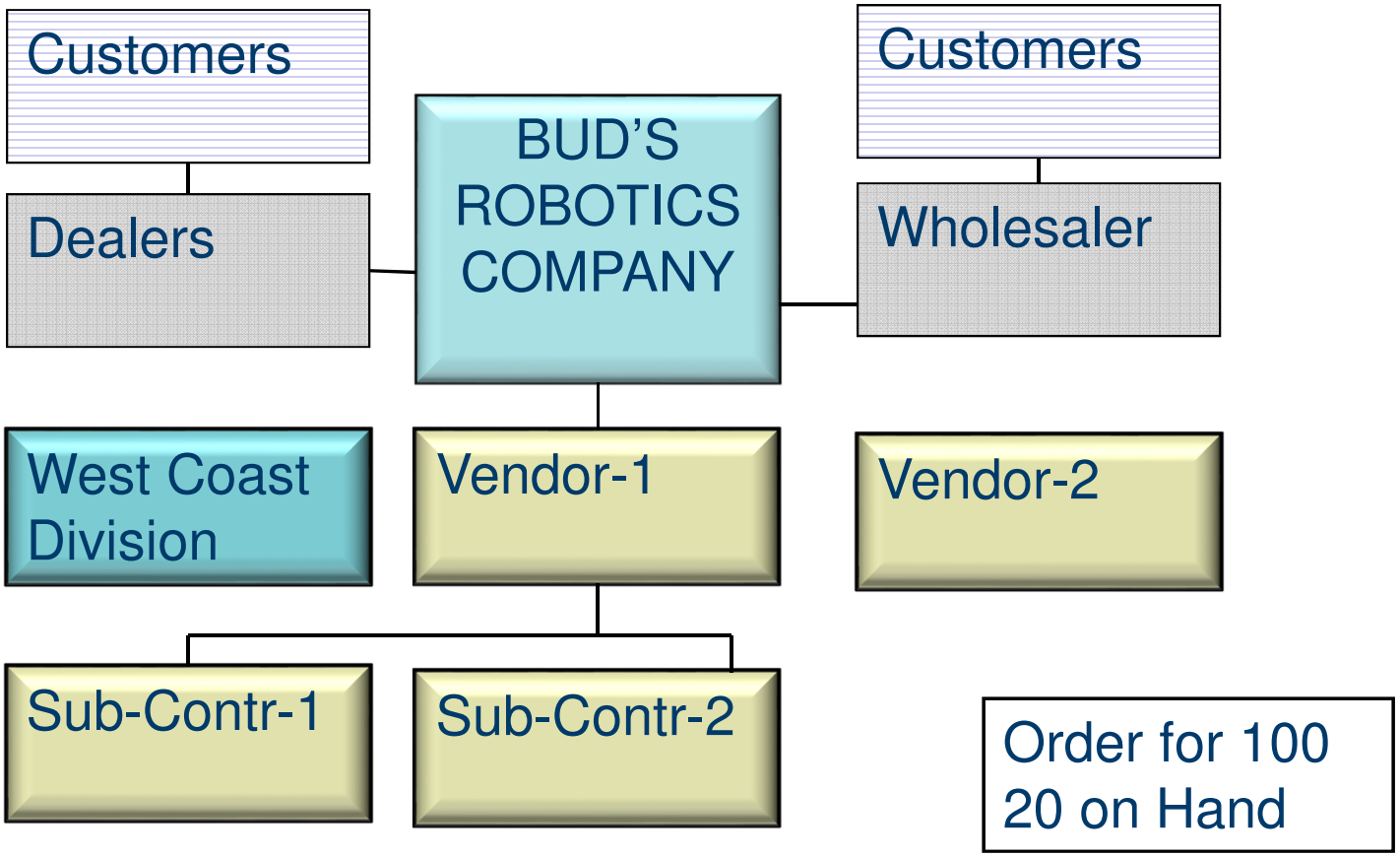
- Human Intentional Events (terrorists, active-shooter, disgruntled employee)
- Quality Control
- People: Resignations, Absenteeism, Pandemics
- IT Related: System downtime, Network/Internet downtime, malware, Ransom-Ware
- **Supply Chain / Vendor, including Geo-Political**

SUPPLY CHAIN vs. VENDOR

- **Henry Ford:**
- Steel
  - Iron Ore
  - Railroads
  - Coal
  - Railroads
- Wood
  - Forests
  - Railroads
- Rubber
  - Plantations
  - Ships

Supply Chain, but no Vendors

SUPPLY CHAIN COMPLEXITIES



Supply Chain Complexity and Risk

- Boeing 787:
  - 2.3 Million Parts
- Boeing 747-8
  - 6 million parts

- 5400 Factories
- 500,000 workers

Agenda

- 1. Introduction
- 2. Vendor Risk vs Supply Chain Risk
- 3. **Which Vendors to Worry About**
- 4. Stages in the Vendor Relationship Life Cycle
- 5. TAKEAWAYS:
  - Vendor Risks You Need to be Prepared For
  - Two Sheets of Paper: Risk Filter and Exit Strategy
- 6. Stages in the Vendor Relationship Life Cycle
- 7. How to Set up a Vendor Risk Management Program
- 8. How to Do a Vendor Risk Assessment
- 9. Q&A

VENDORS…..WHO ARE THEY?

- Anyone who provides goods or services you need but don't provide yourself
- Core Business: supplies; materials; sub-assemblies; etc.
  - Hint: Supply Chain
- HR: Payroll; Benefits; Medical, etc.
- Facilities: HVAC; cleaning; Security; etc.

Vendors…..WHO ARE THEY? Part 2

- Utilities: Data & Phone Lines; etc.
- IT: Hosting; Infrastructure; Consulting; Software development; etc.
- Professional Services: Accounting; Audit; Legal; etc.
- Logistics: Truckers, deliveries; etc.

They Have Various Names

- Vendors
- Outsourcers
- Service Providers
- Suppliers
- Contractors
- 3rd Parties; 4th Parties
- Host

Who Are The Players

- Business Unit:
  - Contract Owner
  - Business Owner
  - Relationship Manager (RM)
- Procurement (a.k.a., Purchasing):
  - Procurement Manager
  - Industry Specialist
- Vendor Risk Management
  - Manager
  - Assessor
- Vendor:
  - Primary Contact
  - Customer Relationship Manager

STAGES IN THE VENDOR RELATIONSHIP

- **Business Need** to do something: go Inside or Outside
- **Sourcing Process**: Identify Long List; Short List, Issue RFP
  - **Vendor Risk Assessment**
- **Contract Negotiations**: SLA for Quality, Timeliness, Change Orders, Additional Capacity; RTO for BC/DR; Right to Audit; etc.
- **Then, For Many Years**: Relationship Monitoring: Performance; Quality, Customer Service; etc,
  - Vendor Risk Assessments, Management Reporting
- Exit Strategy

Vendor Categtorization: “C I A”

- Confidentiality:
  - To ensure privacy
  - Training of Staff
- Integrity:
  - Accurate, trustworthy Data
- Availability:
  - DR, BC Planning
  - HW/SW Maintenance

Agenda

- 1. Introduction
- 2. Vendor Risk vs Supply Chain Risk
- 3. Which Vendors to Worry About
- 4. Stages in the Vendor Relationship Life Cycle
- **5. TAKEAWAYS:**
  - Vendor Risks You Need to be Prepared For
  - Two Sheets of Paper: Risk Filter and Exit Strategy
- 6. How to Set up a Vendor Risk Management Program
- 7. How to Do a Vendor Risk Assessment
- 8. Q&A

Vendor Risks to Prepare For

- Access to Pers. Identifiable Info (PII); Pers. Health Info (PHI)
- Access to Other Confidential Information
- Background of Vendor Staff working On-Site or Remotely
- Financial Health
- Tested BC/DR Plans
- Security of Networks, Logical Access, PenTesting, IDS
- Security of Data: Encryption in Motion, at Rest
- Vendor's Vendors: all of the above

SHEET OF PAPER-1: VENDOR RISK FILTER

- Vendor Name: _____
- In-Scope Services: _____
- Service Criticality: 1 to 5
- $ Impact of Downtime: 1 to 5
- Access to Client Information: 1 to 5
- Access to Infrastructure? Y or N
- Financial Stability: 1 to 5
- Use of Sub-Contractors: 1 to 5
- Location of Vendor's IT Infrastructure & Backup

Sheet of Paper-2: EXIT STRATEGY

- Vendor Name: _____
- In-Scope Services Provided: _____
- Criticality to the Company: 1 to 5
- Who are Alternate Vendors? N & A
  - Time to Convert (vs. RTO): _____
  - Cost to Convert: _____
- Criteria for Activating Exit Strategy
  - Quality, Timeliness, Capacity
  - Contract Terms

HOW TO SET UP A VENDOR RISK PROGRAM

- Identify User and Vendor Relationship Managers
- Define Policies, Standards & Procedures
- Establish Risk-Criteria by Vendor-type Obtain Vendor Risk-Rankings from the VRMs
- Begin Vendor Assessments and Reporting

HOW TO DO A VENDOR RISK ASSESSMENT

- Determine Vendor Ranking, using Risk Filter
- Prepare and send out Questionnaires
  - SIG (from Shared Assessments Org)
  - Request supporting documents pertinent to that Vendor and Engagement
- Assess Questionnaires, and documents, when/if they are returned
  - Consider acceptance of SOC-2 or SSAE-16, or AUP
- Follow up on Issues-Found with Vendors, VRMs to mitigate findings

VENDOR QUESTIONNAIRE CONTENT

- Risk Assessment
- Security Policy
- Organizational Security
- Asset Management
- Human Resources Security
- Physical and Environmental Security
- Communications and Operations Management
- Access Controls
- Information Systems Development
- Incident Management
- Business Continuity and DR
- Compliance
- Privacy

Courtesy of Shared Assessments SIG Questionnaire

CONCLUSION

- We've examined Supply Chain vs. Vendor Risk
- Understand that HIPAA, etc. mandate Vendor Risk assessments
- Learned how to set up a Vendor Management Program
- Learned how to perform Vendor Risk Assessments
- Learned how to create a Risk Filter and Exit Strategy
- Identified the Major Vendor Risks BC needs to Plan For
- So grab the lead and sell Vendor Risk Management to your organization

Resources

- 1. Supply Chain Risk: Jan Husdal
  - www.husdal.com
- 2. Shared Assessments Organization: SIG Questionnaire
  - www.sharedassessments.org
- 3. SOC-2, SSAE-16
  - http://www.ssae16.org/white-papers/soc-2-compliance.html
- 4. Vendor Risk Management terms
  - http://www.gartner.com/it-glossary/vendor-risk-management/
- 5. OCC Bulletin 2013-29 For excellent Roadmap for Vendor Risk Management:
  - http://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html

Final Thoughts

Be **aware** of Risks!

Trust, but thoroughly Vet your Vendors!

- Thank you!

» Q & A

- Please call if any questions:
- Bud Telchin, CBCP
- btelchin@att.net 917-566-4513