

Oh! My supplier did not deliver.....

How to build resiliency in supply chain?

Sunil Bakshi MCA, CISA, CISM, CGEIT, CRISC, CISSP, CDPSE, PMP, CEH, AMIIB, ISO 27001 LA, BS25999 LI, ISO 27001 LA, ISO9001 LA



My supplier did not deliver WHY?

See ISACA.



Visible effect of Pandemic and lockdown

- Whatever may be reason/s ... It *hurts* organization.
 - Logistics failure/ Transportation issues
 - \circ Bad weather
 - $\,\circ\,$ Supplier faces cyber attack
 - Civil disturbance
 - $\,\circ\,$ Pandemic and lock-down
 - Supplier's problems
 - \circ Unavailability skilled resources
 - 0

Question?



- Are these similar or different?
 - Vendor management
 - Outsourcing management (Service provider)
 - Supply-chain management (Supply-chain Partner)
- Commonalities
 - \odot Dependency on third party for providing product and/or service
 - Failure impacts organizations
 - \circ Causes of failure can be independent or common like widespread incident

Let us try to understand

- Understand Supply chain
- IS supply chain
- Issues and need for resiliency
- Building resiliency
 - \circ Governance framework
 - \circ Understanding supply chain partners
 - \odot Associated Risk and mitigation processes
 - \odot Use of automation
- Open session



Supply Chain



- Organization produce goods/services based on market demand.
- Production plan requires ingredients/raw material / Service delivery from suppliers.
- Logistic requirements depends upon the material stocking strategy of organization
- Lower stock results in Higher dependency on logistics – Just In Time (JIT) requires faster supplier response.
- Suppliers for organizational Support services
 Technology, Human resources etc.
- Lean Supply chain focuses on reducing number of suppliers - many times single supplier.



Information System Supply Chains



- Information system (IS) supply chains typically resemble the product supply chain. Partner primarily supply services along with consumables/Spares etc.
- IS supply chains include hardware suppliers, application developers, maintenance service providers, endpoint suppliers, network service providers, cloud service providers, website hosting companies, and so on.
- Adoption of Information and related technologies for Accelerated supply chain including product supply chain.
 - Internet of Things (IoT)
 - Artificial Intelligence (AI)
 - Robotic Process Automation (RPA)
 - \odot Advanced analytics in operational and customer-facing functions.

End-to-end ecommerce and online business models increased digital complexity.

See ISACA **Top Causes of Supply Chain Interruptions – Pre-COVID**



17 February 2021

Impact of COVID on Supply chain



- 94% of Fortune 1000 companies are seeing supply chain disruptions from COVID.
- **75**_% of companies have had negative or strongly negative impacts on their businesses.
- 55% of companies plan to downgrade their growth outlooks (or have already done so).

Source: https://www.accenture.com/in-en/insights/consulting/coronavirus-supply-chain-disruption

Areas of supply chain most impacted by the pandemic?



JIT and Lean models



- JIT helps in reducing capital investments in stocks and faster response to market demands
- JIT depends heavily of supplier response and logistics
 9/11 WTC attacks high-lighted logistic issues
- Lean supply chain focuses on reducing waste and increasing efficiency by limiting number of suppliers, many time a single supplier to deal.
- Current Pandemic high-lighted multiple issues for both

 \circ Supply issues

- Organizations did not received supplies in time.
- Organizations could not supply on time.
- Non-availability of supplies and delayed transportation.
- $\circ~$ Quality issues due to available supplies
- Customers could not get product/service
- $\,\circ\,$ Support staff issues due to lock down and travel restrictions

See ISACA.

Political risk	Environmental risk	Social risk	Strategic risk
Operational risk	Information Technology and Security related risk	Human resource related risk	Legal and regulatory compliance risk
	Economic risk	Concentration risk (single point of failure)	



- Political risk—Unstable regimes, closed borders, customs and tariffs may affect suppliers.
- Environmental risk—Natural disasters (floods, fires, etc.) and epidemics may affect the supplier area and disrupt logistics and the supplier workforce.
- Social risk—Industrial unrest, labor actions, strikes, sabotage and crime may affect supplier and partner locations.
- Strategic risk Risk associated with inappropriate strategic decision.

 \odot Defining incorrect products or services

- Selecting suppliers based on few attributes from among quality, cost, legal and regulatory compliance, dependency, financial stability and logistics.
- \circ Absence of frameworks within an organization to manage suppliers.
- \odot Extend the same supply chain concepts to the functional areas.



- Technical / operational risk
 - $\,\circ\,$ Machine or equipment failure
 - \circ Supplier product and services are not aligned with organizations production plans.
 - $\,\circ\,$ Quality of supplies introduces rejection in final stages of production.
 - \circ Supplier service priorities are not aligned with organization's requirements.
 - \circ Supplier operations are interrupted due to one or more threats.
 - \odot Human mistakes and errors.



- IT and Security risk
 - Supplier's security implementation is weak and not at par with organization's expectations.
 - Weaknesses and vulnerabilities in application resulting in operational failures and frauds impacting organization and stakeholders.
 - Failure of supplier in providing services due to a cyber security incident or attack.
 - Weak continuity planning of the supplier impacting services provided. This can also happen when the continuity plan of supplier and organization are not aligned.
 - Provision of inadequately skilled human resources by the supplier resulting in quality compromises and/or operational issues.
 - Inadequate testing of applications developed and maintained by the service provider resulting in vulnerable applications that may leak information or face cyber-attacks or face operational interruptions.



- Human resources in supply chain:
 - Skills and competency are compromised for cost. Supplier do not have promised skilled human resources.
 - Outbreak, epidemic , pandemic or any such threat
 - \odot Attrition or turnover of skilled
 - \odot Performance of human resources
 - Organization's cannot control and monitor supplier's human resources disputes/issues/problems.
 - Human resources are the weakest link in information security.
 - Impact of regulatory framework on resource availability and failure of organization in diverting another channel for making resources available.



- Legal and regulatory compliance risk
 - \circ Suppliers may fail to comply with legal and regulatory requirements
 - \circ When a supplier provides service direct to customers
 - $\,\circ\,$ When supplier is located in different geo-political environment
 - $\,\circ\,$ Conflicting compliance requirements for supplier
 - $\,\circ\,$ Supplier fall under court order to stop work at a given location.
- Economic risk—Financial instability and lack of cash flow can cripple day-to-day supplier operations.
- Concentration risk (single point of failure)—
 - Dependency on single supplier / Lean model (All eggs in one basket)
 - Industry concentration a single niche supplier or vendor provides fundamental services or infrastructure to an entire industry (e.g., SAP, core banking software, processor chips for hardware manufacturers, industry-specific technologies and robotic automation).
 Geographic concentration



Building resiliency

- Governance framework
- Understanding supply chain partners
- Associated Risk and mitigation processes
- Use of automation



How to build resiliency?



- Establish centralized Supply chain Governance committee
- Framework must provide for:
 - Central inventory
 - \odot SLA and performance monitoring process
 - Change management for suppliers
 - Periodic review of various supply chains against organization's objectives

Supply Chain - Governance Framework





Role of Steering Committee

Policy and Guidelines



- Policy for Supply Chain management to include:
 - \odot Areas where suppliers are to be used
 - \circ Supplier categorization guidelines
 - \odot Selection criteria for suppliers covering basic risk
 - Performance measurement Score card for suppliers
 - \odot Constitution of Steering committee

Supply Chain Framework – Process Cycle

See ISACA.

- Define uniform process framework for selecting Supply chain partners **Renew**, retire Consisting of procedures and guidelines or replace for steps defined ○ Identify requirements for supplier Performance assessment • Define relationship, skill and quality for supplier • Define service levels and timelines Monitoring Conduct Risk management and reporting
 - $\,\circ\,$ Select supply chain partners
 - Contract and SLA
 - \circ Establish monitoring process
 - Monitoring and reporting
 - Performance assessment
 - Decision on Renew, retire or replace



Understand relationship



- Identify and categorize supply chain partners
 - Strategic: Where dependency may or may not be very high but are important for organization.
 - Tactical: that helps in manging operations. Cannot be replaced easily.
 - **Commodity**: Suppliers of material and spares. Redundancy for continuity.
 - Niche: provider of exclusive product and services without which it will be difficult to sustain. Almost impossible to replace and hence critical for continuity.
- Also consider:
 - How important is the supplier to the organization?
 - \odot How important is the organization to the supplier?

Continuity Considerations

- Continuity Considerations focus
 - \circ Cost savings
 - \circ Improved efficiency
 - $\circ\,$ Reduced waste
 - \circ Higher growth
 - Customer loyalty
- Align business continuity plan by considering supplier's continuity plans.
- Involving suppliers while testing business continuity plan
- Participate in supplier's BCP testing.
- Analysis of test result to adjust continuity plan
- Ensure Supplier has aliened their BCP with that of sub-suppliers



Proactive approach



- SMART Supply chain : Use for emerging technologies like AI, IoT for monitoring the supply chains.
 - Intelligent work flows
 - \circ End-to-end visibility
 - Supplier collaboration
 - Order management
- Compromise between Lean and Agile supply chain
- Consider diversifying in emergency e.g. Replace physical delivery to e-delivery or use of Online meeting solutions
- Establish better communication between supply chain partners to detect issues in time.

Summary



- Failure of supply chain has adverse effect on organization although it is supplier that failed reputation of organization is at stake.
- Monitoring supplier performance linked with objectives is important.
- Linking continuity plans so as to get early warnings and sufficient lead time to diversify.
- Always have back up plan when supplier is likely to face interruptions

Open session





Thank You