Journal of Enterprise Information Management

Modeling information risk in supply chain using Bayesian networks

Satyendra Sharma Srikanta Routroy

Received 20 March 2014
Revised 15 September 2014
20 June 2015
17 July 2015
Accepted 4 August 2015

Modeling information risk in supply chain using Bayesian networks

Satyendra Sharma
Birla Institute of Technology and Science Pilani, Pilani, India, and
Srikanta Routroy
Department of Mechanical Engineering,
Birla Institute of Technology and Science Pilani, Pilani, India

Abstract
Purpose – Information sharing enhances the supply chain profitability significantly, but it may result in adverse impacts also (e.g. leakages of secret information to competitors, sharing of wrong information that result into losses). So, it is important to understand the various risk factors that lead to distortion in information sharing and results in negative consequences. Information risk identification and assessment in supply chain would help in choosing right mitigation strategies. The purpose of this paper is to identify various information risks that could impact a supply chain, and develop a conceptual framework to quantify them.
Design/methodology/approach – Bayesian belief network (BBN) modeling will be used to provide a framework for information risk analysis in a supply chain. Bayesian methodology provides the reasoning in causal relationship among various risk factors and incorporates both objective and subjective data.
Findings – This paper presents a causal relationship among various information risks in a supply chain. Three important risk factors, namely, information security, information leakages and reluctance toward information sharing showed influence on a company's revenue.
Practical implications – Capability of Bayesian networks while modeling in uncertain conditions, provides a prefect platform for analyzing the risk factors. BBN provides a more robust method for studying the impact or predicting various risk factors.
Originality/value – The major contribution of this paper is to develop a quantitative model for information risks in supply chain. This model can be updated when a new data arrives.
Keywords Information systems, Information management, Bayesian networks, Risk factors
Paper type Research paper

1. Introduction
A supply chain consists of all the parties involved, directly or indirectly, in fulfilling a customer request (Mentzer *et al.*, 2001). The supply chain not only includes the manufacturer and suppliers, but also transporters, warehouses, retailers and customers themselves. Within each organization, such as manufacturer, the supply chain includes all the functions involved in receiving and filling a customer request. In nutshell, a supply chain is the system of organizations, people, technology, activities, information and resources involved in moving a product or service from suppliers to customers. Vital and relevant information availability to a company in the supply chain, would help in optimizing the entire supply chain rather than just sub optimizing on a local interest. Accurate and timely information sharing across the supply chain improves supply chain visibility and that leads to enhanced supply chain performance (Caridi *et al.*, 2014). This would result into better planned overall production and distribution which can cut down costs and give a more enticing and catchy final product leading to higher sales (Sharma and Bhat, 2013).

Journal of Enterprise Information Management
Vol. 29 No. 2, 2016
pp. 238-254

1741-0398
DOI 10.1108/JEIM-03-2014-0031

In the past couple of decades, companies have been making use of the internet, intranets and extranets to exchange and share data, information, cognizance and knowledge along the supply chain (Balocco *et al.*, 2011; Choe, 2008; Perego and Salgaro, 2010). According to Pereira (2009), effective and efficient use of information communication technology (ICT) among all elements/parties of the supply chain is one of the critical factor for supply chain's success. While information sharing has been considered as one of the important pillar of supply chain efficiency, at the same time information sharing is also a source of vulnerability in the supply chain. In the today's contemporary world, in depth understanding about the various kinds of information risks like Virus, Worms and Trojans is gaining momentum and organizations have become more cautious in their approach toward sharing and managing information. But information risk management efforts are generally focussed within the boundaries of the organization.

This paper attempts to provide a modeling approach for information risk in the supply chain, which are caused by various interrelated internal and external factors. Information risk could also propagate and escalate through various causal links of risk factors and can lead to other types of risks in the supply chain. In order to understand the causal links between various supply chain information risk factors, a Bayesian network (BN) is developed so that each risk factor or variable is presented as a node with the directed links forming arcs between them that shows causal relationships. The probabilistic presentation of the interactions among risk factors is one of the key point of BNs and it allows the estimation of risks and uncertainties better than other models that only account for expected values.

Potential advantages of BNs compared with other approaches (network-based approaches, principal-agent approaches, behavioral approaches, Stochastic models) to modeling supply chain disruptions include the compact representation, the robustness to small alterations of the model, the ability to operate with different variable types, the facilitation of prior knowledge, the ability to handle incomplete data sets and a form of learning can be used. A security risk analysis model using BN was proposed by Feng *et al.* (2014). In the following paper, in Section 2, we represent the relevant research considering the information risk management and various approaches used in information risk modeling. In Section 3, we provide a brief overview of Bayesian belief network (BBN) modeling. In Section 4, we present the details of our model. In Section 5, proposed model is tested through a illustrative example, and present the results and sensitivity analysis to identify the critical information risk factors. In Section 6, we provided the managerial implication and limitations of this research study. The last section of the paper discusses the conclusions and future scope of research.

2. Literature review

Information management plays an important role in the supply chain (Closs *et al.*, 2005; Gunasekaran *et al.*, 2008). Daugherty *et al.* (2006) considered information as a source of competitive advantage, in which the business data process is shared in a controlled way and an integrated and coordinated supply chain can be achieved (Wang *et al.*, 2008; Boulesnane and Bouzidi, 2013). "Information is the substance from which the managerial decisions are made" (Forrester, 1962) and one of the pillars which supports a solid supply chain (Ballou *et al.*, 2000; Ketikidis *et al.*, 2008). In fact, delayed, scarce or distorted information can create serious problems in the supply chain (Chow *et al.*, 2008;

Handfield and Nichols, 2002; Power, 2005). One of the most serious effect is known as the bullwhip effect and was first identified by Forrester (1962). Globalization has caused increased complexity in the supply chain (Craighead *et al.*, 2007). Information technologies designed to manage complex information flows within or between firms helps in creating value in supply chain by lowering the costs or increasing the service level (Biehl, 2005; Papadakis, 2006; Pandey *et al.*, 2010).

Information is a critical driver for supply chain coordination and integration (Faisal *et al.*, 2007). Dell depends on information exchange to help diverse members of a supply chain work together efficiently and effectively. Wal-Mart and Proctor and Gamble have been sharing point-of-sale and real-time inventory information for a long time now. Other companies such as, Cisco, Dillard Department Stores, JC Penney and Lucent Technologies have also initiated similar information sharing strategies (Date and Raoot, 2014). Today's exponential enhancements in the fields of information, computing and communication technologies along with the decline of entry and trading barriers have altered the commercial relationships among supply chain partners enhancing the exposure to various types of risks (Ritchie and Brindley, 2000). Although ICT can be a conduit for information transfer, it can also introduce risks to confidentiality, integrity and availability in the supply chain (Smith *et al.*, 2007).

In supply chain risk management (SCRM) literature authors have talked about operational risk, disruption risk, but SCRM literature is lacking on information risk management in a supply chain. Information risk is a field, which has not been extensively researched. Although it's importance is well recognized in SCM literature. Information risk can be defined as "the probability of loss arising because of incorrect, incomplete, or illegal access to information" (Faisal *et al.*, 2007). Risk is something that might yield loss. Therefore, with regard to "information risk factors can be defined as condition, element, or activity in information sharing and medium of information sharing that may adversely affect the supply chain performance."

In SCRM literature information risk is defined form two different perspectives. These two streams are "Information sharing perspective" and "IT infrastructure security perspective." Information sharing benefits supply chain but however, information sharing in the supply chain can also result into an adverse effect, namely, information leakage (Lee and Whang, 2000; Hoecht and Trott, 2006; Anand and Goyal, 2009). In general, information leakage means confidential information is unintentionally or intentionally revealed to unauthorized parties. Zhang *et al.* (2011) presented a conceptual model of such information leakage.

Another stream of research on information risk in supply chain discusses for "IT infrastructure threats," which may cause security problems (Peltier, 2007; Cavusoglu *et al.*, 2009). Security risk exposure is represented as a function of the probability of the threats and the expected loss due to the IT infrastructure vulnerability. Faisal *et al.* (2007) broadly classified the information risk into four categories, namely, information security and breakdown risks, forecasts risks, intellectual property risks and information sharing risks. Some of the risks such as natural disasters, security breaches have immediate impact and is realized easily whereas certain risk factors such as intellectual property risk are not immediate nonetheless critical for the viability of supply chain. Spekman and Davis (2004) classify information risk in supply chain into: "Security dimension" and "Relationship dimension." Following section provides a discussion on information risk from both perspectives, namely, IT/physical infrastructure and behavioral risks arising due to information sharing.

2.1 Information risk due to security dimension

The large size companies have large networks and thereby large information systems. The larger the information system, more is the failure threat. Although rare, information infrastructure breakdown can devastate today's highly networked environments (Chopra and Sodhi, 2004).

Faisal *et al.* (2007) have listed various forms of security risks (Table I).

2.2 Information risk due to information sharing

ICT facilitates the sharing of data and information. However there can be reluctance in sharing of critical data and relevant information owing to distrust or lack of confidence within the supply chain. The value of information sharing within a supply chain has been analyzed extensively by a number of researchers. Through information and data sharing, the demand information flows upstream from the point of sales to the manufacturer end, while product availability information flows downstream from the manufacturer point to the customer end in a systematic and organized manner (Yu *et al.*, 2001; Lumsden and Mirzabeiki, 2008). Moreover, information sharing ensures that the right and relevant information is available for the right trading partner in the right place and at the right time. However, in a dynamic supply chain environment, critical information cannot be truly and equally shared because of the conflict of interest among the node enterprises. Based on, Jinyan and Qiang (2004), Yuan (2007), Jiang *et al.* (2004), Ahn and Badrinath (2004), we have summed that there are at least nine risks during the process of information sharing in the supply chain.

Table II contains a collection of risk factors that have been previously identified in literature.

Table I contains five risk factors related to IT hardware security. While Table II contains nine risk factors describing information sharing risks in a supply chain. These 14 risk factors identified through SCRM literature review were presented to subject

Security risks	Risk description
Hackers, viruses and worms	Viruses, worms and trojans are common menace to information systems. In a supply chain. Tiers II and III level suppliers who are generally small and medium enterprises, are the ones most susceptible to such problems
Spyware	It is a program that resides on computers linked to the internet and surreptitiously collects various types of personal information
Internal employee frauds	Employee frauds can happen due to various reasons such as employee attrition, intentional/unintentional disclosure of proprietary information or in some cases personal vendetta against the company
Distributed denial of services attacks	The three most common categories of DDoS are bandwidth consumption, resource starvation and resource exploitation. These attacks interrupt legitimate access to the networks that may ultimately result in interruption to supply chain operations
Natural disasters and terrorist attacks	Tsunami, hurricanes, fires or terrorist attacks like 9/11 have brought forth the importance of not only data backup but have made organizations to seriously think of mirror sites to keep the flow of information uninterrupted in a supply chain

Source: Faisal *et al.* (2007)

Table I. Information security risks

Risk factor	Description
Cost increasing	Investment in the infrastructure, software and hardware, staff training will make the supply chain operation cost increase
Asset specificity	The information system and management may be not compatible with other systems
Leaking business secrets	Information sharing has the potential risk of revealing partners business secret
Damaging partners benefit	The retailers insist demand information is business secret and worry about information sharing will damage their benefit
Losing bargaining competence	If all the information is shared in the supply chain, it may cause the risk of part of enterprises losing bargaining competence
Monitoring difficulty	Some partners may disguise as actively involving in information sharing and share benefits of other partners
SCM alliance dissolution	When one partner departs the supply chain, the assets invested will become sunk costs
Information transmission	There are risks how to collect, sort, guarantee the shared information to be transferred quickly and accurately
Information security	Information sharing is easily to be attacked by Viruses, Worms and Hackers
Profit risk	Enterprises of supply chain lose part of higher profit which is originally coming from the exclusive and highly competitive information or resources they have controlled
Management risk	It becomes difficult for the management to handle when enterprises are not willing to share information because of the fear of losing competitive advantage
Moral risk	Information asymmetry is caused when enterprises pay more attention to their own interests and do not maintain a co-operative relationship of mutual trust and benefit

Table II.
Main information sharing risks in supply chain

matter experts (SMEs) and were asked to rate the risk factors according to their relative importance in supply chains and eliminate unimportant risk factors.

In the Table III we have taken into account only such risk factors that disrupt the IS/IT of the supply chain in order to develop a BN model that can help in the analysis of information risk. Information risk in a supply chain has severe impact in times of globalized world, where IT is a key enabler for supply chain performance.

S. No.	Information risk factor	A	B	C	D	E	F
1	Information risk breakdown	X		X			
2	Hackers, Viruses and Worms		X	X	X	X	
3	Spyware			X			
4	Internal employee frauds			X			
5	Distributed denial of services attacks			X			
6	Natural disasters and terrorist attacks			X			X
7	Distorted information				X	X	
8	Cost increasing risk			X			
9	Assets specificity	X	X	X	X		
10	Losing bargaining competence						X

Note: X, denotes the discussion of risk factor in the research paper mentioned at the bottom of the table
Sources: A – Chopra and Sodhi (2004); B – Wu *et al.* (2006); C – Faisal *et al.* (2007); D – Blackhurst *et al.* (2008); E – Wagner and Bode (2008); F – Finch (2004)

Table III.
IS/IT risk factors and their references

Authors, namely, Faisal *et al.* (2007), Cavusoglu *et al.* (2009), and Boulesnane and Bouzidi (2013) discussed the importance of information in supply chain and information threats that can derail SCM performance. There are some conceptual studies on supply chain information risk but SCRM literature lacks on supply chain information risk modeling part. In his research through extant literature review and through SME consultation ten risk factors were identified that are presented in Table III.

3. Research methodology

The study focusses at developing a BN for analyzing the various information risks within a supply chain. A thorough literature review has led us to identification of various risk factors in information security as well as risks associated with information sharing in a supply chain. These risks have to be incorporated in a model establishing relationship between them. For risk assessment, BNs can be used to create information risk profile of a supply chain. Subsection 3.1 provides a brief description of BNs.

3.1 BNs

For the last few years, BNs have become a popular tool for modeling various statistical problems. BNs are being used for modeling uncertain and complex domains such as ecosystems and environmental management. BNs provide a methodology for summing the subjective beliefs with the available evidences (Pai *et al.*, 2003; Cowell *et al.*, 2007; Lockamy and McCormack, 2010, 2012). A BN is an annotated directed acyclic graph (DAG) that encodes probabilistic relationships among nodes of interest in an uncertain reasoning problem (Jensen, 1996; Pai *et al.*, 2003). The representation describes these probabilistic relationships and includes a qualitative structure that facilitates communication between a user and a system incorporating a probabilistic model. BN foundation is based on the work of the mathematician, theologian Rev. Thomas Bayes who worked with conditional probability theory in the late 1700s to discover and reveal a basic law of probability which came to be known as Bayes theorem.

Formally, a BN for a set of random variables $U = \{X_1, \ldots, X_n\}$ is a pair, $B = (G, H)$ where G represents its DAG structure, and H represents the parameters that quantifies the network. The random variables are represented as vertices, and parental relationships between these random variables are represented as edges. If there is an edge from X_i to X_j, then we say that node (variable) X_i is called the parent of X_j and X_j is called the child of X_i. If a node does not have any parent nodes, it is called a root node. On the other hand, a node without any child node is called a leaf or outcome node. Here, it is important to note that there is no distinction between a node and a variable in BNs, and these variables can be discrete or continuous.

For a discrete variable, each node contains one of its states, which may be unknown to the decision maker. A state simply explains the condition of a variable or possible values that a variable may take. A variable X_i with its parents, pa(X_i), specifies a conditional probability distribution, $P(X_i|\text{pa}(X_i))$. This is a conditional probability table (CPT) for a set of discrete variables. Number of states of a parent node exacerbates the CPT complexity. BNs are used to trace how a change in certainty to one variable may affect the certainty on others (Jensen, 1996). If we know the joint probability function of all variables, $P(U) = P(X_1, \ldots, X_n)$, we can answer this question by finding marginal distribution of a variable, $P(X_i)$, or finding the conditional distribution of X_i given the evidence, e, $P(X_i|e)$.

The notion of evidence means that some of the variables are observed and take values from their respective domains. However, to calculate $P(U)$ for a large network is complex and intractable since *P*(*U*) grows exponentially with the number of variables. The usefulness and appropriateness of BNs lies in its veracity that by using Bayes theorem, one can estimate just not the probability distributions of child nodes provided the values of their parents, but even the distributions of the parents given the values of their children. Bayes' theorem states that:

$$P(H|E,c) = \frac{P(H|c) * P(E|H,c)}{P(E|c)}$$

The posterior probability is given by the left-hand term of the equation, $P(H|E,c)$. It represents the probability of hypothesis *H* after considering the effect of evidence *E* on past experience *c*. The term $P(H|c)$ is the a priori probability of *H* given *c* alone. Thus, the a priori probability can be viewed as the subjective belief of occurrence of hypothesis *H* based upon past experience. The likelihood, represented by the term $P(E|H,c)$, gives the probability of the evidence assuming the hypothesis *H* and the background information c is true. The term $P(E|c)$ is independent of *H* and is regarded as a normalizing or scaling factor (Niedermayer, 2003). Thus, BNs provide a methodology for combining subjective beliefs with available evidence.

BNs can used in both ways like: top to bottom, that is used as a predictive modeling and bottom to top, that is used as diagnostic tool. That is, one can move not only from causes to consequences, but also calculate the probabilities of different causes provided the consequences. BNs are used for the analysis of data and expert knowledge especially in fields that are fraught with uncertainty, since they make it possible to treat uncertainty explicitly. They are also used to create "expert systems" that model include expert knowledge about a complicated domain such as medicine and medical research.

BNs can also be supplemented with decision support tools (Jensen, 2001), which is a natural addition to the ability to treat uncertainty in the first place. One of the biggest advantage of using BNs is to facilitate flexible inferences with partial information. However, tremendous gains in computational power along with the development of heuristic search techniques to find events with the highest probability have enhanced the development and understanding of BNs. Correspondingly, the Bayesian computational concept has become increasingly popular in such areas as medical diagnosis and weapon tracking systems and safety science (Brooker, 2011). The methodology has been shown to be especially useful when information about past and/or current situations is vague, incomplete, conflicting and uncertain (Maleki *et al.*, 2013). Pai *et al.* (2003) were among the first researchers to analyze supply chain risks using BNs.

3.2 BBN modeling steps

The following diagram represents the methodological steps used in this study (Figure 1).

Implementation of BBNs modeling requires risk factor identification and then establishing relationship between them. The initial stage in the BBN model development is structural development and evaluation, which on the first iteration will produce an unparameterized causal network. This phase of model development can be undertaken via a knowledge or data-based approach. Knowledge-based model development is done through expert elicitation of parameters. The information risk factors were identified using literature review and then prepared list was sent to

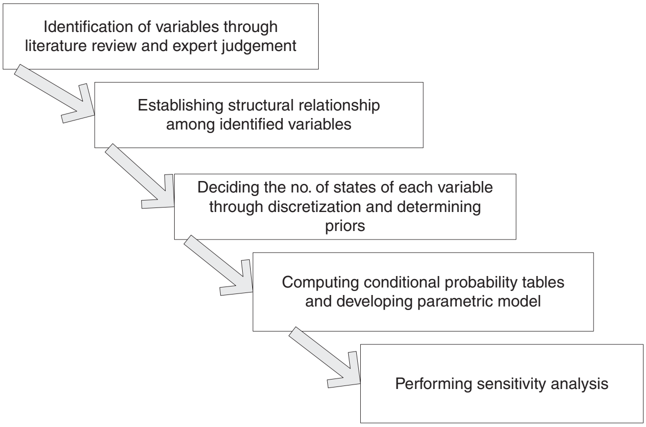

Figure 1. Steps in Bayesian belief network (BBN) model

experts for validation. Once relevant variables were identified, then experts were asked to draw linkages among various risk factors, used in the study.

For establishing structural relationship among variables, Delphi method was used. Once, opinions of experts converged on a particular structure, that was taken for further evaluation. The experts were IT managers and supply chain managers. In step 3, prior to parameterization, all variables were discretized into states. For continuous variables, states were further discretized into sub-ranges. Wherever possible, states were established using recognized classifications, management thresholds or guidelines. Where, these guidelines were not available, sub-ranges were specified with the guidance of the experts. The number of "states" or "classes" assigned to each variable were not pre-determined, but evaluated and assigned on an individual basis. In step 4, expert elicitation is applied to the whole CPTs, rather than individual parameters. For parent nodes, priors were elicited and for child nodes, CPT was elicited for each possible states for particular child node.

In this study, guidance for elicitation was sought from Morgan and Henrion (1990). In the last step, sensitivity analysis is used to measure the sensitivity of changes in probabilities of query nodes(output variables) when parameters and inputs are changed. The query nodes in this study were model endpoints. Two types of sensitivity analyses were used in evaluating the BBN. The first, "sensitivity to findings," considers how the BN's posterior distributions change under different conditions, while the second, "sensitivity to parameters," considers how the BN's posterior distributions change when parameters are altered (Chin *et al.*, 2009). In the next section a brief overview of BBN modeling has been provided.

4. Research model

This research study employs a risk assessment model for quantifying information risks in a supply chain. The model consists of the following risk factors: information breakdown factors, information leakage factors and reluctance in information sharing factors. Information breakdown factors are related to information security factors. Similarly Information leakage factors and reluctance in information sharing factors are related to information sharing risk factors. These risk factors are developed based on literature review and expert interviews. Five senior-level managers in supply chain/IT domain were consulted and based on their feedback, the following model structure has been proposed for information risk analysis. Profile of respondents in this study is explained in next Section 4.1. Model also shows the relationship between the various variables (information risk factors). Each node represents a risk factor and direction of the arrow signifies the relationship between them. This diagram showing structural relationship is also known as influence diagram.

4.1 Data collection

In model structure given in Figure 2, consideration was only given to the relationship between parent nodes and child nodes. This structure was created in consultation with SMEs and that ensures that proposed graphical structure is more likely than other. Next step is eliciting the SME knowledge and past data into probabilities and conditional statements (Zeng and Sycara, 1998). The model uses a set of measures and scales for each risk factor. Measures and scales used in this study are discretized and range of various measures has been shown in Table IV.

SMEs were provided with a questionnaire containing risk factor name and column for indicating their associated probability value. For child nodes, CPTs were provided to SMEs. A probability value is assigned to each range based on SME input in an automotive supply chain. The measures and scales are used to create total information risk profile. The data sample consists five major automobile manufacturers in India. These five companies were OEMs in automotive sector operating in India. The selected

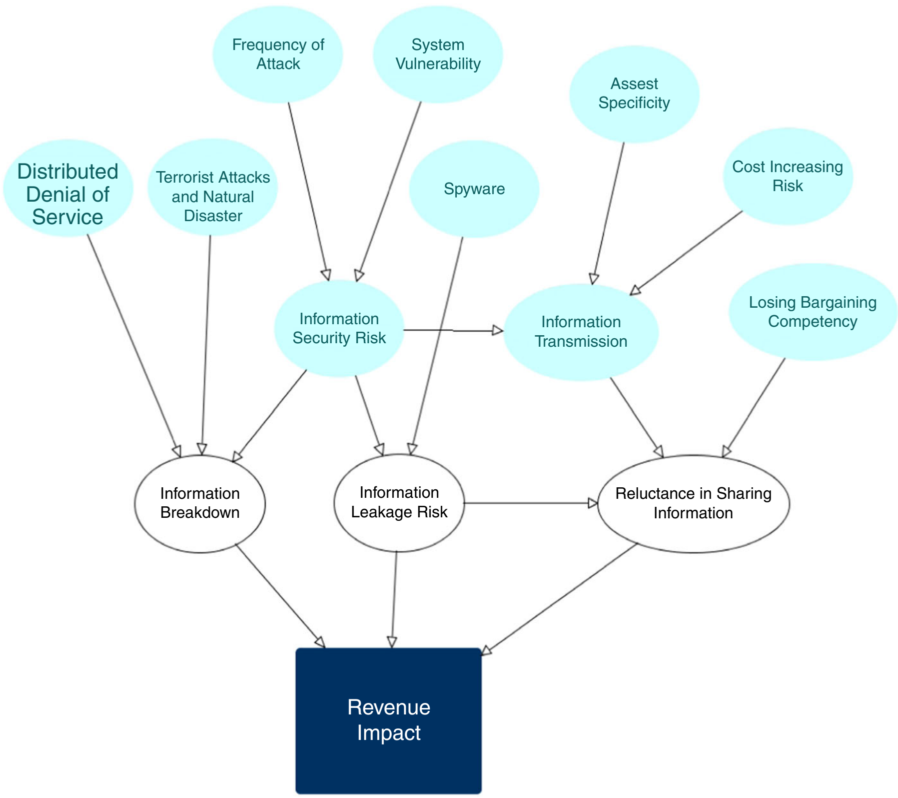

Figure 2.
The proposed framework for Bayesian network

Information risk factor	Measurement scale	
Frequency of attacks	High (100-150)	0.6
	Medium (50-100)	0.227
	Low (0-50)	0.172
System vulnerability	High	0.428
	Medium	0.357
	Low	0.214
Information security	High	0.413
	Medium	0.431
	Low	0.154
Asset specificity	Very high	0.132
	High	0.264
	Medium	0.235
	Low	0.105
	Very low	0.264
Cost increasing risk	High	0.2
	Medium	0.6
	Low	0.2
Losing bargaining competency	High	0.272
	Medium	0.545
	Low	0.182
Information transmission	High	0.183
	Medium	0.693
	Low	0.123
Spyware	High	0.154
	Medium	0.076
	Low	0.769
Terrorist attacks and natural disaster	High	0.0625
	Medium	0.312
	Low	0.625
Distributed denial of service	High	0.25
	Medium	0.416
	Low	0.333
Information breakdown	High	0.093
	Medium	0.620
	Low	0.285
Information leakage	Very high	0.048
	High	0.144
	Medium	0.373
	Low	0.33
	Very low	0.101
Reluctance in information sharing	Very high	0.016
	High	0.22
	Medium	0.514
	Low	0.23
	Very low	0.018
Revenue impact	Very high	0.0
	High	0.114
	Medium	0.404
	Low	0.376
	Very low	0.098

Table IV. Showing the risk factors and the obtained value

OEMs were large and their turnover is more than 5,000 cores and employee size is greater than 2,000. OEMs are considered as focal companies in the automotive supply chain and OEMs lead initiatives related to SCRM.

Any SCRM effort requires a leadership from the large company in the supply chain, who takes a lead role and involves all others in SCRM effort. The managers operating in supply chain domain and are responsible for information technology projects were considered as respondents or SME in this study. These SMEs were having more than ten years of experience in their respective fields. For prescribing range of various risk factors, a group of eight experts in supply chain and information technology were consulted and based on their input measurement scale was developed for each variable in the model. It was hard to find databases for certain risk factors like losing bargaining competency, information leakages. For few variables historical data were available. For these available databases also companies were reluctant to share data. So five point rating scale was used for rating all risk factors.

5. Data analysis

The BN deals with the various information risks involved in a supply chain. The nodes in the BN represent risk factors. The BN was tested for a set of data obtained for various input nodes assigning normal distribution to the rest. The BN was modeled using Agena Risk software. Figure 3 shows the distributions and results obtained after simulating the model using input data.

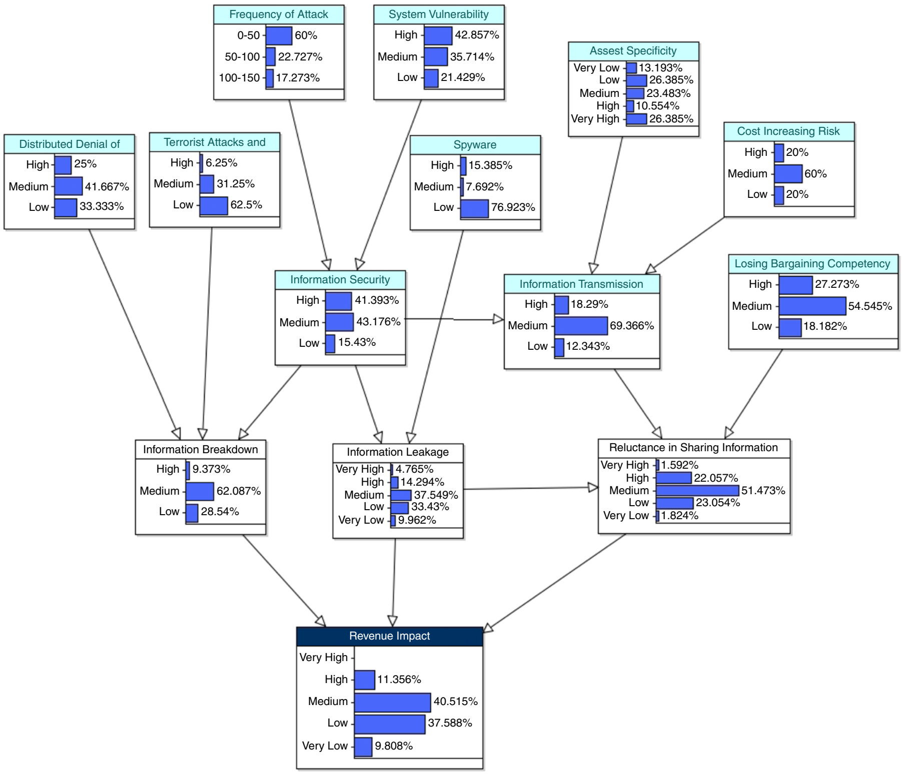

Figure 3.
The results of the simulation done using Agena risk

Thus, the model examines the probability of a company's revenue impact on a company based upon the firms' associated information breakdown, information leakages and information sharing risks. The risk factors, namely, information breakdown, information leakages and information sharing risks were determined based upon the a priori probabilities for risk events which directly influence them. These prior probabilities of parent nodes were ascertained via the data collection process explained in Section 4.1. BNs cannot only be used to model risk and find the impact on revenues but can also be used on a more backward approach (bottom to top) to diagnose the possible causes of variation in profitability due to information supply chain risk factors.

When we know a variable's real state out of possible states in the model, we can study its impact on distributions on other modes as well. BNs not only predicts the backward trends but also incorporates changes due to uncertainty in model. As Figure 4 provides the backward reasoning when provided with data such as high impact on revenue, probability of information breakdown as well as reluctance on information sharing factors are low. Thus it is evident that the impact on revenue is from information leakage which is evident from the results obtained as shown in the Figure 4. Subsequently all other parent nodes have been altered to incorporate the sudden changes in the model. This can help in narrowing down various risk factors that might have resulted in a certain scenario. For example, in the below figure gives these circumstances such that high frequency of attacks or risk from a spy ware will affect company's revenue.

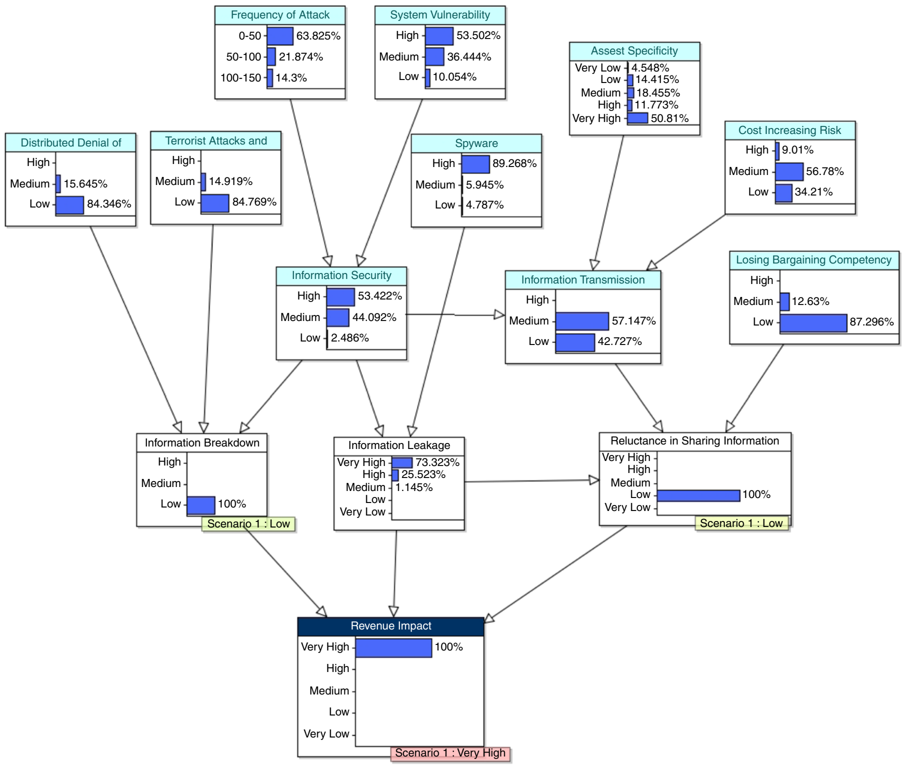

Figure 4.
Analysis of risk factors when results are known

6. Managerial and theoretical implication

In this research paper an information risk analysis model has been developed using BBN. In Bayesian models, reasoning can be done in both ways. The query variable (net impact on revenue) is affected by information risk factors. The impact of these risk factors on business revenue can be studied by managers using BBN. BBN can be used to disseminate understanding about supply chain information risk factors among industry professionals. For some of the risk factors that cannot be expressed in objective data form, their probability can be inferenced using subjective data (expert's judgment). Propagation analysis using BBN helps managers to update the probability, when new data arrives. In risk analysis, probability updating can be defined as the task of computing all posterior marginal's of non-evidence variables given the evidence.

Sensitivity analysis also explains the importance of various risk factors. Backward reasoning can be performed in BBN and responsible factors can be diagnosed. Results of sensitivity analysis show that "lose in bargain power" and "assets specificity" are most important causes of hiding information. Managers can use this model to enquire about what are prominent causes of lack of information sharing that ultimately affects the business performance. Sensitivity analysis can be performed to determine the effects of known risk factors (information breakdown, information leakages and limited information sharing) on company's revenue. A comparison of the firm's risk profiles based upon a priori risk event probabilities and worst-case combinations of information breakdown, information leakages and limited information sharing (excluding the scenario where all three risks have a 100 percent probability of occurrence) is shown in Figure 4. Information leakages proved to be very prominent risk factor.

The most prevalent worst-case combination for the firm is the simultaneous occurrence of information breakdown, information leakages and limited information sharing risk factors.

In information modeling, BN is developed to simultaneously define the risk factors and their causal relationships based on the knowledge from observed cases and domain experts. Then, the security vulnerability propagation analysis is performed to determine the propagation paths with the highest probability and the largest estimated risk value. BBN Model enables organizations to establish proactive security risk management plans for information systems.

The proposed Bayesian model supports the evidence-based practice. The Bayesian modeling can be used to test hypotheses and theories. BBN tests theories in the light of new evidences. This research also provides the directions to researchers, who want to use BBN modeling. In this research, a practical method has been used for structural and parametric learning. This methodology also provides guidelines for updating the posterior probabilities with generation of new evidences. This research provides a theoretical information risk model that has been tested using BBN.

7. Limitations

The study was conducted in automotive industry, therefore, the results could be industry-specific in nature. In addition, the study examined only five companies in the Indian automotive industry and for confidential reasons calculation were not performed for a specific firm, thus limiting the generalizability of information risks in this sector. A limitation related to the use of the BN methodology presented in this study is the ability to access the necessary data needed to construct the BNs. Depending on the established relationship, some companies may be reluctant to share risk profile data with their customers.

However, the most important potential limitation in BBN methodology is to assess risks in supply networks is the supplier's ability to provide accurate information regarding information breakdown, information leakages and limited information sharing risk factors as reflected in the 12 risk factors outlined in Figure 2. There must be willingness to periodically update this information in order to construct a risk profile that is valid and reliable. Managers hesitate to continually update due to deliberate inattention to various risk factors. Expert opinions and judgments are on the center stage of the proposed model. The better decision situations occur only if the knowledge of stakeholders is directed in a well-organized way. Value at Risk calculations were not performed because companies were reluctant to share their revenue impact data.

8. Conclusion and future scope of research

In this research paper, we have proposed a risk assessment model for supply chain information risk using BNs. As we have discussed the capability of BNs while modeling in uncertain conditions, this provides a prefect platform for analyzing the models providing a more robust method for studying the impact or predicting various risk factors at play. The data analysis shows result obtained for a case study and the changes observed in the values of probabilities when certain data sets are known with full certainty. As mentioned earlier the probability distribution can be made more reliable and accurate if filed data are provided to us. One of the positive feature of the BN is its ability to incorporate new data to change probability distribution. Hence, to improve the predictions made in the case study the model need to be fed with more reliable data, which also remains a limitation for the project. Risk profiles for companies and supply networks in other industries should be examined using the methodology illustrated in this study to determine, if industry dynamics significantly influence supply chain risks.

References

Ahn, G.J. and Badrinath, M. (2004), "Secure information sharing using role-based delegation", *International Conference on ITCC 2004*, Vol. 2 No. 4, pp. 810-815.

Anand, K.S. and Goyal, M. (2009), "Strategic information management under leakage in a supply chain", *Management Science*, Vol. 55 No. 3, pp. 438-452.

Ballou, R.H., Gilbert, S.M. and Mukherjee, A. (2000), "New managerial challenges from supply chain opportunities", *Industrial Marketing Management*, Vol. 29 No. 3, pp. 7-18.

Balocco, R., Miragliotta, G., Perego, A. and Tumino, A. (2011), "RFID adoption in the FMCG supply chain: an interpretative framework", *Supply Chain Management: An International Journal*, Vol. 16 No. 5, pp. 299-315.

Biehl, M. (2005), "Selecting internal and external supply chain functionality: the case of ERP systems versus electronic marketplaces", *Journal of Enterprise Information Management*, Vol. 18 No. 4, pp. 441-457.

Blackhurst, J.V., Scheibe, K.P. and Johnson, D.J. (2008), "Supplier risk assessment and monitoring for the automotive industry", *International Journal of Physical Distribution and Logistics Management*, Vol. 38 No. 2, pp. 143-165.

Boulesnane, S. and Bouzidi, L. (2013), "The mediating role of information technology in the decision making context", *Journal of Enterprise Information Management*, Vol. 26 No. 4, pp. 387-399.

Brooker, P. (2011), "Experts, bayesian belief networks, rare events and aviation risk estimates", *Safety Science*, Vol. 49 No. 8, pp. 1142-1155.

Caridi, M., Moretto, A., Perego, A. and Tumino, A. (2014), "Benefits of supply chain visibility: a value assessment model", *International Journal of Production Economics*, Vol. 151 No. 2, pp. 1-19.

Cavusoglu, H., Mishra, B. and Raghunathan, S. (2009), "The effect of internet security breach announcements on market value: capital market reactions for breached firms and internet security developers", *International Journal of Electronic Commerce*, Vol. 14 No. 3, pp. 69-104.

Chin, K.S., Tang, D.W. and Yang, J.B. (2009), "Assessing new product development project risk by Bayesian network with a systematic probability generation methodology", *Expert Systems with Applications*, Vol. 36 No. 6, pp. 9879-9890.

Choe, J.M. (2008), "The effects of EDI usage on production performance through the changes of management control systems", *Production Planning and Control*, Vol. 19 No. 6, pp. 577-589.

Chopra, S. and Sodhi, M.S. (2004), "Managing risk to avoid supply chain breakdown", *Sloan Management Review*, Vol. 46 No. 1, pp. 53-61.

Chow, W.S., Madu, C.N., Kuei, C.H., Lu, M.H., Lin, C. and Tseng, H. (2008), "Supply chain management in the US and Taiwan: an empirical study", *Omega*, Vol. 36 No. 2, pp. 665-679.

Closs, D.J., Swink, M. and Nair, A. (2005), "The role of information connectivity in making flexible logistics programs successful", *International Journal of Physical Distribution and Logistics Management*, Vol. 35, pp. 258-277.

Cowell, R.G., Verrall, R.J. and Yoon, Y.K. (2007), "Modeling operational risk with Bayesian networks", *Journal of Risk and Insurance*, Vol. 74 No. 4, pp. 795-827.

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J. and Handfield, R.B. (2007), "The severity of supply chain disruptions: design characteristics and mitigation capabilities", *Management Science*, Vol. 38 No. 1, pp. 31-155.

Date, G.H. and Raoot, A.D. (2014), "Review on IT adoption: insights from recent technologies", *Journal of Enterprise Information Management*, Vol. 27 No. 4, pp. 488-502.

Daugherty, P.J., Richey, R.G., Roath, A.S., Min, S., Chen, H., Arndt, A.D. and Genchev, S.E. (2006), "Is collaboration paying off for firms?", *Business Horizons*, Vol. 49 No. 3, pp. 61-70.

Faisal, M.N., Banwet, D.K. and Shankar, R. (2007), "Information risks management in supply chains: an assessment and mitigation framework", *Journal of Enterprise Information Management*, Vol. 20 No. 6, pp. 677-699.

Feng, N., Wangb, H.J. and Li, M. (2014), "A security risk analysis model for information systems: causal relationships of risk factors and vulnerability propagation analysis", *Information Sciences*, Vol. 256 Nos 10-11, pp. 57-73.

Finch, P. (2004), "Supply chain risk management", *Supply Chain Management: An International Journal*, Vol. 9 No. 2, pp. 183-196.

Forrester, J.W. (1962), *Industrial Dynamics*, MIT Press, Cambridge, MA.

Gunasekaran, A., Lai, K.H. and Edwin Cheng, T.C. (2008), "Responsive supply chain: a competitive strategy in a networked economy", *Omega*, Vol. 36 No. 4, pp. 549-564.

Handfield, R.B. and Nichols, E.L. (2002), *Supply Chain Redesign: Transforming Supply Chains into Integrated Value System*, Financial Times/Prentice Hall, Upper Saddle River, NJ.

Hoecht, A. and Trott, P. (2006), "Innovation risks of strategic outsourcing", *Technovation*, Vol. 26 Nos 5-6, pp. 672-681.

Jensen, F.V. (1996), " Experts, Bayesian belief networks, rare events and aviation risk estimates", *An Introduction to Bayesian Networks*, Vol. 210, UCL Press, London.

Jensen, F.V. (2001), *Bayesian Networks and Decision Graphs*, ISBN 0387-95259-4, Springer-Verlag, New York, NY.

Jiang, C., Yue, C. and Zuo, J. (2004), "On information system security architecture", *Journal of Systems Science and Information*, Vol. 2 No. 4, pp. 637-646.

Jinyan, X. and Qiang, W. (2004), "Willingness conflict of information sharing in supply chain", *Journal of Modern Management Science*, Vol. 1 No. 2, pp. 60-61.

Ketikidis, P.H., Koh, S.C.L., Dimitriadis, N., Gunasekaran, A. and Kehajova, M. (2008), "The use of information systems for logistics and supply chain management in South East Europe: current status and future direction", *Omega*, Vol. 36 No. 3, pp. 592-599.

Lee, H.L. and Whang, S. (2000), "Information sharing in a supply chain", *International Journal of Manufacturing Technology and Management*, Vol. 1 No. 1, pp. 79-93.

Lockamy, A. and McCormack, A. (2010), "Analysing risks in supply networks to facilitate outsourcing decisions", *International Journal of Production Research*, Vol. 48 No. 2, pp. 593-611.

Lockamy, A. III and McCormack, K. (2012), "Modeling supplier risks using Bayesian networks", *Industrial Management and Data Systems*, Vol. 112 No. 2, pp. 313-333.

Lumsden, K. and Mirzabeiki, V. (2008), "Determining the value of information for different partners in the supply chain", *International Journal of Physical Distribution and Logistics Management*, Vol. 38 No. 9, pp. 659-673.

Maleki, M., Shevtshenko, E. and Cruz-Machado, V. (2013), "Development of supply chain integration model through application of analytic network process and Bayesian network", *International Journal of Integrated Supply Management*, Vol. 8 Nos 1/2/3, pp. 67-89.

Mentzer, J.T., DeWitt, W., Keebler, J.S., Min, S., Nix, N.W., Smith, C.D. and Zacharia, Z.G. (2001), "Defining supply chain management", *Journal of Business Logistics*, Vol. 22 No. 2, pp. 1-25.

Morgan, M.G. and Henrion, M. (1990), *Uncertainty: A Guide to Dealing with Uncertainty in Quantitative Risk and Policy Analysis*, Cambridge University Press, Cambridge.

Niedermayer, D. (2003), "An introduction to Bayesian networks and their contemporary applications", available at: www.niedermayer.ca/papers/bayesian/bayes.html (accessed March 25, 2010).

Pai, R.R., Kallepall, V.R., Caudill, R.J. and Zhou, M. (2003), "Methods toward supply chain risk analysis", *Proceedings of the IEEE International Conference on Systems, Man and Cybernetics, Vol. 5, Washington, DC, October 5-8*, pp. 4560-4565.

Pandey, V.C., Garg, S.K. and Shankar, R. (2010), "Impact of information sharing on competitive strength of Indian manufacturing enterprises an empirical study", *Business Process Management Journal*, Vol. 16 No. 2, pp. 226-243.

Papadakis, I.S. (2006), "Financial performance of supply chains after disruptions: an event study", *Supply Chain Management: An International Journal*, Vol. 11 No. 4, pp. 25-33.

Peltier, T. (2007), *Information Security Risk Analysis*, 2nd ed., Auerbach Publications, Boca Raton, FL.

Perego, A. and Salgaro, A. (2010), "Assessing the benefits of B2B trade cycle integration: a model in the home appliances industry", *Benchmarking: International Journal*, Vol. 17 No. 4, pp. 616-631.

Pereira, J.M. (2009), "The new supply chain's frontier: information management", *International Journal of Information Management*, Vol. 29 No. 3, pp. 372-379.

Power, D. (2005), "Supply chain management integration and implementation: a literature review", *Supply Chain Management: An International Journal*, Vol. 10 No. 3, pp. 252-263.

Ritchie, B. and Brindley, C. (2000), "Disintermediation, disintegration and risk in the SME global supply chain", *Management Decision*, Vol. 38 No. 8, pp. 575-583.

Sharma, S.K. and Bhat, A. (2013), "An empirical exploration of supply chain design factors and their influence on supply chain performance", *International Journal of Business Performance and Supply Chain Modeling*, Vol. 5 No. 3, pp. 239-257.

Smith, G.E., Watson, K.J., Baker, W.H. and Pokorski, J.A. II (2007), "A critical balance: collaboration and security in the IT-enabled supply chain", *International Journal of Production Research*, Vol. 45 No. 6, pp. 2595-2613.

Spekman, R.E. and Davis, E.W. (2004), "Risky business: expanding the discussion on risk and the extended enterprise", *International Journal of Physical Distribution and Logistics Management*, Vol. 34 No. 5, pp. 414-433.

Wagner, S.M. and Bode, C. (2008), "An empirical examination of supply chain performance along several dimensions of risk", *Journal of Business Logistics*, Vol. 29 No. 1, pp. 307-325.

Wang, M., Liu, J., Wang, H., Cheung, W.K. and Xie, X. (2008), "On-demand e-supply chain integration: a multi-agent constraint-based approach", *Expert Systems with Applications*, Vol. 34 No. 6, pp. 2683-2692.

Wu, T., Blackhurst, J. and Chidambaram, V. (2006), "A model for inbound supply risk analysis", *Computers in Industry*, Vol. 57 No. 3, pp. 350-365.

Yu, Z., Yan, H. and Cheng, T.C.E. (2001), "Benefits of information sharing with supply chain partnerships", *Industrial Management and Data Systems*, Vol. 101 No. 3, pp. 114-119.

Yuan, Q. (2007), "Information sharing risk and its weakening in ASC", *Journal of Information*, Vol. 4 No. 4, pp. 89-91.

Zeng, D. and Sycara, K. (1998), "Bayesian learning in negotiation", *International Journal of Human-Computer Studies*, Vol. 48 No. 2, pp. 125-141.

Zhang, D.Y., Zeng, Y., Wang, L., Li, H. and Geng, Y. (2011), "Modeling and evaluating information leakage caused by inferences in supply chains", *Computers in Industry*, Vol. 62 No. 4, pp. 351-363.

Further reading

Cullen, S., Seddon, P.B. and Willcocks, L.P. (2005), "IT outsourcing configuration: research into defining and designing outsourcing arrangements", *The Journal of Strategic Information Systems*, Vol. 14 No. 4, pp. 357-387.

Ganguli, P. (2000), "Intellectual property rights: mothering innovations to markets", *World Patent Information*, Vol. 22 Nos 1/2, pp. 43-52.

Irani, Z., Sharif, A., Love, P.E.D. and Kahraman, C. (2002), "Applying concepts of fuzzy cognitive mapping to model: the IT/IS investment evaluation process", *International Journal of Production Economics*, Vol. 75 Nos 1/2, pp. 199-211.

Kuikka, S. and Varis, O. (1997), "Uncertainties of climatic change impacts in Finnish watersheds: a Bayesian network analysis of expert knowledge", *Boreal Environment Research*, Vol. 2, pp. 109-128.

Lee, H., Padmanabhan, V. and Whang, S. (1997), "Information distortion in a supply chain: the bullwhip effect", *Management Science*, Vol. 43 No. 4, pp. 546-558.

Li, L. (2002), "Information sharing in a supply chain with horizontal competition", *Management Science*, Vol. 48 No. 3, pp. 1196-1212.

Tang, C.S. (2006), "Perspectives in supply chain risk management", *International Journal of Production Economics*, Vol. 103 No. 2, pp. 451-488.

Yuan, Q., Xiaokang, Z. and Qiong, Z. (2007), "Research on finance optimization in supply chain", *Proceedings of the 4th International Conference on Innovation and Management, (I)*, pp. 1084-1091.

Corresponding author

Satyendra Sharma can be contacted at: satyendra.sharma1979@gmail.com

This article has been cited by:

1. Md Abul Kalam Azad. 2016. Predicting mobile banking adoption in Bangladesh: a neural network approach. *Transnational Corporations Review* **8**:3, 207-214. [CrossRef]