the newsletter of Reliability, Maintainability, and Supportability

September 2018
Volume 22
Issue 3

Inventory Management: Bedrock of Supportability by Lloyd H. Muller

Supportability is predicated on having the right materials on hand at the right time for use by maintainers. If they aren't there, the airplane, tank, car or whatever is broken remains so. It's useless. This article will review the basics of ensuring the availability of materiel by exploring the concept of Economic Order Quantity (EOQ) analysis.

Materiel availability is the outcome of good inventory management. Without it, stock out costs are incurred. Commercial airplanes are grounded. Trucks can't haul goods. Taxis can't carry their passengers to their destinations. Military units can't move forward in combat. All this spells lost revenue or failed mission accomplishment. The importance of adequate inventory is clear.

To ensure a common understanding of what inventory is, here is a definition: "The number of units of and/or value of stock of goods a company holds [for future use]." This stock essentially has two costs. The first is the cost of the stock itself and all of the elements involved with its direct management. That is, there are costs of capital, warehousing, taxes, insurance, depreciation

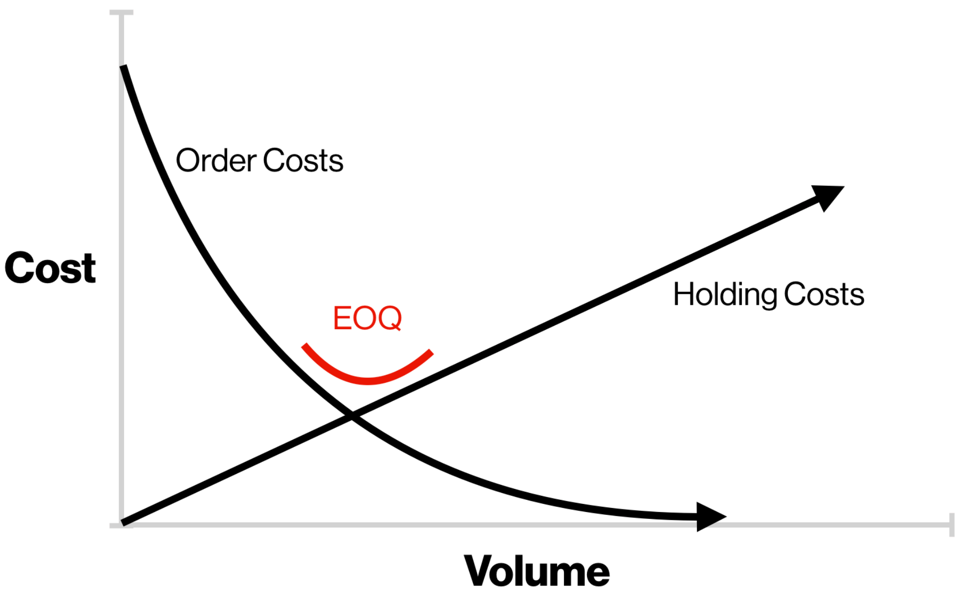
Continued on Page 2

Unreliable Infrastructure: Pay Less Early-on or Much More After Failure by Russell A. Vacante, Ph.D.

There is a failure in the United States to either recognize and/or make the building and maintenance of a reliable infrastructure a high priority. Not very long ago the United States had an infrastructure that was the envy of the world. This is no longer the case. Much of our infrastructure is old and in a state of needed repair. Our infrastructure has fallen victim to the often faulty thinking in our defense community and other major institutions that economically and socially determine the safety and general well-being of our socio-economic fabric. Poor understanding of or neglect of a fundamental system engineering principle on the part of our national leaders is to blame. Having an infrastructure in which reliability requirements are a major life-cycle design factor is less expensive than having to pay the bill of replacing or repairing infrastructure after an environmental or man-made national emergency.

Throughout our life-time we have experienced Hurricane Okeechobee in 1928, Hurricane Katrina in 2005, Hurricane Harvey in 2007, Hurricane Hugo last year and currently the vast destruction of the Carolinas caused by Hurricane Florence, just to mention a few natural disasters that are costly to life and the national economy. One life lost due to

Continued on Page 13



and obsolescence. These costs are summarized as holding costs and are expressed usually as a percentage of the inventories' value.[1] The second are those ordering costs associated with resupplying exhausted inventory levels. They include the cost of the processing of orders, fixed costs such as personnel and information systems, and transportation.[2]

The conundrum presented by these two costs is that they conflict with each other. That is, if the purchasing manager buys large quantities to enjoy volume discounts in stock costs and transportation rates, the inventory manager suffers increased holding costs. As one goes down, the other goes up. Here is a graphic illustration of this situation.

The trick to solving this conundrum is finding a balance between the two elements and derive a lowest overall cost. This means that the cost advantages of both elements must be sub-optimized in order to get an Economic Order Quantity.

There is fortunately a formula that derives the EOQ. It is cited here:

The definitions of the formula's components are:

$$Q = \sqrt{\frac{2RA}{VW}}$$

Q = EOQ
R = Total annual stock requirement
A = Order costs
V = Unit cost (price)
W = Holding cost percentage

Here is an example:

Price (V) = \$50/unit @ < 2000 units
Annual usage (R) = 4000/year
Carrying cost (VW) = 0.20
Order Costs (A) = \$50
EOQ = 200 units/order

To determine this order quantity's cost, managers use a Total Annual Cost formula that is cited here:

$$TAC = \left(\frac{1}{2}QVW\right) + A\frac{R}{Q}$$

Using the same definitions and data from above, the Total Annual Cost equals \$1,020.00. If readers enter any other volume for Q, costs will rise. It doesn't make any difference whether the factor is larger or smaller, the resulting cost will be higher.

Now there are important assumptions that must be understood.

1. Demand is constant and fulfilled.
2. Replenishment time is constant (response time between order entry and materials receipt).
3. Costs are constant.
4. No inventory is in transit.
5. Each item has its own EOQ and no interaction exists between different items.
6. The planning horizon is unlimited.
7. Purchasing capital is unlimited.

Clearly, industrial processes are not as stable as demanded here, and accommodations must be made for them. This means that the EOQ formula must be altered to account for conditions of uncertainty. Discussing these issues is beyond the scope of this paper. What is important, however, is understanding the basic theory of EOQ. Whatever conditions exist for any particular situation, this basic theory remains unchanged.[3]

Many readers of this article will cite modern management concepts such as Just-In-Time (JIT) inventory supply and ask, does EOQ apply? Its premise is that inventory on hand is a cost that must be avoided at all costs. Large manufacturers use it all the time. In fact, Lee Iacocca cites it as being an important part of his

[1] Coyle, John J., et.al. The Management of Business Logistics: 5th Edition. St. Paul, Minn., 1992. Page 564.

[2] Coyle John J., el al. Supply Chain Management: A Logistics Perspective, 10th Edition. Boston, MA: Cenage (Is this word correct? Learning, 2017. Page 303.

[3] Ibid. Page 317

THE BALUSTER GROUP

SDVOSB SERVICE DISABLED VETERAN-OWNED SMALL BUSINESS

Management Expertise • Engineering Experience • Strategic Insights

Management & Technical Expertise

The BALUSTER Group is a Service Disabled Veteran Owned Small Business (SDVOSB) that solves challenging management and technical questions. The company has competencies with regulatory, engineering and technical expertise, as well as, claims and litigation experience. BALUSTER's management and engineering consultants are experts in their fields and provide clients access to a full range of management, engineering, scientific and regulatory capabilities.

The company's core strength lies in its' management and technical personnel's comprehensive multi-disciplinary expertise and practical experience. With advanced degrees (Ph.Ds, MBAs, M.Eng, etc.), regulatory expertise and industry knowledge, BALUSTER's team is uniquely capable of addressing a wide range of projects, regardless of complexity or timeline.

The BALUSTER Group Team

The BALUSTER Group's Federal team offers a unique collaborative approach to solving problems that focus on appropriately staffing each engagement with the best-suited subject matter experts. This allows our clients to leverage the depth of knowledge held across our management and technical practice groups.

www.theBALUSTERgroup.com

To learn more about the BALUSTER Group Federal team, call at (571) 334-4807, or send an email to cjbonanti@theBALUSTERgroup.com

SDVOSB SERVICE DISABLED VETERAN-OWNED SMALL BUSINESS

The Federal team is comprised of former senior executives from the U.S. government, business management executives, senior level engineers, policy analysts, and researchers.

COMPANY CAPABILITIES

- Accident Investigation & Analysis
- Aircraft Accident Reconstruction
- Applied Mechanics
- Automotive Accident Reconstruction
- Automotive Defect Analysis
- Automotive Regulatory Compliance
- Automotive Research & Testing
- Autonomous Vehicle Technology Integration & Policy
- Aviation Operations and Policy
- Block Chain Integration
- Chemical Engineering & Analysis
- Child Product Safety
- Commercial Vehicle Operation, Safety and Regulations
- Consumer Product Safety
- Crash Avoidance Technologies
- Crashworthiness
- Design Analysis
- Energy Analysis & Integration
- **Engineering Consulting**
- **Environmental Engineering & Science**
- Fire & Explosion Investigation & Analysis
- Hazardous Material & Waste Transportation
- Heavy Trucking & Commercial Vehicles
- Industrial Hygiene & Incidents
- Infrastructure
- **Management Consulting**
- Mechanical Engineering
- National Environmental Policy Act (NEPA)
- Railroad Technology & Safety
- Regulatory & Compliance
- Research & Design
- Risk Assessment & Analysis
- Safety Analysis & Engineering
- Statistics & Reliability
- Transportation Engineering & Research

successful recovery program for Chrysler's return from bankruptcy during the 1980s.[4] However, the EOQ model still plays an essential role in the JIT concept. It just means that ordering costs have been driven down to the point where inventory levels can be driven to zero. One cost is substituted for the other in order to derive an EOQ level.

So, there you have it: the down and dirty of an important element of any successful support program. Inventory is a complex and costly element of logistics. If it is not managed effectively, costs will rise and support to any program will suffer. Do it right, and managers are renowned as geniuses. The choice is simple. ■

About the Author

Dr. Lloyd Muller is the Vice President of the RMS Partnership Inc. His academic duties include course design and development and the teaching of online and onsite logistics courses. He also a contributing author to the RMS Partnership's quarterly newsletter and semi-annual professional journal. Dr. Muller is a widely published author with numerous books, articles and reviews to his credit.

As a manager, Dr. Muller served 30 years as a USAF officer in numerous logistics positions (with professionally increasing responsibilities-- his last position as colonel was that of Deputy Commander of Logistics of the 16th Air Force providing direct support to the Allies in Operation Desert Storm). As such, he managed programs and activities dealing directly with every facet of logistics both in the United States and abroad. Much of this experience involved diplomatic dealings with member nations of NATO. Subsequent to his military retirement, Dr. Muller served as a consultant in behalf of the Department of Defense in support of foreign military programs. He is fluent in Italian and German due to his varied experiences in the Mediterranean and Middle Eastern cultures.

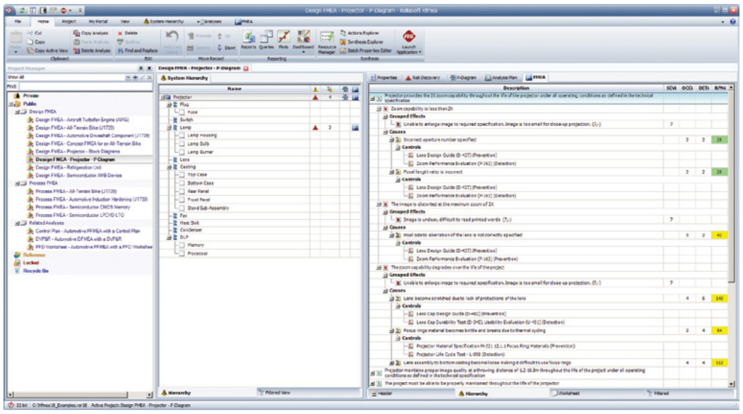
Academically, Dr. Muller started his fulltime career as an Assistant Professor for Embry Riddle Aeronautical University (1991–1993). Before this assignment, he taught logistics in Turkey at the Middle East Technical University, business courses for the University of Maryland and statistics for La Verne University. He has also taught logistics as a contract professor at the US Navy Supply Command. Currently, he is an associate professor of management with the Florida Institute of Technology. Of particular importance there was his development of their graduate logistics curriculum.

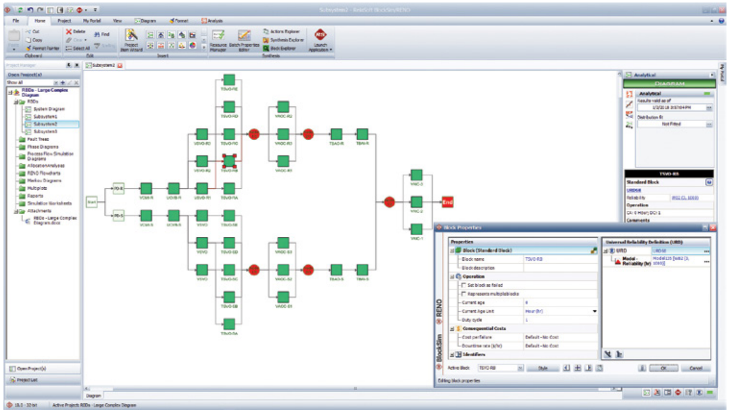
[4] Iacocca, Lee. Iacocca: An Autobiography. New York, NY: Bantam Books. 1984. Page 186.

Prenscia HBM

Reliability and maintainability software and services

ReliaSoft promotes the use of engineering methodologies to evaluate and improve reliability and maintainability through software, services and solutions. Our products facilitate a comprehensive set of reliability analysis techniques, including life data analysis (Weibull analysis), quantitative accelerated life testing, system reliability/maintainability, reliability growth, design of experiments, standards based reliability prediction, FMEA, RCM, RBI, FRACAS and others. We also offer an extensive curriculum of reliability training courses that provide thorough coverage of both the underlying principles and theory, as well as the applicable software. Total life cycle support and expert resources are available on demand for organizations and projects of any size.





ReliaSoft

www.hbmprenscia.com

Supply Chain Cyber Security by Katherine Pratt

In 2008, the National Institute of Standards and Technology (NIST) Supply Chain Risk Management (C-SCRM) program initiated the development of C-SCRM practices, a multi-pronged approach for non-national security systems, such as global supply chain risk management.

Today, supply chains (SC) have nested systems such as sourcing, quality, continuity, vendor management, as well as many other functions. They have three major global markets: U.S., Europe, and Global. These retailer/channel level ecommerce retailers are considered 'Fast Moving Consumer Goods' (FMCG), and considered a global growth driver!

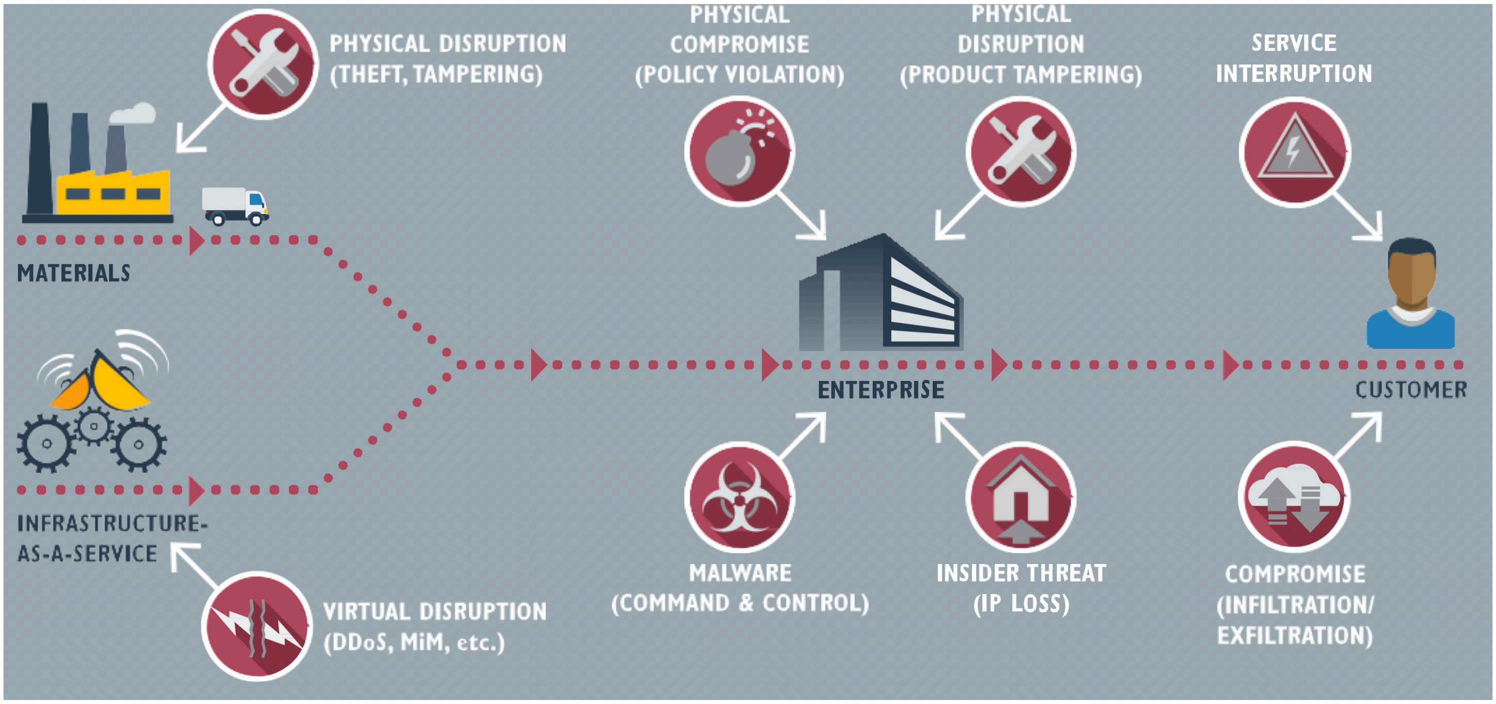
SC security is a program that focuses on potential risks associated with an organization's external suppliers of goods and services. Many of these suppliers may have extensive access to resources and assets within the enterprise environment or to an organization's customer environments, some of which may be sensitive in nature.

There are many ways a supply chain breach could occur. For example, a software manufacturer could be breached via malware that modifies source code, which then may be distributed to other user enterprises. Another compromise vector might be the theft of a vendor's credentials that enable remote access to an enterprise the vendor works with, thereby leading to infiltration of the enterprises' network from a perceived trusted source—the vendor network.

In the past several years, there have been many high-profile breaches with SC involvement, such as the retailer Target, whose theft included roughly 110 million customers' data, and over 40 million payment cards' information. This breach was accomplished through one of their vendors: Fazio Mechanical Services. In 2015, the U.S. Office of Personnel Management (OPM) had a breach of 22 million records, including sensitive data to numerous federal employees, contractors and military personnel.

As these attacks have become more sophisticated, the data breaches have included intellectual property, and sensitive government information. In 2015 the U.S. Office of Personnel Management (OPM) revealed a massive breach of 22 million records, including sensitive data tied to numerous federal employees, contractors, and military personnel. These breaches originated from stolen credentials from OPM background-check providers, and security vendors, such as RSA Security, LLC, which is a subset of Dell Technologies.

When sensitive data has been breached and exposed, the impact to


PHYSICAL DISRUPTION (THEFT, TAMPERING)
PHYSICAL COMPROMISE (POLICY VIOLATION)
PHYSICAL DISRUPTION (PRODUCT TAMPERING)
SERVICE INTERRUPTION
MATERIALS
ENTERPRISE
CUSTOMER
INFRASTRUCTURE-AS-A-SERVICE
VIRTUAL DISRUPTION (DDoS, MiM, etc.)
MALWARE (COMMAND & CONTROL)
INSIDER THREAT (IP LOSS)
COMPROMISE (INFILTRATION/ EXFILTRATION)

organizations and consumers (i.e., users of the business' products) is extensive and includes financial penalties, legal costs, loss of consumer confidence, adverse stock prices, and damage to reputations. The damage further extends into loss of consumer confidence, stock price drops, and loss of professional reputations. Furthermore, the customers (purchasers of business products), who can then become the targets of phishing attacks, identify theft, as well as then having to deal with replacing their payment cards and bank accounts. In 2015, the average cost to an organization for a data breach was $6.5 million U.S.[1]

Despite the growing threat and evidence surrounding the supply chain attack vector, there are few specific compliance mandates addressing third parties, even though third-party risk is usually implicated in a number of other areas, as for example: vendor due diligence, risk management and contract requirements. However, some compliance and regulatory bodies have issued guidance explicitly dealing with vendor management and third party risk.[2]

This guidance describes how to evaluate contracts with vendors and other organizations, in building a Vendor Management Program as well as which types of controls and best practices to look for when evaluating the use of third-party services (i.e., using due diligence) *before* they are contractually engaged.

Building a Vendor Management Program

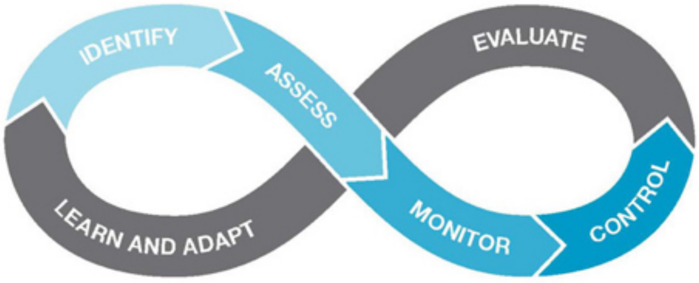
1. Define and Rank Your Vendors
2. Specify Each Vendor's Primary Contract(s)
3. Establish Guidelines & Controls to Ensure Consistent Processes
4. Integrate Each Organizations' Assessment and Audit Practices

When defining your vendors, identify which vendors are "mission critical," and in whose performance would strongly affect revenue generation or adversely affect clients, or the organization as a whole (i.e., through direct contact or loss of sensitive data), or where it may be difficult to find an appropriate or timely replacement. Examples of such vendors may include important partners, financial or legal services, hard-to-find software vendors, and the like. Different tiers of criticality will require separate approaches to policy enforcement.

Next, you will need to define a primary contact that can effectively serve as a liaison between your organizations' security, risk and compliance teams for each vendor. The assigned individual(s) using judgment and expertise will conduct a risk-based approach, as well as standard processes and categorizations on the vendors and report to senior management.[3]

So, you may wonder where to begin? Organizations should evaluate their vendor management programs addressing SC security; all roles and responsibilities will need to be defined and managed using a risk-based approach both internally as well as externally. A risk-based approach is a methodology that enables prioritizing activities based on previous analysis of data, as well as maintaining continuous diagnostic and mitigation compliance.[4]

Begin by creating an action plan for each supplier. Possible actions include the initiation of a development plan, a sustainability plan, a sustainability audit, and/or the phasing out of a supplier. It is good practice to examine relevant compliance and



Risk Management Framework (RFM)

[1] "2015 Cost of Data Breach Study, United States," Paneman Institute Research Report, May 2015
[2] www.fdic.gov (Use search term "fi108044a")
[3] "Combating Cyber Risks in the Supply Chain," by Dave Shackleford, Sept 2015
[4] "Solutions – Risk Management Framework" https://www.steelcloud.com

standards' frameworks to see how they apply to your organization and its security posture. Various tools can be used to manage SC risk, such as:

Audits: Conducting regular audits is a key component of a robust risk management framework, allowing organizations the ability to uncover issues before they become significant problems for the organization.

Certification: All supplier risks should be addressed, such as bribery, corruption, child exploitation, poor environmental practices, and potential breaches of legislation and or regulations.

Training: Consideration should be given to provide training to suppliers as well as their own staff, to reduce the risk of its suppliers engaging in conduct that may affect the brand of the organization.

Cyber Risk Surveys: When procuring software, by deploying automatically scheduled cyber risk surveys to both potential and current vendors, this is a way to ensure suppliers comply with an organization's IT security standards.

The Internal Risk-Based Approach

The internal approach is based upon the internal supplier qualification process, as well as upon regular supplier quality audits; these processes should be designed to systematically identify SC potential sustainability risks. Any supplier not meeting the pre-defined threshold, is then evaluated individually, and steps are created to either bring them up to the new required level of standards or be replaced.

The External Risk-Based Approach

In order to better identify potential SC risks, external sources, such as non-governmental organization (NGO) databases, media reports or information from your compliance ombudsman, may be used. Reports of suspected breach of the Code of Conduct requirements, must pass through a 'clearing process' to determine the next steps to be taken. Examples include an external sustainability audit, or an incident-driven inspection focusing on the identified breach. In order to achieve a complete risk screening for a particular portfolio, a risk-mapping framework, containing both country and commodity mapping should be created.[5]

Country Risk-Mapping

Several sustainability risk indicators, such as water scarcity, human rights, or corruption, comprise the country's risk-mapping framework.

Commodity Risk Ratings

Incorporating sustainability into the SC provides focus not only on countries, but also on commodity categories. These categories of environmental, labor practices and occupational health and safety are rated in terms of the risks involved in sourcing different materials.[6]

According to various Supply Chain Resilience reports the top causes of disruption are:

- Contaminated foreign food products[7]
- Unplanned IT and telecommunications outages;

[5] https://www.sustainabilityconsortium.org/projects/commodity-mapping/

[6] https://w5.siemens.com/cms/supply-chain-management/en/sustainability/detection/risk-based/pages/approach.aspx

[7] https://www.theguardian.com/australia-news/2017/jun/02/frozen-berries-recalled-as-precaution-while-tests-for-hepatitis-a-continue

WHERE…commodities are produced for different supply chains

WHAT…potential issues or risks occur in these commodity-producing regions

HOW…a user can address these issues by utilizing KPIs and working with partners on the ground

- Cyber-attack and data breach; and
- Adverse weather[8]

In 2015, fruit contaminated with hepatitis A virus from brand "Creative Gourmet" of frozen mixed berries was imported from China and Chile, but was packed in AU. (1) In 2017, the Australian health authorities still continue to find new cases of the affected strain of hepatitis A virus. This is an example of retail organizations held accountable for supplier inadequacies. Outsourcing key functions does not mean the retail organization is immune to reputation damage as a result of third party supplier actions.[9]

Climate Change is another consideration for sourcing supply chains less prone to the affects of increasing flooding due to climate changes. For instance, many parts of India suffer flooding every year during the annual monsoon rains from June to September. In December of 2015, due to record amounts of rainfall, complicated by a denser 'cold pool' of air in that mountainous region which 'trapped' the clouds enabling over 19.5 inches (494 mm) of rain in less than 24 hours, created devastating flooding conditions.[10]

Increased globalization of the SC market, has resulted in almost every organization to interact with a foreign entity in its supply chain, often without even being aware that they are engaging with foreign companies, or being aware from whom they are actually procuring goods and services. Furthermore, if an organization involved in the global marketplace engages with a third party domiciled overseas with no operational presence in the U.S., that is not governed by the laws of the buyer, it is not likely to be subject to the jurisdiction of the U.S. legal system. Furthermore, supplier location and the costs associated with traveling there to undertake an audit, plus potential language barriers, differences in foreign accounting requirements, and cultural challenges, such as religion or even if the intended auditor is male or female, may complicate the ability to conduct an audit. There are a variety of other legal considerations—such as bribery, and corruption, regulatory compliance, etc., but the key take-away is that all parties should have a detailed understanding of the various legal and regulatory risks, and have a range of legal and other strategies in place to mitigate these risks accordingly.

The risks associated with managing a supply chain are many and varied and include:

Continuity of Supply: Ensuring that sufficient goods and services are available to allow an organization to operate or fulfill client requirements (i.e., Minimum of Production and being "fit" for purpose); [Supply-Chain-Risk-Management-White-Paper-Final.pdf, Chapter 4 & Schedule 2 of the Competition and Consumer Act of 2010] – *Note: If a key supplier fails in its contractual obligations, they could face a range of penalties, including liquidated damages and termination of the contract.*

Regulatory: Including breaches

[8] "Supply Chain Risk Management White Paper, Final" https://www.rmia.org.au/wp-content/uploads/2016/12/Supply-Chain-Risk-Management-White-Paper-Final.pdf

[9] https://www.theguardian.com/australia-news/2017/jun/02/frozen-berries-recalled-as-precaution-while-tests-for-hepatitis-a-continue

[10] "A Look Back Into the December 2015 Floods of Chennai – What Role Did The Eastern Ghats Play? https://researchmatters.in/news/look-back-december-2015-floods-chennai-%E2%80%93-what-role-did-eastern-ghats-play

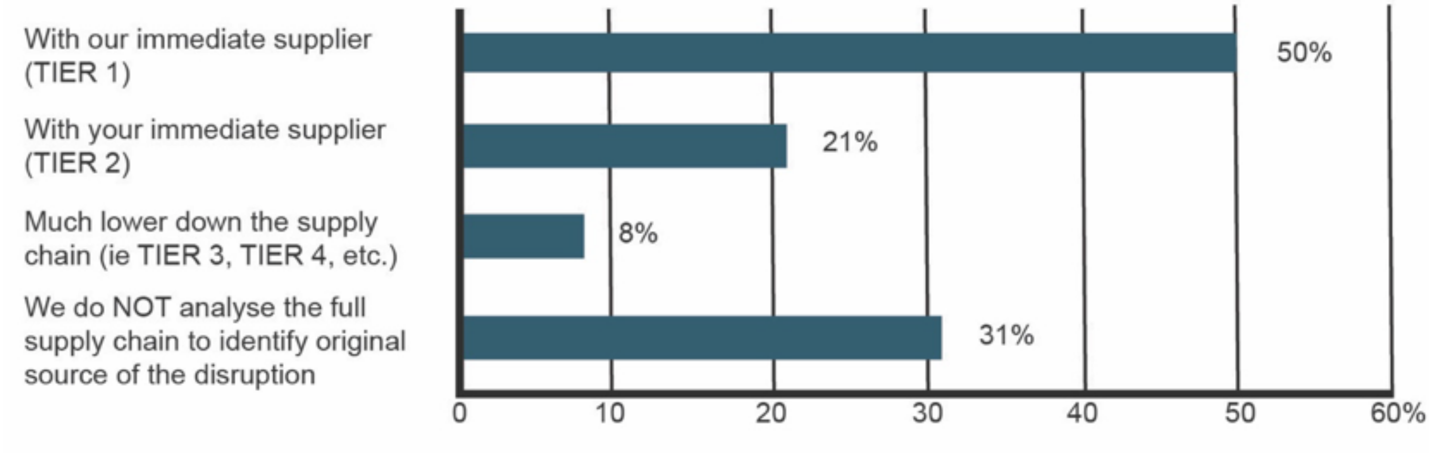


Figure 2: Tier level where incidents occur.

*Tier level where incidents occur ("Supply-Chain-Risk-Management-White –Paper-Final.*pdf) of bribery and corruption legislation (Competition and Consumer Act 2010) and relevant environmental laws;

Legal: Such as breaches of contract, rights to audit and jurisdictions; and

Quality: Particularly the supply of goods and services, which are not fit for purpose.

The most common reasons for the failure to report SC incidents include: the existence of silos within organizations, which impede reporting; and a lack of priority given to an SC risk management by senior management.

These issues of lower level SC disruptions, therefore, increase the importance of developing an organization-wide basis for increased visibility over all suppliers.

SC disruptions have a number of sources and origins, and many organizations do not have a process to report these types of incidents, or even by which country and firm the products originate from.

Effective SC management is lacking because of the complexity of international interfaces, which result in reporting disruptions and hinder visibility over suppliers. This key lack of knowledge is a possible point of failure for organizations impacted by supplier failures. It is paramount that employees at all levels continually identify and manage risks in their areas of responsibility. Senior management should be involved with strategic risks, whereas the procurement staff should focus on tactical issues.

Key Risk Identification areas include:

- Routine supply chain risks include: unexpected transit delays, or changes in customer orders, or problems with suppliers.
- Natural disasters—although these are unpredictable, effective organizations can anticipate disruptions and develop contingency plans.
- Political and civil unrest should be considered, particularly in the context of the countries from where relevant suppliers reside.
- Laws and regulations, including the potential unexpected application of new regulations in a particular country, or even changes to relevant pre-existing regulations.
- Terrorism acts, although not frequent, often result in additional SC costs from increased security and other requirements.
- Technology is not impervious to failure, and therefore, can be an impediment in the implementation of SC activities.

The challenge is to recognize the *full* scope of SC network, and its inherent vulnerabilities.

In implementing a risk program, there are four key processes needed to ensure effective management supply chain risks are mitigated and managed:

1. **Risk identification:** Understanding where the risks are. It is vitally important that SC organizations be aware of their SC vulnerabilities, including the sources of risk, as well as how to manage each of their risks to increase control and achieve justified confidence in their SC processes.
2. **Risk Assessment:** Deciding on how critical the risks are to the ongoing operations of the organization. Undertaking a SC Risk Assessment is essential for any organizations' success, as it provides improved skills and capabilities to be able to define and develop assured quality and safety practices in the growing field of SCM. Being small, lean or operating on smaller margins, providing just-in-time service and or supplying a single product amplifies the impact of supplier disruptions.
3. **Risk Treatment:** Developing strategies to manage the risks. SC threats vary from natural disasters, political instabilities, or even becoming involved in another's organizations' disputes. To better manage these and other threats, an organization needs to know where their suppliers are located, what susceptible events affect the regions in which their suppliers are located, which suppliers are critical to the Organization and defining what types of events suppliers may be susceptible to that may disrupt the SC processes.
4. **Risk Monitoring:** Allowing organizations to understand changes in the supply chain and anticipate potential issues before they become problems. Developing an effective strategy to mitigate all of the SC issues requires risk or business continuity managers to educate and inform procurement workers to better understand which suppliers are critical to their organizations' continuity of supply. Your organization's procurement personnel need to better understand all of the business

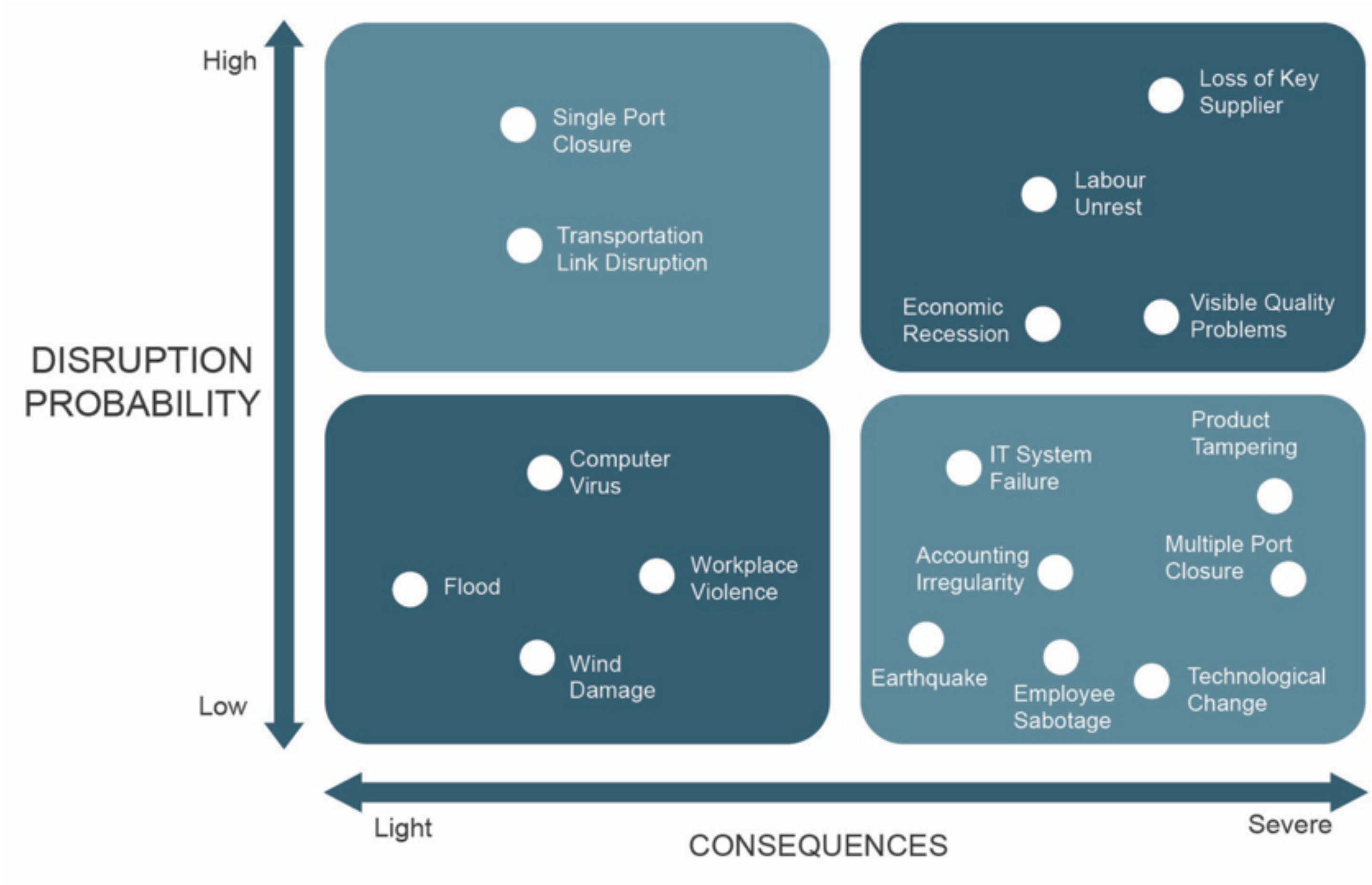


Figure 3: Vulnerability Map

Massachusetts Institute of Technology Paper, vol. 47, 2005) Supply-Chian-Risk_Management-White-Paper-Final.pdf

consequences of losing suppliers, so supplier selection should be made not only upon commercial grounds, such as cost, but also on a supplier's resilience to disruption in their operations.

5. **Risk Strategy:** An Organizations' supplier strategy to mitigate risk should include:

- The use of redundant supplier's products and or services.
- Enforceable contractual obligations, which require suppliers to maintain secondary sources of materiel.
- Enforceable penalty clauses, that are subject to supplier failure to deliver goods and services as per their contract.

In evaluating a potential supplier, Procurement should consider:

- The quality of all of the supplier's products and or services – not just the one being supplied;
- The history of all previous incidents.
- "Key Person" dependencies.
- Financial stability.
- Supplier capacity.
- Their business continuity planning.

Staff with business continuity knowledge should support the procurement manager in assessing each supplier's level of business continuity planning as regards to its internal product(s) validity, quality systems and practices.

Subsequent to a supplier being contractually engaged, a Supplier Relationship Manager should be assigned to monitor the Supplier in areas such as:

- The performance and quality of the supplier, with any drop in quality being investigated as potentially indicative to potential problem or failure.
- Near misses in quality may indicate potential major issues, such as Occupational Health Services (OH&S) breaches.
- Any suppler mentioned in the press or online regarding any issue such as scandals, financial irregularities, or pending legal actions against the supplier.[11]

A way to track supplier vulnerabilities is through an Enterprise Vulnerability Map to categorize the relative likelihood of potential threats.

[11] Risk Management Institution of Australasia (RMIA), White Paper: "Managing Supply Chain Risk", November 2016, by Guy Underwood

Threat Analysis

Cyber threats are potential cyber events emanating from unintentional actions or as a result of attacks developed by malicious parties that exploit vulnerabilities and that can cause harm to a system or an organization.

Consideration must be given to threat origins, taxonomies of threats, influential environmental trends, and systematic prediction of emerging threats. Analysis of these aspects cannot be a static concept; the cyber domain is rapidly evolving thus requiring a continual process of monitoring and adapting to emerging threats.

Perpetrators and Their Motivations

The perpetrator of cyber attacks, (also known as 'threat actors'), include individuals (unintentional or malicious), issue-motivated groups, organized crime, business competitors, terrorists and nation states. The sophistication of these actors can range from non-technical opportunists through to well-founded, long-term strategic technical innovators. Perpetrators may also have one or more specific motivations driving their behaviors.

There are numerous motivations that drive these perpetrators (aka threat actors) to conduct cyber attacks. Some actions are malicious, others acts could be non-technical, opportunistic, or even unintentional. Whereas most are likely to be well funded, long term strategic technical innovators with one or more specific motivations driving their behaviors.

Perpetrator Motivations

Gain Notoriety

Undermine Confidence Destabilize a Country

Revenge

Gain Competitive Advantage

Effect a Change of Government

Elevate status within own clique

Influence Opinion

Shutdown Enemy/Offensive/Defensive Systems

Financial Gain

Steal Intellectual Property

Conduct Espionage

The Threat Landscape

One example of a future threat is that of Hardware Trojans. This is a type of threat that can be inserted into electronic circuits, at any stage of design and development, manufacturing, distribution or maintenance, and include system level changes, such as adding chips, circuitry, or changing existing chips by introducing new logic functions, or subtle physical process variations during the manufacturing process. For example, in 2008 the EFTPOS chip and pin machines being built in China were tampered with either during manufacture or shortly after coming off of production, and then resealed. These allowed for financial credentials to be recorded at point of sale, stored, and later forwarded via embedded cell phone circuitry, to overseas criminal gangs.[12]

Companies are outsourcing their SCs because the return on assets metrics gives advantage to companies that have outsourced their SCs and thus have lower assets bases.[13]

One cannot help but wonder if in the long term, this assets management advantage is really only a short-term gain.

The various tools and processes addressed herein should not be considered as all inclusive, as the global market is always changing due to internal and external pressures, and therefore, the need for constant world market-analysis is a given if you plan to use global SC market options. It is critical to remember when the SC gets 'broken,' it is often the organizations' brand that will be impacted, not the supplier's. Therefore, SC risk management plays a key role in ensuring the sustainability of any organization, and must be dealt with appropriately across the entire organization's global supplier network. ■

About the Author

Katherine Pratt holds a B.A of Business Administration in Management Systems from the University of Iowa. She is president of Enviro-Logistics Inc., West River, Maryland and has provided comprehensive services to agencies and corporations in the areas of Access SQL, technical writing and contract administration. She has been a professional logistician and contracts administrator for over 17 years, currently serves as the Coordinator of Environmental Affairs for RMS Partnership Organization and has been a member of the Board of Directors for the Society of Logistics Engineers (SOLE).

[12] http://www.telegraph.co.uk/news/uknews/law-and-order/3173346/Chip-and-pin-scam-has-nettedmillions-from-British-shoppers.html

[13] "Another View of Best Supply Chains", by Dan Gilmore, Editor of Supply Chain Digest; http://www.scdigest.com/firstthoughts/18-06-15.php?cid=14330

Editorial, from Page 1

faulty infrastructure is one life too many. Those on the receiving end of deaths and injuries resulting from infrastructure failure know too well the pain and suffering associated with such a situation. However, the reported 2500 deaths due to the Okeechobee hurricane, the 1200 deaths resulting from Katrina or the 2975 deaths reported by Hurricane Maria in Puerto Rico does tell us something about our national priority interest when it comes to building and caring for our infrastructure.

It is sadly ironic that our national government and business leadership can provide costly, but often insufficient, natural relief funding to repair or replace faulty infrastructure after a natural disaster but little if any, for less cost funding to correctly build and maintain our natural infrastructure prior to a national natural disaster. The loss of life and the enormous amount of property damage caused by a poorly designed and maintained infrastructure, whether it's to our electrical grid, our portal water, our communication systems or our highways and bridges due to a natural disaster, is not acceptable. It is an indication of national leadership failure with respect to providing direction and resources for adopting a life-cycle systems engineering approach to infrastructure design and maintenance. This is an approach that would help ensure that robust reliability requirements are integral to the life-cycle design of our infrastructure.

As the loss of life and damage to property can be mitigated by adopting a systems engineering approach that makes robust reliability requirements a priority, a similar approach should be taken to man-made technology driven 21st century systems.

It is a generally accepted fact that our personal computers, electronic and communication systems are subject to internal and outside intrusions from domestic and foreign actors that can result in a devastating loss of life and much economic chaos. The reports of hacking into our personal computers, our banking and voting systems, as well as electronic grid should serve as a warning of our venerability to attacks on our domestic and national security systems. The potential loss of life and damage to our domestic communication-electronic infrastructure systems can be lessened significantly by implementing a systems engineering, life-cycle engineering approach with robust reliability requirements.

From a national security perspective, the potential for foreign adversaries interfering with our electronic-communications systems to include satellite positioning and communications, logistics and supply chain management systems, central and tactical voice and visual transmissions and receptions, and sensitive design and manufacturing processes is well known by the Department of Defense and related defense industries. Less understood is how to identify the sources, type and frequency of intrusions into our defense communications systems and what needs to be done to increase their reliability in a manner that will greatly reduce bad actor penetration into our systems.

With the advent of advance technologies and our increased dependence both domestically and militarily upon them, enemy nations-states or individuals can, and have, hacked into our systems unseen and from distant shores. The need for our adversaries to physically risk their presence, for example, in placing explosive charges that could damage our domestic infrastructure and military systems and equipment has greatly diminished. However, the advance technology of the 21st century has exponentially increased our domestic and military infrastructure risk to penetration from an increased number of advisories. North Korea, Iran, and a number of non nation-state enemies with sophisticated computer knowledge and skills now have the potential ability to intercept, interfere or destroy our domestic-military electronic communication systems. The resources to launch such an attack are relatively inexpensive while much of the information on how to hack into our systems is freely available on the "dark web" and elsewhere on the internet.

The message of this article is that we need to learn from our past experiences whether it pertains to damage and destruction caused by nature or a result of the evolution of advanced technologies. Our past experience should be an instructional tool that greatly increases our attention and priority to domestic and defense related infrastructure design, care and protection issues from a life-cycle systems engineering perspective. We need to have consistent cogitative awareness that the pervasive worldwide availability of advanced technologies places our infrastructures at greater risk than ever before from an increased number of adversaries that desire to do us harm. Robust reliability life-cycle design requirements can be a major step forward towards safeguarding our domestic and defense related infrastructures. All that is needed is the will and desire of our government and business national leaders to make resources available for establishing a high reliability infrastructure program--prior to rather than after a national disaster. To do so will save lives, cost less, and most likely better secure our national well-being. ■

Interested In Contributing?

If you are interested in sharing your knowledge in future editions, please contact Russ Vacante at president@rmspartnership.org
Articles can range from one page to five pages and should be of general interest to our members.