Issues in Information Systems
Volume 24, Issue 1, pp. 70-83, 2023

DOI: https://doi.org/10.48009/1_iis_2023_106

How an outside perspective can help an organization enhance their supply chain risk mitigation strategy

Fred Hoffman, *Mercyhurst University, fhoffman@mercyhurst.edu*
Rajkamal Kesharwani, *Mercyhurst University, rkesharwani@mercyhurst.edu*
Jacob Maynard, *Mercyhurst University, jmayna35@lakers.mercyhurst.edu*

Abstract

As a consequence of globalization, enterprise supply chains have extended, become more complex, and become increasing vulnerable to disruption. To improve their resiliency to supply chain disruption, both commercial and government organizations have increasingly turned to Supply Chain Resource Management, or SCRM, which requires an enterprise to have full visibility into their supply chain and a shared understanding throughout the organization of supply chain risk. SCRM also requires organizations to periodically rethink and update their risk management strategy. To mitigate the risk of *Groupthink* and other forms of internal cognitive bias, organizations sometimes seek out external expertise when updating their SCRM strategy. In this case, an academic team of specialists from Mercyhurst University was brought in to assist a government client by first examining how comparable civilian and government organizations approached SCRM and then proposing a tailored solution based on risk categorization, quantification, documentation, and analysis.

Keywords: Knowledge management, supply chain risk management, Groupthink

Introduction

Technological advances impact the way business is conducted (Alicke et al., 2017). A century ago, the Ford Motor Company achieved phenomenal business success by exploiting then-recent advances in transportation and communication to create a vertically integrated supply chain, one in which it owned all the sources of raw materials and components used to manufacture their automobiles (Helper & Sako, 2010). Not only did Ford own their own factories, but also rubber plantations in Southeast Asia and a fleet of merchant ships that transported rubber back to the United States to produce automobile tires (Winn et al., 2012). In recent years, such Information Age developments as the internet, mobile telephony, and the drop in cost associated with digitized data storage have similarly spurred changes in business practices (Abdel-Malek et al., 2005).

Strategic sourcing to acquire raw materials and components can now extend corporate supply chains around the world; as a result, two of the more well-known factors increasing both the importance and the risk associated with supply chains have been outsourcing and globalization (Gurtu & Johny, 2021). Since it is neither time-efficient nor cost-effective for the U.S. government to manufacture either finished products or the components of goods ranging from weapons systems to spacecraft, external providers have become increasingly essential (DoD, 2022). Just like commercial firms, then, U.S. federal government organizations now also have supply chains that rely on contracted firms to provide them with raw materials, components, and finished products (DoD, 2022).

The increased risk of supply chain disruption

Because supply chains have become more complex, there has been an increased potential for *supply chain disruption*. Supply chains can be disrupted by a host of different initial triggers, ranging from weather events and pandemics to labor and transportation problems (Gurtu & Johny, 2021). Supply chain disruptions are a more common occurrence than in the past (Labonte & Weinstock, 2022). For example, "the global automotive industry has faced a 30% increase in the number of disruptions from 1,300 in 2016 to nearly 1,700 in 2017" (DuHadway et al., 2018, p. 2). These disruptive events have compelled practitioners to explore the vulnerabilities in supply chains and evaluate risks and possible impacts (Gurtu & Johny, 2021).

Additional supply chain concerns for government organizations

In addition to having the same supply chain risk management concerns as commercial firms, government organizations must also concern themselves with supply chain threats posed by a variety of malicious state and non-state actors (DoD, 2022). Another risk for government entities is a reliance on too few eligible, interested, and qualified vendors. For some government clients, the challenge of having too few suitable vendors is compounded by the fact that the government client may have unique design, construction, or administrative requirements, too small an order, or other complicating factors such as counterfeit products, tampering, theft, malicious software, etc. (Mondschein et al., 2022). These factors all further complicate the supply chain picture (DoD, 2022).

Supply chain risk management

According to risk management theory, the four choices one typically has when considering risk are acceptance, avoidance, mitigation, and transfer (Cagno et al., 2007). One thing an organization cannot do with risk, however, is *eliminate* it. Fan and Stevenson (2018) identified the four stages of SCRM as "risk identification, assessment, treatment, and monitoring" (p. 20). For an organization, SCRM not only involves thinking about "the probability of something unwanted happening," but also "the potential consequences if it did" (McChrystal & Butrico, 2021).

Why it is essential to think about risk correctly

Thanks to information technology, organizations are better equipped than ever to assess risk, calculate probabilities, and quantify threats (Eckhart et al., 2019). What has not changed, however, is the importance of *how* one approaches, and contemplates, risk.

The client's supply chain situation

In this case, the government client had some additional supply chain challenges. For example, there were multiple subordinate elements reporting their own risks, but without working from a shared concept of risk or how to consistently characterize it. Some of those organizational elements had very few available vendors, in part because the government client had stringent production requirements that were more onerous than those of most commercial clients. Fortunately, the government client recognized the need for a vigorous, comprehensive approach to conducting SCRM.

How the client approached SCRM

The government client took a systematic, comprehensive approach to SCRM. Among the client's objectives

were aggregation of risks identified by subordinate reporting units, development of risk categories and sub-categories, and development of a quantifiable, comprehensible, and consistent means to identify those risks in greatest need of attention.

The value of an outside perspective

Outsiders can help an organization overcome the dangerous bias of Janis' (1972) *Groupthink*, a bias that occurs among members of a highly cohesive group who fail to adequately consider alternatives because of their desire for unanimity (Janis, 2008). To introduce diversity into their comprehensive SCRM methodology, the government client team brought in an academic team from Mercyhurst University that included one professor who was an experienced Red Teamer and Certified Supply Chain Practitioner, a second professor whose expertise was in risk management, and a student who was highly proficient in open source intelligence (OSINT) and analysis, which involved mastery of the tools and techniques necessary for obtaining and analyzing publicly-available information. The focus of this article is on the contributions this academic team made to Phase I of the government client's SCRM efforts.

Review of the literature

The impact of globalization on supply chains

Multiple authors researching supply chain management (Abdel-Malek et al., 2005; Tsay et al., 2019) have noted how, to maximize profitability, companies identify and retain those activities they consider to be core competencies, while outsourcing those activities that can be done more cheaply and efficiently by external suppliers. Due to globalization, firms often seek to lower their costs by contracting with overseas providers to obtain raw materials and components (Glushkova et al., 2019). Shih (2020) observed how the proliferation of tiers and organizations in an enterprise supply chain have made it increasingly difficult for an enterprise to have adequate visibility into their supply chain.

The increased risk of supply chain disruption

Several authors (Dolgui & Ivanov, 2021; Gurtu & Johny, 2021) have observed how a supply chain disruption can then combine with other factors to produce a *ripple effect* that cascades and negatively impacts the performance of the entire supply chain. For example, DuHadway et al. (2018) examined how the Ford Motor Company was forced to suspend production of its F-150 pick-up trucks due to a fire at a supplier facility; suspending production meant temporarily laying off 7,000 workers and delaying production. Andersson and Pardillo-Baez (2020) examined whether the management philosophy

Lean Six Sigma (L6S) improves management awareness and the management of supply chain risk. L6S is an amalgam of two distinct approaches; Lean addresses process flow and waste, while Six Sigma addresses variation and design (Andersson and Pardillo-Baez, 2020). Using a case study methodology, interviewing personnel involved in L6S from various companies, Andersson and Pardillo-Baez (2020) found that Lean decreased variation while increasing risk, whereas 6S decreased and controlled both variation and risk. Andersson and Pardillo-Baez (2020) concluded that L6S values, methods, and tools can be quite effective in companies' efforts to control and manage risks, in some cases resulting in documented, substantial savings.

Supply chain resilience was also of interest to Kwak et al. (2018), who described it as the adaptive capability to prepare for, respond to, and recover from unexpected events with connectedness and control. They described resilience as a capability that is achieved by redundancy, flexibility, agility, responsiveness,

visibility, and collaboration. They surveyed personnel working for various South Korean manufacturers and logistics firms, then analyzed the resultant data using confirmatory factor analysis and structural equation modeling to validate their hypothesis, that the level of SC (supply chain) innovation has a positive impact on robustness capability.

Supply chain *resilience* was also of interest to Baryannis et al. (2019), who asserted that, "Resilience puts more emphasis on the proactive ability to adapt in preparation for unexpected events so that it is possible to quickly recover from them and reinstate continuity of operations in the supply chain" (p. 2184). Baryannis et al. (2019) studied whether SCRM was "a suitable application area for Artificial Intelligence (AI) techniques" (p. 2179), seeking to understand the extent to which AI could assist with SCRM. Based on their review of the existing literature on AI and SCRM, they concluded that, "While the so-called Big Data and associated analysis techniques have made a considerable impact in various research fields and applications, this has not yet been made evident in the field of supply chain research, despite the potentially transformative capabilities of data science" (Baryannis et al., 2019, p. 2191).

Additional supply chain concerns for government organizations

In their review of risk literature, Gurtu & Johny (2021) found that for commercial firms, "the events causing disruption were presumed to be unintentional" (p. 3). In addition to the unintentional risks facing commercial firms, a U.S. government entity must also consider the possibility that nefarious actors might seek to *intentionally* disrupt its supply chain (Osunji, 2021). To mitigate that threat, the U.S. government has companies undergo a laborious clearing process, as a result of which the government can end up with too few specialized, cleared vendors providing critical components for such items as weapons, aircraft, or spacecraft (DoD, 2022). The danger of relying on too few specialized vendors was examined by Porter (2008), who described how in the airline industry "plane and engine manufacturers, along with unionized labor forces, bargain away the lion's share of airlines' profits" (Porter, 2008, p. 24).

Supply chain risk management

"Risk management refers to strategies, methods, and supporting tools to identify and control risk to an acceptable level" (Alhawari et al., 2012, p. 51). Commercial firms and government organizations alike increasingly attempt to avoid supply chain disruption through *supply chain risk management* (SCRM), which applies the principles and approaches of risk management to supply chains and is "a systematic and phased approach for recognizing, evaluating, ranking, mitigating, and monitoring potential disruptions in supply chains" (Gurtu & Johny, 2021, p. 1). Gurtu and Johny (2021) performed a detailed literature review of international journal articles published between 2010 and 2019 that were focused on supply chain risk. Based on their study, one of their findings was that SCRM can be divided into two broad categories of approaches. The first is the strategy for comprehensive risk management, and the second is a focused approach to a specific disruption. Their review of the SCRM literature also led to determine that there were seven identified categories for controlling supply chain risk: (1) prevention, (2) rescheduling, (3) conjecture, (4) numerical and economic, (5) vertical integration, (6) risk-sharing, and (7) technology and security. Fan and Stevenson (2018) conducted a literature review on SCRM, reviewing articles published between 2010 and 2016 to identify SCRM terms and concepts and evaluate the role played by theory in SCRM. They found that while research emphasized organizational responses to supply chain risks, the use of theory in addressing SCRM was limited, and that most of the papers examining risk mitigation focused on a single stage of SCRM. Fan and Stevenson (2018) found that while companies use a wide variety of approaches to identify risk, such as the analytical hierarchy process, value-process engineering methodology, the Ishikawa diagram, and value stream mapping, very limited attention was paid to risk monitoring.

A paradigm shift in approaching supply chain management

Given the expansion of modern supply chains and the potential downstream impacts of a disruption anywhere in a supply chain, enterprises must now modify the way they conceptualize, communicate about, and manage supply chain risk. Using Kuhn's (1962) famous description of a *paradigm* as being the theories, standards, methodologies, and beliefs employed within a particular field, Carter et al. (2008) even argued that changes to supply chains had reached a point where a *paradigm shift* in the field of supply chain management had become necessary.

Consistent with this notion, Huang (2020) advocated for what he called a *holistic* approach to supply chain risk management. Two components of this approach would require an enterprise to "rethink and define an effective supply chain risk management approach" and also establish "a dedicated supply chain risk management organization with interfaces to all relevant business functions" (Huang, 2020, p. 1). What Huang (2020) advocated was precisely what the Team advocated to their client: Not only would it be important for the client to rethink their supply chain and the threats to it, but all business functions would need to have a shared understand of supply chain risk and a standardized, common, and comprehensible language for reporting on potential, emerging, or actual risks.

Effectively managing supply chain risk requires the risk management team to not only identify and have an accurate understanding of individual risks, but also of the way some risks can interact with *other* risks. For example, McChrystal & Butrico (2021) pointed to *Operation Eagle Claw*, the 1980 failed attempt to rescue American citizens held hostage in Iran, as a historical example where the inability to correctly conceptualize risk resulted in disaster. In the planning for *Eagle Claw*, the probability of each of 10 sequential steps succeeding was assessed to be 90%. However, as McChrystal and Butrico (2021) explained, "[E]ven if the realistic probability of the force's completing each step was 90 percent (or .9) , the overall probability Eagle Claw would succeed was not 90 percent. In actuality it was: .9 × .9 × .9 × .9 × .9 × .9 × .9 × .9 × .9 × .9 = .348" (p. 29). In other words, the planners assessing risks to *Operation Eagle Claw* determined the likelihood of success was 90%, when in reality the likelihood of success (which depended on successfully overcoming each of the 10 identified risks) was actually 34.8%.

McChrystal and Butrico (2021) also noted that correctly perceiving risks involves suppressing the biases that cause ignorance or discounting of many risks and cautioned that not addressing a problem from multiple perspectives may lead to overlooking critical factors. In this context, *diversity* means bringing in outsiders who can offer not only subject matter expertise, but also a fresh perspective and fewer of the biases maintained by members of the organization itself.

Methodology

An outside perspective

Consistent with the recommendations of McChrystal and Butrico (2021) and others, the client solicited academics to provide an outsider's perspective on their efforts to improve their SCRM practices. Believing that outside academics could help mitigate Groupthink and other analytic biases within their own organization, a commercial contractor selected the Mercyhurst University team (hereafter: the "Team") to support the government client due to the team's experience with risk management, supply chain decomposition and analysis, and open-source intelligence capabilities (OSINT). The government client faced multiple SCRM challenges that the Team sought to address. Structurally, the government client included an oversight body responsible for SCRM and a multitude of individual, geographically dispersed reporting sites. The oversight body provided the contractor and the Team a limited subset of identified

individual risks provided by some of their reporting sites and tasked them to create, quantify, and test a comprehensive and standardized risk reporting framework. The purpose of this initial step was to ensure the government client not only had a complete operating picture but could quickly and accurately determine which risks were the greatest across their entire enterprise.

Non-standardized risk identification and reporting

The first challenge the Team found was that there was no standardization as to how the government client's individual reporting sites assessed and reported their own supply chain risks. The client owned a significant number of risks, but since the client's individual reporting sites used different methodologies to identify and assess their supply chain risks, those identified risks were not consistently expressed and, when aggregated, did not lend themselves to comprehensive analysis. Although each individual reporting site was able to tailor a SCRM framework specific to their own needs, risks reported above their organizational level were of limited value due to the lack of standardization vertically across sites. Without the ability to assess risks vertically, the client was unable to comprehensively compare risks, analyze these risks, identify common factors creating risk, or establish effective mitigation policies.

A four-step approach

Given that the government client lacked a standardized system for identifying, reporting, examining, and analyzing risks, the Team took a four-step approach to improving their SCRM system. First, the Team examined all relevant government and private sector risk management documents to craft an optimal SCRM approach for the client. Rather than "re-invent the wheel", the Team felt it would be better to examine how *other* government and private sector organizations were addressing SCRM. Second, the Team sought to improve the quality and utility of risk data collection by developing a standardized, comprehensive risk matrix, usable by all reporting sites, that could clearly and consistently identify supply chain risks throughout the enterprise. Third, the Team created a standardized methodology for quantifying all identified risks. Effective quantification would enable the government client to not only identify those risks requiring immediate attention, but also identify whether there might be common contributing factors contributing to those risks which could then be addressed. Fourth, the Team sought to establish effective techniques for aggregating and visualizing the identified risks to provide actionable insights.

Assessing the SCRM Approach Using Open-Source Information

The first step the Team took to resolving the government client's challenges was to gather and assess existing literature on government and private sector SCRM practices. Some of the benefits of examining existing literature are the identification of effective benchmarks, analysis of common approaches, and consideration of how other organizations approached SCRM and framed their SCRM discussions. *Benchmarking* is a competitive intelligence technique for examining how a peer competitor performs a function. The Team utilized the benchmarking technique to assess how SCRM was performed by similar organizations. While the client's supply chain risks are significant, they are hardly unique. Research into SCRM approaches enlightened the Team to common SCRM challenges and mitigation opportunities. Additionally, open-source information assisted in the framing of SCRM discussions between stakeholders. The Team's approach to evaluating publicly available SCRM documents was to identify scope, scalability, and lessons learned. One of the government client's most significant challenges was determining the scope necessary to achieve their objectives. After the client provided the Team with limited, raw supply chain risk data, the Team sought to effectively bound the risk use cases. Knowing that the client was looking to vertically compare standardized risks across reporting sites, the Team identified three macro "lenses" with which to view supply chain risk, which were *supplier focused* risk management, *product focused* risk

management, and *risk focused* management. Supplier focused risk refers to the risks from suppliers. This method often assesses suppliers in tiers.

Supply chain decomposition and mapping are techniques used to visualize those supply chain tiers. Given the threats to their supply chain by both state (China, Russia, and Iran) and non-state (criminal groups, terrorists, malicious individuals) actors, government clients in the defense acquisition space commonly employ these techniques (Epic Global, 2020). The scope of product focused risk management is the product. This method often assesses the decomposition of a product by supplier and location. For example, the Cybersecurity and Infrastructure Security Agency (CISA) regularly assesses the product decomposition of 5G telecom infrastructure to ensure products and components from perceived threat actors (such as China's Huawei) do not find their way into the supply chain (GAO, 2020).

The scope of risk focused management views risks individually, quantifies these risks, and then aggregates them to provide the client with actionable insight. This method assesses the risks at the smallest level of granularity, then quantifies these risks at this level, aggregates them into categories, subcategories, and any other method applicable to the client's needs (Loredo et al., 2015). For example, assume a risk of *transportation blockades* in a dataset is the lowest level of granularity. The risk of *transportation blockades* could aggregate with other risks and belong to the subcategory of *terrorism/sabotage* within the higher-level category of *environmental risks*. Because the scope of risk focused management aligned with the client's objectives, the risk focused management scope was chosen. While the raw data provided to the Team was useful to filter through possible frameworks to determine scope, scalability was another challenge. The Team was provided limited risk data to use for creating the SCRM framework. The Team needed to create a framework that not only worked with the limited risk data but could also scale to an exponential number of risks as the number of reporting sites (and risk data) increase. Because of the Team only had access to limited data, assessing all available sources was essential to understanding the requirements to scale supply chain risk management to a large organization.

From the research, the team found he most effective means to scale was by aggregation of the risks (Moore et al., 2015). Another essential element in the research was assessing risk management lessons learned, both within the government client organization and externally. The Team used lessons learned from all available sources to by filtering the components of the lessons learned into the government client's SCRM framework to determine the effectiveness of the framework's elements. The components the Team used for the lessons learned included trigger events, threats, categories, and strategies. An event triggers a threat, which requires a strategy in response. For example, the event of Covid-19 triggered such threats as supply disturbances, limited suppliers/products, and other threats which required strategies in response. The Team used these events and threats to test the categories tailored to the client. Additionally, these strategies were identified as potential risk mitigation techniques. From evaluating all available sources, the Team was able to create a precise scope for the clients SCRM framework, ensure this framework was scalable, and then implement/test the framework using external lessons learned.

Identifying Risks

The client did not task the Team with risk identification; instead, this was left to the reporting sites. While the Team was not responsible for risk identification, it presented the government client with risk identification methodologies to ensure the highest number of risks could be identified. In order to ensure that all potential risks were identified, the Team encouraged the client to ensure all stakeholders participated in risk identification. Because each reporting site practiced differing approaches to SCRM, the team's focus within the identification step was to ensure the standardization of data collection. The standardization of data collection and risk identification steps included standardizing the SCRM terms, data validation, and

surveying the reporting sites. The Team created standard SCRM definitions for all the reporting sites to ensure standardization of the data collected. Also, the team used data validation techniques to enforce standardization for the data collection. For example, an Excel sheet was utilized to collect the risk's the reporting sites identified. The Excel sheet drove the reporting sites to input data in a specific, standardized manner. Additionally, the Team used a survey to encourage stakeholder participation and input into the categories, subcategories, aggregations, and processes. The Team used a risk register to store the identified risks and data collected from the reporting sites. While there are many tools to use as a risk register, the Team used an Excel spreadsheet due to its relative simplicity. Along with storing the identified risks, the Team used the Excel based risk register to conduct calculations, automate the visualization of data, conduct root cause analysis, and explore mitigation tactics for similar risks.

Quantifying Risks

Quantifying risk involves standardization, comparison, and aggregation. The client needed a standard approach to quantification to enable risk comparison across reporting sites and aggregation to further understand and analyze the data. The consideration the Team addressed in the quantification steps included choosing the best fitting model to address the client's challenges, accuracy of the risks, and risk threshold. The model used for the quantification of risks depends on the needs of the client. For instance, other organizations might consider variables such as vulnerabilities, exposure, and detection (Faizal & Palaniappan, 2014). Additionally, the range is dependent on the use case. Some organizations with precise metrics to calculate the risk quantification variables (likelihood, consequence, cost, etc.) use a large risk score range such as 1-100. Because the client oversees a multitude of reporting sites and the metrics used in their risk quantification variables are broad, the Team determined a range of 1-25 would be adequate. The model that the Team determined would best fit the client needs was the DOE/DoD quantification method (DoD, 2017). This method states the risk score (the total risk in a numeric form) is equal to the likelihood of a threat occurring, multiplied by the consequence of the threat. The consequence is equal to the cost of the threat plus the schedule impact, divided by two. The risk level is the risk score ranked as: very low, low, moderate, high, and very high. A popular method to visualize the quantification is a risk matrix. The function for calculating the risk score for each individual risk is shown below. The definitions of the variables are shown in Table 1.

Table 1: Definitions of the variables. Author generated.

Risk Score	Convergence of the likelihood and consequence scores
Risk Level	Risk score expressed and ranked from *very low* to *very high*
Likelihood	Probability of an event occurring
Consequence	Consequence is the outcome of an event
Cost	The risk impact to budget
Schedule	The risk impact to project schedule

The accuracy of the risks is dependent on the metrics used to determine the risk variables. One of the challenges the client expressed was the difficulty in creating a standard SCRM framework across multiple reporting sites due to the site differences in size, budget, and capabilities. For instance, if a risk variable cost has a metric stating a very low-level cost is 0 – 50,000 USD for a risk, then all sites owing a risk cost of 0 – 50,000 USD must report this cost as very low. But this is potentially an inaccurate depiction of the risk variable cost for all sites. For one site 0 – 50,000 USD could equate to a very low level while 0 – 50,000 USD of another site's budget could equate to a moderate level. To correct this, the Team based the metrics determining the risk variables on a *percent* instead of a *fixed* number. This enabled the client accurate risk

scores relative to factors such as size, budget, capabilities. The last quantification consideration the Team assessed for the government client was the risk threshold, which is the appetite an organization has for risk. Risk surpassing the threshold is outside the tolerance of the organization. The Team determined that a risk threshold would not benefit the client due to the differing capabilities of the reporting sites, otherwise, risk thresholds are highly recommended (DoD, 2017).

Aggregating and Visualizing Risks

The Team used a Risk Breakdown Structure (RBS) to organize the individual risks, sub-categories, and categories. The alternative aggregating/grouping methods are not included in the RBS. The Team utilized categories proposed by the client based off DoD recommendation but created the subcategories specific to the organization. The benefits of aggregating/grouping the risks are each aggregation/grouping of the risks provides a differing view of the data and creates actionable insights for the client.

The Team grouped and aggregated the risks by a multitude of methods. Reference Annex 6 and 7 for aggregation methods and visualization of risks. The first set of aggregation and visual methods utilized for the client are by category, subcategory, and lifecycle. The categories chosen were recommended by the client and are categories used by the DoD in risk assessments (DoD, 2017). The categories allow the client to determine a broad view of the most threating risks exists across all participating sites. The subcategories were tailored to the needs of the client. By subcategories, the client can determine umbrella strategies to mitigate threats across sites.

The supply chain life-cycle categories are based on the SCOR methodology (APICs, 2017). By supply chain lifecycle, the client can use this to determine the product stage with the most threatening risks across sites. Additionally, this could assist the client in determining a timeframe to introduce strategies. The second set of aggregation and visual methods utilized for the client are by handling strategy, a site stop light chart, and by a site bar graph. The risk management handling strategies are common practice across the industry (Cagno et al., 2007). By handling strategy, the client can determine the mitigation strategies effectiveness across reporting sites. The stoplight chart that offers the client a quick snapshot into the average or greatest risks from each site by category. The site aggregation offers the client a snapshot of the sites risk performance in comparison to other sites. The third set of methods utilized for the client are visual methods and not aggregations and include risks as individuals and a procurement strategy graph. The risks as individuals allow for an individual threat comparison across sites. The procurement strategies map out the client's risks into broad strategies to address those threats. While the Team placed the axes at 2.5 for likelihood and consequence, this can be adjusted based on the client's needs.

Other Methods to Visualize Risk

The following sets of aggregations and visuals were not used for the Team's client but depending on the use case can offer actionable insights. The first set of aggregations are adversarial and non-adversarial. An adversarial threat refers to a threat associated with malicious intent, while a non-adversarial heart is all other conditions. This grouping reveals the source of the attack that is most threatening, impactful, and likely to the client. The second set are differing visual methods of aggregation previously mentioned including a box and whiskey chart, radar chart, and bar chart with a threshold. The analyst can use all these visual methods aggregating by category or site. The box and whisker chart offers the minimum, lower quartile, median, upper quartile, and maximum of the risk scores per category or site. The radar chart demonstrates the average risk score per category, average site risk score, and the risk threshold. This chart allows the client to determine where the most threating and the majority of risks exists with a single site, easily compare to the average, and compare to the threshold. The bar chart demonstrates the average risk score per category,

average site risk score, and the risk threshold. This chart allows the client to determine where the most threating and the most risks exists with a single site, easily compare to the average, and compare to the threshold. The last set of aggregations and visual representations of risk are the geospatial map and bubble chart. The geospatial map demonstrates risk per country. This can assist the client in comparing risk across countries if applicable. This bubble chart demonstrates risk as individuals, risk score, and category. Each bubble represents an individual risk, the size of the bubble represents the risk score, and the color of the bubble represents the category the risk belongs to. This can assist the client in visualizing large sets of data.

Results

The Team's SCRM methods and fresh perspective introduced in this essay enabled the client to conduct a standard, accurate, and effective SCRM process across all reporting sites. With this process, the government client now has the capability to capture data, aggregate it, analyze it, and visualize risk to empower more effective decision-making about risk responses. For instance, after the Team's efforts, the client was able to gain three significant insights. First, there was one reporting site that had a significantly higher overall SC risk than the other sites. This had previously gone unnoticed due to the incomparability of the risks and lack of standardization. Second, the client noticed they had a dependency on high-risk suppliers. While the client had suspected this might be the case, the inability to effectively visualize the risks across reporting sites had prevented them from confirming this. Third, the client noticed trends within the risks recorded in the register across reporting sites. By recording and understanding these trends, the client was able to identify effective mitigation policies across reporting sites.

Discussion

Consider an outside perspective

Both the government client and the contractor expressed appreciation to the Team for their contributions to the client's SCRM methodology. This experience validated to all three groups the wisdom of McChrystal and Butrico's (2021) recommendation regarding the value of outside perspectives.

Leverage existing literature

Another takeaway from this effort was the value of examining available, existing literature concerning supply chain risk management. Examining how government and private sector organizations approached SCRM enabled the Team to quickly identify and recommend appropriate best practices. Where necessary, the Team created components for the process (such as risk sub-categories); however, the Team saved considerable time by first familiarizing itself with existing best practices. An efficient and effective way to approach SCRM is through a combination of tried-and-true "best practices" and tailored techniques that capture the way a particular enterprise operates.

Avoid a "One Size Fits All" approach to SCRM

While SCRM has become relatively standardized on the macro level, a "one size fits all" approach is inadvisable. For example, the Team adopted risk categories identified in the literature, but tailored risk sub-categories to align with the risks identified by the government client's reporting elements.

Effective communication is indispensable

Communication is more than just conversation. As McChrystal and Butrico (2022) asserted, there are four key "tests" to determine whether communication is effective: (1) There must be the *ability* to pass information; (2) there must be a *willingness* to pass information; (3) the message passed must be of *good quality*; and (4) the meaning of the message must be *clear* to its recipient. Within an enterprise, one of the most critical aspects of SCRM is effective communication. During this project, there was frequent and clear communication between the government client, the contractor, and the Team. Communication between the reporting sites and the government client's team responsible for SCRM improved after the government adopted the standardized risk matrix and quantification methodology proposed by the Team. Having a "common operating picture" throughout the enterprise enables an organization to comprehensively and accurately identify, and then address, risk.

SCRM is an ongoing process

A recommendation is that SCRM is not a "once-and-done" effort; rather, it is an ongoing process. The world changes, and as a result we must periodically check our assumptions to ensure the risks we assessed in the past have not been affected by such unforeseen events like Covid-19 or a container ship getting stuck in the Suez Canal for several weeks. "The most dangerous assumptions are those we make unconsciously, particularly when our biases influence our judgment. The most common is for individuals, and even sophisticated organizations, to assume that things will continue in a certain way, or in an established direction, because that's what our experience has been thus far. It's helpful to remember that things stay the way they are – until they don't" (McChrystal & Butrico, 2022, p. 248).

Periodically pressure test the system

While this admittedly lies beyond the scope of this article, it is important to emphasize the importance of pressure testing the system by imagining what one would do in the event certain risks actually materialized. Having an effective process for identifying, quantifying, and analyzing risk is only the first part of SCRM; the second, and equally vital part, is considering steps that could be taken (avoid, accept, mitigate, or transfer) in response to those risks – *before* they actually materialize.

References

Alhawari, S., Karadsheh, L., Talet, A. N., & Mansour, E. (2012). Knowledge-based risk management framework for information technology project. *International Journal of Information Management, 32*(1), 50-65.

Alicke, K., Benavides, L., & Sankur, A. (2017, November 9). Three game-changing supply-chain technologies. Retrieved July 1, 2022, from https://www.mckinsey.com/business-functions/operations/our-insights/three-game-changing-supply-chain-technologies.

Andersson, R., & Pardillo-Baez, Y. (2020). The Six Sigma framework improves the awareness and management of supply-chain risk. *The TQM Journal, 32*(5), 1021-1037. doi:10.1108/tqm-04-2019-0120

Baryannis, G., Validi, S., Dani, S., & Antoniou, G. (2019). Supply chain risk management and artificial intelligence: state of the art and future research directions. *International Journal of Production Research, 57*(7), 2179-2202.

Bonvillian, W. B. (2017). US manufacturing decline and the rise of new production innovation paradigms. Retrieved from https://www.oecd.org/unitedstates/us-manufacturing-decline-and-the-rise-of-new-production-innovation-paradigms.htm

Cagno, E., Caron, F., & Mancini, M. (2007). A Multi-Dimensional Analysis of Major Risks in Complex Projects. *Risk Management, 9*(1), 1–18. http://www.jstor.org/stable/4143841

Carter, C. R., Sanders, N. R., & Dong, Y. (2008). Paradigms, revolutions, and tipping points: The need for using multiple methodologies within the field of supply chain management. *Journal of Operations Management, 26*(6), 693-696.

Department of Defense Risk, Issue, and Opportunity Management Guide for Defense Acquisition Programs. (2017, January). Retrieved from https://acqnotes.com/wp-content/uploads/2017/07/DoD-Risk-Issue-and-Opportunity-Management-Guide-Jan-2017.pdf

Dolgui, A., & Ivanov, D. (2021). Ripple effect and supply chain disruption management: new trends and research directions. *International Journal of Production Research, 59*(1), 102-109. doi:10.1080/00207543.2021.1840148

DuHadway, S., Carnovale, S., & Kannan, V. R. (2018). Organizational communication and individual behavior: Implications for supply chain risk management. *Journal of Supply Chain Management, 54*(4), 3-19.

DuHadway, S., Carnovale, S., & Hazen, B. (2017). Understanding risk management for intentional supply chain disruptions: risk detection, risk mitigation, and risk recovery. *Annals of Operations Research, 283*(1-2), 179-198. doi:10.1007/s10479-017-2452-0

Eckhart, M., Brenner, B., Ekelhart, A., & Weippl, E. (2019). Quantitative Security Risk Assessment for *Industrial Control Systems: Research Opportunities and Challenges, 9.* 52-73. 10.22667/JISIS.2019.08.31.052.

EPIC Global Supply Chain Risk Assessment. (2020, March). IHS Markit. Retrieved from https://haslam.utk.edu/wp-content/uploads/2021/08/EPIC-Global-Supply-Chain-Risk-Assessment-2020.pdf

Fan, Y., & Stevenson, M. (2018). A review of supply chain risk management: definition, theory, and research agenda. *International Journal of Physical Distribution & Logistics Management, 48*(3), 205-230. doi:10.1108/ijpdlm-01-2017-0043

Faizal. K, and Palaniappan, D. P. L. K. (2014). Risk Assessment and Management in Supply Chain. Retrieved from https://globaljournals.org/GJRE_Volume14/3-Risk-Assessment-and-Management.pdf

Federal Agencies Need to Take Urgent Action to Manage Supply Chain Risks. (2020, December). Government Accounting Office. Retrieved from https://www.gao.gov/assets/gao-21-171.pdf

Gelderman, C. & Donald, D. (2008). Application of Kraljic's purchasing portfolio matrix in an undeveloped logistics infrastructure: The Staatsolie Suriname case. *Journal of Transnational Management, 13*. 77-92. 10.1080/15475770802059610.

Glushkova, S., Lomakina, O., & Sakulyeva, T. (2019). The economy of developing countries in the context of globalization: Global supply chain management. *International Journal of Supply Chain Management 8*(1), 876-884.

Gurtu, A., & Johny, J. (2021). Supply Chain Risk Management: Literature Review. *Risks, 9*(1). doi:10.3390/risks9010016

Helper, S., & Sako, M. (2010). Management innovation in supply chain: appreciating Chandler in the twenty-first century. *Industrial and Corporate Change, 19*(2), 399-429. doi:10.1093/icc/dtq012

Huang, J. (2020). How to drive holistic end-to-end supply chain risk management. *Journal of Supply Chain Management, Logistics and Procurement, 2*(4), 294-306.

Janis, I. (1972) *Victims of Groupthink*. Boston: Houghton Mifflin.

Janis, I. (1991). Groupthink. In E. Griffin (Ed.) *A First Look at Communication Theory*, p. 235 - 246. New York: McGrawHill.

Kuhn, T. S. (1962). *The Structure of Scientific Revolutions*. University of Chicago Press.

Kwak, D. W., Seo, Y. J., & Mason, R. (2018). Investigating the relationship between supply chain innovation, risk management capabilities and competitive advantage in global supply chains. *International Journal of Operations & Production Management, 38*(1), 2-21. doi:10.1108/ijopm-06-2015-0390.

Labonte, M., & Weinstock, L. R. (2022, May 13). Supply disruptions and the U.S. economy. Retrieved from https://crsreports.congress.gov/product/pdf/IN/IN11926

Abdel-Malek, L., Kullpattaranirun, T., and Nanthavanij, S. (2005). A framework for comparing outsourcing strategies in multi-layered supply chains. *International Journal of Production Economics, 97*(3), 318-328. ISSN 0925-5273, https://doi.org/10.1016/j.ijpe.2004.09.001.

Loredo, E. N., Raffensperger, J. F., & Moore, N. Y. (2015). Measuring and managing Army supply chain risk. RAND. Retrieved from https://www.rand.org/content/dam/rand/pubs/research_reports/RR900/RR902/RAND_RR902.pdf.

McChrystal, S., and Butrico, A. (2021). *Risk: A User's Guide*. Penguin.

Mondschein, J., Welburn, J. W., & Gonzales, D. (2022). Securing the microelectronics supply chain - Four policy issues for the US Department of Defense to consider. Retrieved from Santa Monica, CA: RAND Corporation

Moore, N. Y., Loredo, E. N., Cox, A. G., & Grammich, C. A. (2015). Identifying and managing acquisition and sustainment supply chain risks. Retrieved from RAND Corporation, https://www.rand.org/pubs/research_reports/RR549.html.

Winn, M., Pinkse, J., & Illge, L. (2012). Case studies on trade-offs in corporate sustainability, corporate social responsibility and environmental management, 19(2), 63-68.

Ney, V. A. (2021). *Energy sector cybersecurity supply chain risk management*. Utica College, New York

Osunji, O. (2021). Know your suppliers: A review of ICT supply chain risk management efforts by the US government and its agencies. *Cyber Security: A Peer-Reviewed Journal*, *4*(3), 232-242.

Porter, M.E. (2008). The five competitive forces that shape strategy. *Harvard Business Review*, p. 24-41.

Pournader, M., Kach, A., & Talluri, S. S. (2020). A Review of the Existing and Emerging Topics in the Supply Chain Risk Management Literature. *Decision Science, 51*(4), 867-920. doi:10.1111/deci.12470

Securing Defense-Critical Supply Chains. (2022, February 24). Retrieved from https://media.defense.gov/2022/Feb/24/2002944158/-1/-1/1/DOD-EO-14017-REPORT-SECURING-DEFENSE-CRITICAL-SUPPLY-CHAINS.PDF

Shih, W. (2020). Is it time to rethink globalized supply chains? *MIT Sloan Management Review, 61*(4), 1-3.

Tsay, A. A., Gray, J. V., Noh, I. J., & Mahoney, J. T. (2018). A review of production and operations management research on outsourcing in supply chains: *Implications for the theory of the firm. Production and Operations Management, 27*(7), 1177-1220.