Vulnerability as a Relevant Supply Chain Attribute for SCOR

Olufemi Adetunji
Department of Industrial and Systems Engineering
University of Pretoria
Pretoria 0002, South Africa

Abstract

Given the scale and frequency of risk faced by supply chains today, a case is made for the inclusion of vulnerability as a distinct attribute when using SCOR to model supply chains. Argument is made that agility metrics may not capture the risks involved in supply chain at the desired level. Also, using the ideas of operational buffering, it is shown that the classification of VaR as a strategic metric of agility is not perfectly fitting. It is suggested that VaR should possibly be one of the strategic metrics of vulnerability. Some other metrics that could jointly measure the vulnerability of a supply chain were then proposed. An argument is made that this will make SCOR more easily applicable to modelling a wider range of supply chains, which is typical of today's business environment.

Keywords
Reference modelling, SCOR, Agility, Vulnerability, Supply Chain Risk, Value at Risk.

1. Introduction
One of the most fundamental shifts in the paradigm of business management today is that firms no longer compete as individual entities, but as parts of an extensive supply chain that spans large geographical expanse and industries (Lambert, 2006). This has led to the development of globally challenging and operationally complex chains, consisting of diverse industries and specialists, operating across many national boundaries and diverse socio-cultural partnerships. Speaking the same language and sharing common strategic goals and performance measures across such complementing partners in a supply chain would have been nearly impossible without the evolution of supply chain reference models.
The Supply Chain Operations Reference (SCOR) model is one such process reference model. The SCOR model (simply called SCOR) is a product of the Supply Chain Council (SCC) and has become about the most accepted supply chain reference model today. This is evidenced from the growth of the council membership from a consortium of 69 members in 1996 to more than a thousand corporate members as at 2010 (SCC, 2011). SCOR is an elegant and painstakingly detailed model that clearly ties the supply chain competitive strategy to the supply chain attributes. These attributes are then tied to the strategic (or level 1) metrics. The strategic metrics are linked to the diagnostic (levels 2 and 3) metrics. The metrics are linked to the organisational processes. The processes are linked to the industry best practices, and the best practices serve as mechanisms for continuous and breakthrough improvements of the supply chain processes.
While SCOR is good and very applicable as it is, the Supply Chain Council has acknowledged the need to continually review and improve the model in order to make it more relevant to the industry and to improve on the goals of its design. As at the time of writing this paper, version 10 is the latest, and version 11 is a work in progress. The changes relevant to this paper are discussed in section 2.2
The main contribution of this paper is towards the definition of the structure of the SCOR reference model for more generalisablility. The argument is that there appears to be a salient unidentified dimension of supply chain attributes in SCOR, for which the name vulnerability seems most appropriate based on the popularity of the term in the body of work that also seeks to address supply chain risks. Vulnerability seems pervasive in all supply chains, but also seems not to have received enough strategic attention in SCOR classification. Proposal is made for a structure of the strategic (level 1) metrics of vulnerability and how it would enhance the modelling of some supply chains that could prove challenging when using SCOR as it currently is highlighted.
The remaining section of the paper is structured as follows: firstly, an overview of reference models in general and a discussion of supply chain reference models was made in some more details; next is a review of SCOR's supply chain attributes and their strategic metrics in more detail as a background to the focus on supply chain agility, one of SCOR's attributes; next is an analysis of agility and its metrics and, based on operational management principles of buffering, it was shown that it appears to address issues that are fundamentally different from vulnerability; and that

Value at Risk (VaR) which is currently one of its strategic metrics, seems more like a metric of vulnerability, together with some other possible metrics to be discussed later; next, an argument is presented for vulnerability as a distinct supply chain attribute and the possibility of it encompassing the GreenSCOR in its strategic dimension; a possible framework for decomposing vulnerability to some key areas that could each be captured by a strategic metric, which together will measure the vulnerability attribute of a supply chain was then proposed; finally, the likely benefit of the proposed re-classification in a possibly more pervasive and user-friendly application of SCOR in some identified supply chains was shown.

2. Reference Models in Practice

The use of reference models seems synonymous to the analysis and synthesis of information systems. One of the classic efforts in this area is the Open System Interconnections (OSI) that forms the basis for the revolution in internet connectivity and computing, where a seven layer model, starting from the application layer to the physical layer. While the OSI effort is revolutionary in the networking environment, the Universal Modelling Language (UML) is also revolutionary in the software environment. UML is produced from the amalgamation of work from three competing factions in the field of object modelling. It has since been one of the most important skills of a system analyst.

Reference models have become pervasive in many industries today. They enable practitioners to easily communicate intentions, collaborate and exchange information with better clarity, and to maintain a good knowledge management system. These reference models are basically related to different industries and have some regulations or standard system managed by a body, usually the International Organisation for Standardisation (ISO). One example is found in the e-learning environment where there is the Sharable Content Object Reference Model (SCORM). It is actually an initiative of the Advanced Distributed Learning (ADL) of the United State's Department of Defence. The management of spatial data is another example area that has received attention for reference modelling. There are the Spatial Reference Model (SRM), the Spatial Reference Object Model (SROM), the Open Geospatial Consortium (OGC) reference model and others. The purpose of these models is to harmonise systems of referencing and storing spatial data and exchanging information amongst the practitioners. There is the Open Archival Information System (OAIS), which is tailored towards the preservation, management and distribution of archival information. While the goal here is not to discuss reference models and their standard definition in too much detail, it is apparent that reference modelling is an important area of information management and exchange and preservation of knowledge today. Many academic and industry based papers are also available on each of these models, but such would not be referenced in this paper. The Supply Chain Management (SCM) field today, given its relevance, popularity and demands, also has a number of reference models that have been proposed and is being utilised in its modelling. The SCOR is one such important reference model in the supply chain industry.

2.1. Supply Chain Reference Models for global competitiveness

The period from the 1990s till now has been described as the supply chain era by authors like Hopp and Spearman (2008), Chase and Jacob (2011) and Langley et al (2009). It is, therefore, not surprising that there has also been a growth in the evolution of reference models for supply chain management. While there are many models that could be used to model supply chain processes, three of the popular models are discussed here. These are the American Productivity and Quality Centre (APQC)'s Process Classification Framework (PCF), the Global Supply Chain Forum (GSCF)'s framework and the Supply Chain Council (SCC)'s SCOR. The main foci of each of these models are discussed, and then the discussion dovetails towards the nature of the SCOR model.

The PCF is part of the efforts being made by America at being globally competitive, regaining the lost ground in manufacturing and maintaining a forte in services. Some notable efforts were made since the deficiency of using the basic scientific management principles were obviated by the challenge mounted by the Japanese companies in the seventies and eighties. Such efforts include the institution of the Malcolm Baldrige National Quality Award, which is similar to the Deming Prize by the Japanese to encourage national productivity and competitiveness. There was also the development and advancement of the SERVQUAL to drive competitiveness in the service industries led by the Zeithaml et al (1990) and others. The European Foundation for Quality Management (EFQM) also launched their quality award and presented their excellence model as a tool to enhance global competitiveness.

The PCF framework was developed by the Productivity and Quality Centre together with some industry partners. This model has since been adopted by many organisations as a quality framework to enhance their competitiveness (Oakland, 2003, Spearman and Hopp 2008).

The GSCF framework is another process focused supply chain model. Its philosophy, as different from SCOR and PCF, is the cultivation of relationships in a supply chain. It also has a process decomposition system of its own,

comprising of eight "super processes" from which other lower level processes were isolated. Lambert ed. (2006) is a very good introductory reading for this model.
While the PCF has been developed to cover almost every activity of an organisation, and so, very broad in terms of its scope, SCOR focuses more on the "super processes" 5, 6 and 7 of the PCF, but at more depth.

2.2. SCOR's attributes and strategic metrics

The SCOR links processes together in a cross-organisational manner, allows for benchmarking against the industry and competitors, helps to perform the necessary gap analysis, and provides remedies to close the identified gaps, usually by drawing from its repertoire of best practices, which is integrated with its processes. This gives it not only a performance measurement or diagnostic capability, but also that of continuous improvement.
SCOR defines five dimensions, called the supply chain attributes, along which every supply chain can be measured. Relative to the firm of interest, three of these attributes (Reliability, Responsiveness and Agility) are outward facing while two (Cost and Asset) are inward facing. Metrics are defined for each of these attributes. The supply chain attributes and metrics as defined in SCOR 10 are presented in Figure 1. The four metrics of agility, like the others, are shown under it.
The performance of the supply chain is measured by the level of achievement of these metrics and the supply chain strategy is reflected in the desired level of achievement of each of these level 1 metrics of SCOR. Three levels of achievement, Superior, Advantage and Parity, are defined for a firm relative to the other industry participants. Performance gaps are defined in two terms: competitive gap is the difference between strategic target and the achievement level of a metric; parity gap is the difference between the median level of achievement in the industry and the level of achievement by the firm under study.

3. Formal SCOR definition of Agility attribute and its strategic metrics

SCOR defines agility as the ability to respond to external influences or market place changes to gain or maintain competitive advantage. In SCOR 9.0, it was measured by three metrics; upside supply chain flexibility, which is the number of days required to achieve and maintain an unplanned 20 percent increase in quantities delivered; upside supply chain adaptability, which is the percentage increase in delivery quantities that can be achieved and sustained within 30 days; and downside supply chain adaptability, which is the reduction in quantities ordered sustainable at 30 days prior to delivery with no inventory or cost penalties. In version 10.0, a fourth metric, supply Chain Value at Risk, was added as a strategic metric for agility, and this was defined as the sum of the product of the probability of risk events and the monetary impact of each of the events for all the supply chain functions. In practical terms, this can be interpreted to mean the expected value of monetary loss that the supply chain is capable of making at a particular point in time.

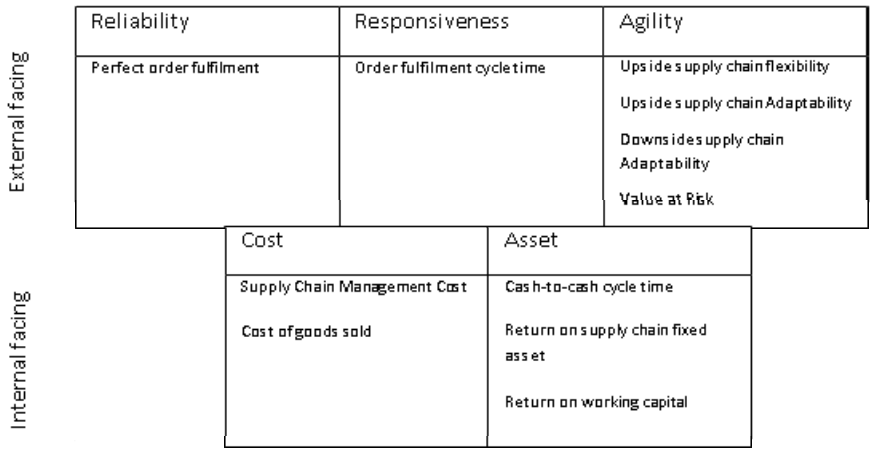

Figure 1: SCOR version 10 attributes and their strategic metrics

The structure and content of SCOR has been modified in the different versions. In the version 9.0, for instance, GreenSCOR and Supply Chain Risk Management (SCRM) functionalities were added as some of the improvements made over version 8.0 (the tenth revision). The expansion of the library of best practices is the main review focus for version 11. The main improvements of version 10 over version 9 are: (1) the definition and linking of supply chain skills to supply chain processes, and (2) re-classification, consolidation, renaming and removal of some old metrics

and creation of some new ones. Of the re-classifications made, the relevant one to this study is the treatment of Supply Chain Risk Management (SCRM) metrics, and that is discussed next.
In version 9, two SCRM metrics, Value at Risk and Mitigation Cost, were defined and placed at the diagnostic level 2, under the Total Supply Chain Management Cost (TSCMC), which is one of the strategic metrics of the supply chain attribute "Cost", an inward facing attribute. This was further reviewed in SCOR version 10 by moving Value at Risk, VaR, from measuring Cost, an inward facing attribute, to measuring Agility, an outward facing attribute. Also, the level of VaR was shifted upwards from a level 2 diagnostic to a level 1 strategic metric, with some level 3 metrics associated with it also redefined as level 2 metrics. But the mitigation costs metric was left as a diagnostic level 2 metric of the Cost attribute (SCC 2006, 2008, 2010).
In the following section, the appropriateness of this reclassification from cost to agility is re-evaluated with a motivation for why the metric could have still been a cost metric. It is pointed out why there could be some ambiguity in the classification except when the accounting treatment of the metrics is clarified. It was argued that the reclassification activities could probably be as a result of an implicit attribute, vulnerability, not yet defined in SCOR. Discussion of some other possible strategic metrics of vulnerability (in addition roVAR) is later done in section 8. It is, however, pertinent at this point to review the concept of system buffer as it helps in analysing the consistency, or otherwise, of VaR as a strategic metric classified under Agility.

4. Definition and implications of system buffers

A production system buffer is any production resource that is available in quantities more than the exact amount needed for the purpose of delivery of goods or services at any particular point in time. Hopp (2008) has noted that this is necessary in any system in which there is some form of either input or process variability. He argued further that variability in production system is further amplified by batching, and the implication is that variability in production or supply chain system will be buffered by some combination of inventory, capacity or time. The same principle was highlighted in Webster (2008) but the term buffer was replaced with system slacks.
A similar discussion was made in Yang and Yang (2010). They noted that handling supply chain risk usually involves creating redundancy or flexibility in the system. Creating redundancy involves over-deploying of some resources, which is akin to buffering. Solutions like having multi-skilled workforce, supplier cooperation and coordination as well as the development of versatile equipments were part of what they classified as building of flexibility. One would like to point out that it may be rather difficult to place some of these solutions entirely in a class. Consider having versatile workforce or machine for instance, most machine flexibility are usually achieved at the expense of high system utilisation. This follows naturally from product versus process alignment. A good discussion on this can be found in Chase et al (2011, pg199).
The presence of buffer implies that the utilisation of the system is lower than its capacity, which gives the system stability against variability and helps in achieving an agile system and high customer satisfaction during cases of demand or supply fluctuations and prevent lost sales. But it also has cost implications in that underutilised capacity implies an unrealised revenue opportunity and high inventory buffer implies high holding cost. These have the potential to erode the bottom line of the company. Time is the last buffer that is not usually apparent because in cases where there is no inventory to immediately meet demand, given enough supply lead time and provided the production rate is more than the usage rate, an unplanned surge in demand can eventually be met.

4.1. Agility metrics as measures of buffers

It can be observed from the definition of upside measures of agility (flexibility and adaptability) that they are related to some buffers in the supply chain. This suggests that there are either existing or accessible buffers in the supply chain that could be used to meet an unplanned surge in demand. In the case of downside adaptability, is also suggests the presence of some form of time buffer that can allow the delay of the commencement of some key processes, without which inventory or cost would have been incurred from the day the order is firmed with the customer. But can Value at Risk (VaR) be considered to be some form of slack in the system? The answer is hardly a yes. It may, however, be pertinent to address why the VaR is being determined to address this question properly. Should the reason be to seek out the best among many alternative processes, then, it is better treated as a vulnerability variable because this is not really related to agility or buffering. Should it be to insure the critical supply chain processes against some failure, then, it depends on the financial treatment of hedging the risk involved. This is discussed in the next section.

4.2. Implications of the manner of hedging of Supply Chain Risks on VaR's classification

Consider two possible approaches to financially hedging the supply chain risk. This is important because it may help to clarify whether VaR should appropriately be a cost or agility metric. There are two main ways the cost could be

treated in practice: provisioning and payments. If a particular risk is covered by insurance, for instance, it is likely that the risk is covered by another party, and that fund is paid out. This is usually in the form of a premium paid to the insuring party that would assume responsibility for that risk in case of eventualities. Such cost is then treated as an expense because the money paid out for insurance is not recoverable in case the undesirable event does not occur. This makes the metric look like a cost metric.

If, on the other hand, a provision is being made continually into an emergency account or fund, then the fund is available in the organisation as some form of slack against days of emergency. This makes the treatment of the metric to appear similar to the other ones in the Agility category which can be seen essentially as slacks in some other forms like capacity, inventory or time. The interesting thing to point out is that the agility strategy can be achieved through a mix of these four assets; inventory, capacity, time or cash, and the four are essentially inter-changeable through a logical view of conversion and conservation of assets.

It is, however, worth pointing out that whichever way the treatment is made, it can still be assumed that some expense in incurred, even if it is indirectly. Consider a provision being made for such risk instead of a premium being paid; the firm is forced to keep the fund in an account that would likely yield much less than another more financially rewarding but riskier option. This is a case of opportunity cost, and it can be seen as lost income. This argument puts VaR more firmly under cost than agility.

If even one bets on the ability of a supply chain member to respond without incurring any tangible cost, then there must be some implicit slacks, within the supply chain. And one reality is that even if the slack is maintained by another supply chain partner for the firm under consideration, the cost would still be transferred back to the entire supply chain somehow because every slack must be paid for. Slacks are, generally, more related to agility, even though they have cost implication. This makes it more difficult to decide whether contingency planning suggests agility or cost.

The idea of Value at Risk, however, seems more compatible with insurance payout than an own provisioning, making one to conclude that it might be better to treat VaR as a cost variable than an agility variable. This is more so because VaR does not make much sense if an organisation is providing for the risk eventuality by setting money apart within their organisational structure because VaR is only a measure of expectation, and the expected value hardly occurs. It makes more sense if it is used in pricing a regular premium payout. This argument would be more apparent once supply chain risk is reviewed and an expanded definition for supply chain vulnerability is provided below. A categorical classification of supply chain risks would then be made and the strategic level metrics for each of broad categories of supply chain risk defined. The financial risk category would naturally swallow up VaR as one possible metric for it. The organisation can then decide to use VaR as its financial risk metric if it is suitable.

The only possible use of VaR that may not involve any cost, therefore, is when one compares many possible scenarios to determine which option has the least monetary implication so as to choose such option, in which case the metric does not appear to fit under agility. It would still seem more like a comparison of two levels of vulnerability. This is apart from the possible difficulty (or even sometimes impossibility) of determining the monetary value of some actual events.

5. Supply Chain Risk: definition and sources

The definition of supply chain risk is as diverse as the context or industry of interest, and in many cases, it is intertwined with its causes and classification. Kaplan and Garrick (1981) defined risk as a triplet of scenario, frequency and consequence of events that may contribute negatively. Hazard was defined as a source of potential damage and risk as hazard divided by safeguard. March and Shapira (1987) defined supply chain risk as a variation in the distribution of possible supply chain outcomes, their likelihoods and their subjective values. Zsidisin (2003) provided his “grounded” definition that supply risk is the probability of an incident associated with an inbound supply from an individual supplier failure or the supply market occurring, in which its outcomes result in the inability of the purchasing firm to meet customer demand or causes threats to customer life and safety. These definitions are in tandem with many mathematical definitions of risk, including the popular value at risk (VaR) used as a measure of financial risk and also adopted in the SCOR model, which computes expected value of risk from the probability and effects of each of the possible outcomes of the risk event.

Many authors have provided sources of supply chain risk. Blackhurst et al (2005) feel it may be the outcome of unexpected variations such as capacity constraints, machine breakdowns, uncertain yields, quality problems, a fire or even natural disasters occurring in a supplier facility. Cucchiella and Gastaldi (2006) noted how various types of risks like accounting, asset impairment, supplier country characteristics, competitive, customer, downside, financial, interaction, legal, product, regulatory, reputation, shared, supplier size and disruption risks can affect the supply chain of an outsourcing company. Other risks that occur rather infrequently, but that could critically cripple or get a company out of business, as mentioned by Hopp (2008) include environment hazards like the hurricane, and the act

of public enemy like terrorists amongst others. He then went ahead to develop a likelihood and consequences table to suggest how each should be handled. He suggested highly frequent but low impact risk like variation in process completion time or demand changes could be better managed by buffering (inventory or capacity) including use of best practices like risk pooling (centralisation, postponement, capacity chaining, etc). They could even be ignored altogether if the impact is too small on the process. Some more high level failures like some key members bailing out on the company or a strategic supplier failing or going bankrupt may necessitate having contingency plans as opposed to having material or capacity backups which may be rather too expensive. Some even still rarer but high impact situations like terrorist attacks and large scale environmental disaster may only be handled through crisis management because it is very difficult to predict when and how these may occur. This calls to question the appropriateness of utilisation of buffering in managing supply chain risks of the latter type, where frequency of occurrence is very low, prediction of location of occurrence is very difficult, the scale of effect could be very large, and pattern of evolution could be completely unique. This usually leads to carrying too expensive buffer, while this buffer may actually be worthless in the face of the actual occurrence of event.

5.1. What are the main classes of risks involved Supply Chain management

Classifying supply chain risk is a challenging task in itself. This is more so because the context has to be defined before the classification can be very meaningful. Some documented examples like Rao and Goldsby (2009) and Valany (2009) are based on industry sector, Tang (2006) based on sources in the supply chain: demand, supply, product and information management. Cucchiela and Gastaldi (2006) have used the internal and external activities of an organisation to classify the types of risks inherent in a supply chain. Internal risks, they noted, include capacity unavailability, information delays and regulatory non-compliance. External risks include competitor action, political environment, market price fluctuations, uncertain costs and supplier quality. Others include Svensson (2000) which classified based on qualitative and quantitative bases, Juttner (2005) based on demand, supply and environment, while Chopra and Sodhi (2004) used some nine parameters.

In this paper, classification focuses on all the risks included in the supply chain based on end to end approach, using functional areas to which they are related. This approach lumps internal or external risks together provided they affect similar functional aspects of a supply chain. The hope is to make such classification as generic as possible so that it may be easily integrated into level 2 processes in SCOR, which is our reference model of interest. Supply chain risks are, thus, classified into five: financial, informational, operational, occupational and regulatory. Financial risk covers the potential for monetary loss that the supply chain can be exposed to as a result of all its activities. Information risk includes the susceptibility of all of the supply chain activities to information inefficiency and external attacks. Operational risks include all forms of uncertainty in the input transformation processes while using the resources of the organisation to meet the demands of the customers. Occupational risk includes all the hazard of job that the workers of the company may be exposed to as a result of their job specification. Regulatory risk includes the potential for regulatory body to act against the organisation as a result of non-compliance to some stated or implied rule, or from the public based on their expectation from the firm as a responsible corporate citizen. This is further discussed in sections 8 and 9.

6. Supply Chain Vulnerability and Supply Chain Risk

Wagner and Bode (2006) state that there is no agreement about what is defined as supply chain risk among the scholars in the field. They emphasise the need to clarify the difference between four terms: supply chain risk, supply chain disruption, supply chain risk source and supply chain vulnerability. Also, in defining supply chain risk, while the formal mathematical definition used in decision theory considers it as not necessarily evil based on the concept of variance, which could be either negative (bad) or positive (good) deviation from expectation, the dictionary definition suggests a negative perspective. For the purpose of supply chain risk, they opine that the practitioners hold more to the negative side, and that such paradigm seems alright, given the effect of risk in the supply chain context. They define supply chain disruption as unintended, untoward situation which leads to supply chain risk. Supply chain risk sources have been discussed earlier and this is closely interlinked with risk classification.

Supply chain vulnerability, however, is said to be different from supply chain risk and disruption. While disruptions are usually external events that may affect the supply chain of the firm, vulnerability is related to the nature of the supply chain itself. A good definition for supply chain vulnerability was given by CIPS (2006) which defines it as a point of weakness or possible threat to the supply chain network. Vulnerability, they note, doesn't make the supply chain to fail, but provides an opportunity for failure once an external factor, defined earlier as disruption, affects the supply chain. Wagner and Bode (2006) capture this succinctly by noting that two organisations may be affected by the same disruption, but the effect on each depends on their different vulnerability levels. They conclude that the supply chain risk of an organisation is therefore a complex interplay of the activities of the risk sources present in a

supply chain, the disruption to trigger the sources and the vulnerability of the chain itself. This suggests that while two firms may have the same types of disruption, they may have different risk profiles due to different levels of vulnerability. Conversely, while two firms may have similar levels of vulnerability, their risk profile may differ based on their environment. To clearly manage supply chain risk, therefore, one needs an understanding of both the triggers and the vulnerability.

7. Case for vulnerability as a SCOR attribute

Having defined vulnerability and clarified its relationship to risk sources, disruptions and supply chain risk itself, attempt is made to make a case for vulnerability as a supply chain attribute in SCOR. To do that, one would like to answer the following six questions. Most answers would draw on the discussions made earlier.

7.1. Question 1: Should the attribute be risk or vulnerability?

While this question seems rather difficult to answer, the existing body of literature appears to have made vulnerability appear more like the actual supply chain attribute than risk. From the reference made to Wagner and Bode (2006) and CIPS (2006) in section 6, it suggests that risk is a consequence of two factors: vulnerability (which is innate to the supply chain); and disruption which is the external trigger of risk events. This suggests that once either of the two is prevented or ameliorated, then supply chain risk is curtailed or mitigated. To be consistent with this classification, therefore, one would rather stick to vulnerability as the supply chain attribute of interest, although the purpose is to control risk. Also, there could be factors that are not risks per se, but could still make the company vulnerable. One may, therefore, use vulnerability as the attribute and the risk classifications of financial, information, operational, occupational and regulatory risks for the control.

7.2. Question 2: Is there a difference between supply chain vulnerability and supply chain agility?

There appears to be a difference between supply chain vulnerability and supply chain agility, but they also have some interplay in supply chain risk. From the discussion of agility made earlier, agility seems to focus on the ability to recover if there is a failure, or take advantage of opportunities inherent in a general industry crisis, while vulnerability focuses on potential to fail if there is an undesirable event. The two are closely linked, but should be technically different. One may want to think of it this way: while agility measures can handle the risk components related to operational issues, there may be the need for something more than that for some other risk events like the acts of external aggression or a public enemy act. This means one needs more than agility metrics to fully account for vulnerability.

7.3. Question 3: Are there supply chains in likely need of other risk metrics than cost?

The strategic metric used for measuring supply chain risk in SCOR is the Value at Risk (VaR). VaR is defined as the sum of the probability of risk events and the monetary impact of these events across all the supply chain functions. This definition suggests the following: firstly, the probability of these events can be reasonably defined; and secondly, the value of for each event can be reasonably estimated. But it is not all supply chains that this definition fits very well. Consider the management of an electoral process, for instance. Compromising the supply process through the hijack of electoral materials or more importantly a hijack of the information system destroys the credibility of the process, especially in many African countries where contesting political parties openly claim suspicion of the electoral bodies, either due to precedence or to blackmail the umpire. Even if the error is fixed, the damage might still be incalculable. Consider again a military expedition; failure of some core functions could mean much more than the money lost. In fact, the whole war could be lost as in operation Barbarossa. Or consider an airline that could be attacked by terrorists; recovery is much less important than prevention. More scenarios could be developed including hijack of nuclear materials or an occupational risk like deadly infection in a medical concern or exposure to radiation. And yet there usually the need to model these chains too in many real life scenarios. This suggests that while there is need for some cost based measures in a supply chain risk management, the risk is much more than what monetary value can quantify in some other instances.

7.4. Question 4: Are there risk dimensions still inherent in some other SCOR metrics?

The answer to this question appears to be yes. To discuss this issue, consider one important SCOR metric; the order fulfilment cycle time, which measures responsiveness, an attribute of supply chain in SCOR. This is defined as the average actual cycle time consistently achieved to fulfil customer orders. It is mathematically defined as the sum of total time for all orders delivered divided by the total number of orders delivered. This measure captures the expectation for order delivery, but does not consider the spread of the fulfilment time. This will call to question how the consistency of delivery in the definition is measured. Two organisations with the same expected lead time but

different variance have the same expected cycle time (level of responsiveness), but cannot make the same claim of consistency to their customers because one would more consistently deliver while the other may not. This is the popular "flaw of averages". While one may argue about finding a way to incorporate this in the VaR analysis, it would most likely not achieve the same strategic result.

A more subtle one is the calculation of perfect order fulfilment, the strategic metric for reliability, which is also a supply chain attribute in SCOR. It has four level 2 metrics, and all orders must have 100 percent in each in order to have an overall 100 percent. If one company achieves 100 percent along three of the four level 2 metrics and 60 percent in one, it has a 60 percent achievement level. But a situation can be constructed in which another supply chain will achieve a 60 percent level of achievement in all the other level 2 metrics and still have 60 percent overall as well. These two may appear to have the same level of achievement in reliability score based on the current model, but they actually have different vulnerability levels. An example could make this clearer. If a supply chain disruption occurs affecting both chains in one of the dimensions where the former has 100 and the later 60 percent, and it reduces the achievement of each supply chain by 30 percent of their total orders, the latter's supply chain reliability performance may drop to as low as 30 percent while the former may still remain at the same level of 60 percent reliability as previously measured by SCOR. This example serves to indicate that there is a need to still highlight some important differences in supply chains that appear to have similar performance gaps along other metrics, but actually have different levels of vulnerability.

7.5. Question 5: How Different is VaR from Risk Mitigation Costs?

This is another important question seeing that VaR is a level 1 metric of agility while risk mitigation cost is a level 2 metric of cost. But a leading question to this would be to identify the purpose of calculation of VaR. If the purpose is only to only compare the expected monetary exposure of two supply chains for strategic decisions, but not to make financial commitment to insure such then they may be separate. In this case, however, it then seems more like a vulnerability metric than an agility metric. But then, one may still need some more risk dimensions other than money in order to make the best decision. But if determining VaR leads to making a financial outlay, then, it may probably be more appropriate to treat VaR as a form of risk mitigation cost as well. If VaR guides in the determination of the value of a fair premium to insure the chain, then it is probably more related to risk mitigation cost too. So, the separation probably needs to be re-investigated.

7.6. Can environmental considerations be incorporated into vulnerability?

Based on the classification of supply chain risk adopted in this paper as discussed, one should be able to include environmental concerns as some dimensions of vulnerability. Regulatory risk was defined to include the potential for the action of any regulatory body to act against the organisation as a result of non-compliance to some stated or implied rule, or the action of the public masses based on their expectation from the firm as a responsible corporate citizen. With the current trend in corporate environmental responsibility and the global sensitivity of environmental issues today, it is apparent that organisations would be getting more and more conscious of adherence to environmental standards. This risk may not always be that of forced legislative compliance, since companies in countries like Canada, for instance, might in the interim still be shielded from such, but there is almost a global pressure from the public masses on the other hand, which could make firms domiciled even in such "protected" countries to be forced to comply since most of them also manufacture and/or trade globally. This puts environmental compliance well in the domain of regulatory vulnerability. For as long as any company would do business in or with another country where environmental compliance is mandatory, they may also have to comply with the demands of the laws of the countries of their trading partner; probably including carbon taxing.

8. Vulnerability dimensions and their possible metrics

The objective of this section is not to provide actual metrics for vulnerability as an important dimension of a supply chain, but to argue the possibility of creating such in practical terms. Proper design and definition of metrics would be better done in another paper not to get distracted from the main issue at hand, which is the appropriateness of vulnerability as a supply chain attribute in SCOR, because it could take some reasonable space to address such at the level of details deserved.

Defining strategic (level 1) metrics for vulnerability may be done along the line of the suggested classes of risk as suggested in section 5.1, i.e. financial, informational, operational, occupational and regulatory. When building a SCORcard for the supply chain of interest, only the relevant ones would be selected from these metrics based on the strategic priorities of the supply chain in question.

While one does not give precise metrics for the dimension of vulnerability here, suggestion of some possible paths to defining one for each of them is made. Financial risk metrics are diverse, and many of these, of which VaR is one,

are available in the field of Financial Engineering. Good readings include Dowd (1998), Jorion (2001), Alexander (2001), Basak and Shapiro (2001) and Hull (2003). VaR may be a good choice though. One reason is due to the simplicity of its computation once the probability component is defined. Another reason is that it is easy to explain its concept to non-mathematically savvy users unlike some other risk metrics. A probably weightier factor in its favour is the popularity of the model and its acceptance in the financial sector based on the Basel accords.

Information security is another big field of research for which many metrics are already defined. Many of such quantitative metrics are built as weighted aggregate of a number of digital vulnerability or resilience issues including strength of encryption, right of access control, session time out, concurrent access prevention etc. Hinson (2006), Patriciu et al (2006), Savola and Neinonen (2011), Wang et al (2011) and Sissa et al (2011) are good references. Also, Payne (2006) and Chew et al (2008) are essential readings for people not inducted into the world of information security metrics.

Operational metrics could capture many of the process issues mentioned earlier like variance of cycle time, joint variance of the various level 2 metrics of reliability in SCOR, etc. Metrics for occupational risks could be taken from the field of occupational safety. Metrics could be defined based on the level of compliance to some standard expectation or the number of incidences reported (e.g. rate of hazard) for some factors. Regulatory risk can be measured based on the level of compliance to some stated rules or number of incidences observed for selected variables as well. Models indicating levels of environmental compliance or others showing level of emissions, level of recycling etc are good candidates here. These are already defined in GreenSCOR. Also, there are many countries with issues like local content, affirmative action, anti-trust rules, anti-graft rules and cabotage rules amongst others. This is where the level of compliance or number (or ratio) of observed incidences or regulatory infractions, number of near misses of incidents etc can be used to evaluate the regulatory vulnerability of such companies.

8.1. What should be the goal of vulnerability metrics: compliance or prevention?

In deciding what metrics are defined for each of the categories of risks identified, the goal of the measurement needs to be clarified: compliance or prevention. In the former, the interest is in being seen to have complied, even if there is incidence, so as to, at least, be covered against litigation and penalties. This is more like the goal post approach. The latter focuses on how much the risk is likely eliminated or mitigated. This is the capability approach. Which one seems adequate depends on the context, although the general trend of philosophy now is the latter.

Taking the VaR, for instance, it measures the instantaneous monetary value of loss that the supply chain is exposed to at that point in time to a certain level of confidence. But a flip side is to consider that one can decide to use this level of confidence of covering a particular level of exposure to make out a probability metric term, and this would be addressing the capability of the system in handling financial risk. If risk management in such case is handled by paying a premium to a third party, then VaR can be calculated but treated as a level 2 cost variable. In this case, probability of failure would be a strategic metric in vulnerability, while VaR would be part of the level 2 cost metrics like CO.2.7: Mitigation Costs. The full treatment may need to be investigated by an appropriate SCC focus group. Similar analysis could be done for some other dimensions of risk, like operational risk and the monetary equivalent of such errors could be determined. A possible model that can be adapted for converting such risk into monetary equivalent can be found in Langley et al (2009, pg 172).

9. A suggested Structure of SCOR attributes and strategic metrics

The inclusion of vulnerability as an attribute in SCOR would mean there are three (3) outwards facing and three (3) inward facing attributes in SCOR. The general structure of SCOR appears very good as it is, so one only presents how the inclusion of vulnerability might fit into the existing structure. This is given in Figure 2. The definition of the exact metrics has been avoided for now. A general framework for level 2 metrics for vulnerability is presented next.

9.1. Possible structure of level 2 metrics

The general structure of level 2 metrics for all the strategic metrics in vulnerability can be defined in a manner consistent with most other SCOR metrics. The level 2 metrics for VaR are already defined, and can simply be reclassified. The level 2 metric for informational risk can be defined in terms of plan informational risk, source informational risk, make informational risk deliver informational risk and return informational risk. The level 2 metrics for operational risk can be Source Variability, Make Variability, Deliver Variability and Return Variability. A similar approach can be adopted for the other vulnerability classes too.

10. Conclusion and anticipated benefits of changes in SCOR's strategic structure

Given the magnitude and frequency of risks facing supply chains today, including vulnerability as a supply chain attribute brings risk to a more strategic level, thereby making its management more holistic and receiving the attention it deserves. Such inclusion could further generalise and simplify the application of SCOR in some critical service chains like the military, health and others where there are risks with very low frequencies but catastrophic consequences. This would be done while still preserving parsimony of metrics as much as possible.

Areas to be explored as a sequel to this paper include the full definition of lower level metrics of vulnerability which cannot receive the desired attention in this paper. This can be followed by an empirical implementation of the proposed revised model in some service chains where such inclusions would prove valuable.

	Reliability	Responsiveness	Agility
External facing	Perfect order fulfilment	Order fulfilment cycle time	Upside flexibility Upside Adaptability Downside Adaptability
	Cost	**Asset**	**Vulnerability**
Internal facing	Supply Chain Management Cost Cost of goods sold	Cash-to-cash cycle time Return on supply chain fixed asset Return on working capital	Financial risk metric Information risk metric Operational risk metric Legislative risk metric Occupational risk metric

Figure 2: Proposed structure of attributes and strategic metrics for SCOR

Acknowledgement

The author wishes to acknowledge the contribution of the Research Development Programme for their financial assistance in furthering this research and others.

References

Aissa, A.B., Abercrombe, R.K., Sheldon, F.T. and Mili, A., Defining and Computing a Value Based Cyber-Security Measure, *Information Systems and E-Business Management*, pp. 1-21, 2011.

Alexander, C., Market Models: A guide to Financial Data Analysis. Wiley, Chichester, 2001.

Basak, S. And Shapiro, A., Value-at-Risk based Management: Optimal Policies and Asset Prices, *The review of Financial Studies*, vol. 14, pp. 371-405, 2001.

Blackhurst, J., Craighead, C.W., Elkins, D. and Handfield, R.B., An empirically derived agenda of critical research issues of supply chain disruption, *International Journal of Production Research*, vol. 43, no 19, pp. 4067 – 4081, 2005.

Chew, E., Swanson, M., Stine, K., Bartol, M., Brown, A. and Robinson, W., Performance Measurement Guide for Information Security, National Institute of Standards and Technology, US Department of Commerce, 2008.

Chopra, S. And Sodhi, M., Managing Risk to Avoid Supply Chain Breakdown, *MIT Sloan Management Review*, vol. 46, no. 1, pp. 53 – 62, 2004.

CIPS: http://www.imperiallogistics.co.za/documents/Supply-Chain-Vulnerability.pdf, January 21, 2012.

Cucchiela, F. and Gastaldi, M., Risk Management in Supply Chain: a real option approach, *Journal of Manufacturing Technology Management*, vol. 17, no. 6, pp. 700-20, 2006.

Dowd, K., Beyond Value at Risk, Wiley, Chichester, 1998.

Hopp, W.J. and Spearman, M.L., Factory Physics, 3rd Ed., McGraw-Hill International, 2008.

Hull, J.C., Options, Futures and Other Derivatives, 5th Ed., Prentice-Hall, Upper Saddle River, NJ, 2003.

Jotion, P., Value at Risk, McGraw-Hill, New York, 2001.

Lambert, D.M., Supply Chain Management. In Lambert D.M. (Ed.), Supply Chain Management: processes, partnerships and performance. SCMI, Sarasota Florida, pg 1, 2006.

Langley, J.C., Coyle, J.J., Gibson, B.J., Novack, R.A. and Bardi, E.J., Managing Supply Chain: A Logistics Approach, 8th Ed. South Western Cengage Ltd, 2009.
March, J. and Shapira, Z., Managerial Perspectives on Risk and Risk Taking, *Management Science*, vol. 33, no. 11, pp. 1404 – 1418, 1987.
Oakland, J.S., TQM text with cases, 3rd Ed. Elsevier, Butterworth Heinemann, 2003.
Olson, D. L. and Wu, D., Risk Management Models for Supply Chain, *Supply Chain Management: An international Journal*, vol. 16, no. 6, pp. 401 – 408, 2011.
Patriciu, V.-V., Priescu, I. and Nicolaescu, S., Security Metrics for Enterprise Information System, *Journal of Applied Quantitative Methods*, vol. 1, no. 2, pp. 151-159, 2006.
Payne, S.C., A guide to security metrics, SANS Security Essentials, GSEC Practical Assignment, Version 1.2e, 2006.
Savola, R.M. and Heinonen, P., A visualisation and modelling tool for Security metrics and measurements management, *2011 Information Security for South Africa*, proceedings of the ISSA 2011 conference, art no 6027518, 2011.
The Supply Chain Council, Supply Chain Operations Reference Model, Version 8, SCC Inc, 2006.
The Supply Chain Council, Supply Chain Operations Reference Model, Version 9, SCC Inc, 2008.
The Supply Chain Council, Supply Chain Operations Reference Model, Version 10, SCC Inc, 2010.
Wagner, S.M. and Bode, C., An empirical investigation into supply chain vulnerability, *Journal of Purchasing and Supply Management*, vol. 12, pp. 301 – 312, 2006.
Wang, J.A., Guo, M. And Wang, H., Measuring and ranking attacks based on vulnerability analysis, *Information systems and E-Business Management*, pp. 1-36, 2011.
Webster, S. Principles and tools for supply chain management. Mc-Graw Hill, NY, 2008.
Yang, B. and Yang, Y., Postponement in Supply Chain Risk Management: a complexity perspective. International Journal of Production Research, vol. 48, no.7, pp. 1901 – 1912, 2010.
Zsidisin, G.A., Panelli, A. and Upton, R., Purchasing organisation involvement in risk assessments, contingency plans and risk management: an exploratory study, *Supply Chain Management: An international Journal*, vol. 5, no. 4, pp. 187 – 197, 1999.
Zsidisin, G.A., A grounded definition of Supply Chain Risk, *Journal of Purchasing and Supply Management*, vol. 9 no. 5/6, pp. 217 – 224, 2003.

Biography

Olufemi Adetunji is a Senior Lecturer in the department of Industrial and Systems Engineering at the University of Pretoria, South Africa. He earned B.Sc. in Agricultural Engineering from University of Ibadan, Ibadan, Nigeria, Masters in Industrial and Production Engineering from the University of Ibadan, Ibadan, Nigeria, and PhD in Industrial and Systems Engineering from University Pretoria, Pretoria, South Africa. He is a certified SCOR professional, and has published journal and conference papers. Dr Adetunji has done research projects with a number of government and private institutions in South Africa.