

Information Security Issues In Global Supply Chain

Topic Area: Risks management issues in global supply chains.

Authors:

Anand S. Kunnathur

College of Business Administration
University of Toledo,
2801 W. Bancroft Street,
Mail Stop 103
Toledo, Ohio – 43607 - 3390. USA.
Phone: 419.530.5644
Fax: 419.530.7744.
akunnat@utnet.utoledo.edu

Sridhar Vaithianathan

ICFAI Institute for Management Teachers,
Survey No. 156/157, Dontapally Village,
Shankarpally Mandal, Ranga Reddy District,
Hyderabad – 501 203. Andhra Pradesh, India.
Tele-Fax: +91-8417-236671
Mobile: 99899 04245
sridhar_we@yahoo.com

&

Further Contact, Kindly Correspond to:

Anand S. Kunnathur

College of Business Administration
University of Toledo,
2801 W. Bancroft Street,
Mail Stop 103
Toledo, Ohio – 43607 - 3390. USA.
Phone: 419.530.5644
Fax: 419.530.7744.
akunnat@utnet.utoledo.edu

Affidavit

This is to confirm that the paper contains original work of the authors. The paper has not been earlier published or has not been sent for publication elsewhere, and all copyright requirements in respect of material used directly or indirectly in the paper have been duly met. The authors are responsible for the views expressed and material used in their papers.

Information Security Issues In Global Supply Chain

ABSTRACT

The control of information flow and their security are of great importance to organizations participating in the global supply chain. Significant gap exists in the research literature on supply chain information security (SCIS). Based on literature review, the paper suggests a framework highlighting the issues that demands attention for securing inter-organizational information flows in the global supply chain management (GSCM). The paper also suggests future research direction.

Keywords: Information Security, Global Supply Chain Management, Inter-organizational information flow, Supply Chain Information Security.

EXECUTIVE SUMMARY

Whilst there have been isolated calls in the literature stressing the importance of information security issues in managing the supply chain effectively, the supply chain information security (SCIS) issues have neither been discussed in detail nor received its attention due. In this paper we suggest a framework to bring out the issues enfolding SCIS. The framework captures the main facets that demands attention. The issues are mainly 1) infrastructural issues, 2) strategy development parameters and issues, 3) local protocols issues, 4) emerging technologies impacting the flow of information in the supply chain, and 5) power and control issues in inter-organizational systems.

Infrastructural issues mainly deals with the organization structure, technology competence and training, organization learning and relationship with partners. Strategy development parameters and issues underline the need for well thought out strategy for securing information flow between organizations. Local protocol issues points out that accounting practices, culture issues might well eliminate or exacerbate security breaches. Emerging technologies like Blackberry, wireless enabled PDAs, ad-hoc networks, and RFIDs might introduce wide variation in both standards and infrastructure across organizations in the supply chain. This mandates the need for development of a SCIS strategy that includes the securing of information handled and flowing through emerging technologies. Power and control issues lay emphasis on different perspectives that might arise from different stakeholders in terms of who should control the security and underscores the importance of relationship management within the supply chain. The study might well serve as a starting point for future research paths in SCIS and tries to imbibe in the minds of practitioners and researchers alike to have a critical look in to the information security issues and fix the issues before it affects the firms' bottom line.

Information Security Issues In Global Supply Chain

INTRODUCTION

Supply Chain Management (SCM) refers to the practices and processes aiming for effective and efficient flow of materials and information between a company and its immediate suppliers and customers. Strategic, logistical, and other operational issues in managing the supply chain have received a lot of attention from researchers. However, little attention appears to have been paid to ensuring the security of information flows in the global supply chain management (GSCM). Security of the information flows is not only a necessity for ensuring smooth operation of the supply chain, but also for preserving relationships and for maintaining a competitive strategic posture. The weakest link, as the cliché goes, defines the chain. In trans-border, multinational environments, there are many links in the chain and not all of the same level of security. In the present era of information technology enabled supply chain, information is vital to the success of the business and will be accountable for a significant share of the business's various indicators of success, including its cash flow and market value.

The process of shipping goods around the world is long and complex (Schary and Skjott-Larsen, 2001). Many managers are still unsure of necessary actions in light of the new challenges to enhance their logistics security programs (La Londe, 2002). To address the security concerns of manufacturers and transportation companies without compromising supply chain efficiency, the US Customs office launched several initiatives, including the Customs-Trade Partnership Against Terrorism (C-TPAT), Container Security Initiative (CSI), the 24-hour rule, Operation

Safe Commerce (OSC), Smart and Secure Trade Lane (SST), and Partners in Protection (PIP). These security programs involve all parties in supply chains, including foreign governments, to ensure border security. Though these programs are welcome measures to enhance security of the movement of goods, but it does ignore the information security (IS) issues, which is more vulnerable than the former.

Prior to 1980s, companies made tradeoffs between quality and cost with the belief that quality can only be achieved at the expense of the cost. However, since 1980s, many companies have found that better quality can lead to lower defects and failure costs, higher customer satisfaction, more sales, and higher profits. Manufacturers learned to focus on “prevention” and took a total quality management approach by working closely with suppliers and customers to improve quality. A similar mindset exists regarding information security issues. Managers are holding a passive attitude toward information security mechanisms contemplating that security of information flows involve forgoing part of firm’s profitability.

Companies such as Dell and Whirlpool are sharing information with suppliers and customers to decrease costs and improve customer service. The flow of information through their supply chains enables them to match supply closely to consumer demand and to anticipate changes in the marketplace. In fact, the justification for the growth of inter organizational information systems (e.g., electronic data interchange (EDI), enterprise resource planning (ERP), supply-chain applications, and e-market places) is based on the growing awareness that leveraging information can be beneficial to all parties involved.

On the flip side, ‘Information security continues to be ignored by top managers, middle managers, and employees alike. The result of this unfortunate neglect is that organizational

systems are far less secure than they might otherwise be and that security breaches are far more frequent and damaging than is necessary'. In summary, whilst there have been isolated calls in the literature stressing the importance of IS issues in managing the supply chain effectively, the information security issues have neither been discussed in detail nor received its attention due. In this paper we try to bring out the issues enfolding security of information flow between the firms and across the supply chain partners. The paper proposes a framework comprising the issues that need to be addressed in terms of enhancing information security in SCM.

LITERATURE SURVEY

The literature surveyed in this paper highlights many relevant issues pertaining to importance of information flow/sharing and securing information flows/shared information in the supply chain. Some of the ideas and issues obtained from the literature are outlined below.

Doherty and Fulford (2006) argue that the organizations' should have information security policy and strategic information system plan in place to operate in secure manner and to effectively deploy new information systems to meet organization's strategic objectives respectively. Lia et al., (2006) classifies three levels of information sharing between organizations – 1. exchanging transactional information such as order quantities, prices, 2. sharing operational information such as inventory levels, costs and schedules, and 3. sharing strategic information like point-of-sale information, real time demand. Further, it suggests that in both electronic markets and electronic hierarchies require effective sharing of information across organizations in order to reduce transaction costs, inventory costs, and serve their customer better. Kritzinger and Smith (2008) proposes Information Security Retrieval and Awareness (ISRA) model that can be used by industry to enhance information security awareness among employees. The model focuses more

on non-technical information security issues more than technical issues stressing that equivalent weight should be given to non-technical issues involving people to secure information flow. Study by Fawcett et al., (2007) found that an organization's technological connectivity together with its cultural willingness to share determine how much useful information will be shared to help the company and the supply chain to succeed. Karkkainen et al., (2007) by employing case study data from 16 Finnish companies proposed three categories - (1) transaction processing; (2) supply chain planning and collaboration; and (3) order tracking and delivery coordination - of inter-firm IS use. Findings represent well the actual purposes for which interfirm IS are used by the companies in the management of supply chain activities.

Information system technologies aid firms across the world to enhance information sharing across the firms or between supply chain partners or across the supply chain. Lee et al., (2000) and Raghunathan (2001) have found that the sharing of demand information in supply chains typically increases the performance of the supply chain by increasing availability and reducing inventory related costs. Today, companies are increasingly seen as parts of multi-company, multi-echelon networks, i.e. supply chains, delivering goods and services to the final customer (Christopher, 2005). The existing literature on supply chain management (SCM) is extensive (Mentzer et al., 2001; Tan, 2001) and proposes that integrated control of these multi-company networks can provide significant benefits (Norek and Pohlen, 2001). The utilization of information systems (IS), in turn, is considered an essential requirement for managing these networks, and has been associated with significant improvements in supply chain efficiency (White and Pearson, 2001). Also it is crucial that information needs to be managed before a sale is made, while satisfying the sales order, during after-sales maintenance, responding to customer demand, so on and so forth. Further, to achieve overall customer satisfaction, proper

management of both the goods movement and information flow throughout the supply chain is necessary.

Coffee (2004) has indicated that securing information flows has become more difficult because of the emergence of web-based communications, the Internet, wireless networks, etc. Those conclusions are also supported by an Entrust white paper, published in 2004, which adds that with the openness of e-business comes the reality of information exposure and risk. With some organizations creating extranets for vendors, suppliers, and preferred customers to tie their networks together, companies are realizing the importance of information security. In order to secure data that is dispersed across a diverse environment, a solution needs to be scalable, yet comprehensive enough to deliver authentication, access control, encryption and digital signatures- that enable accountability and privacy (Entrust, 2004). Other security considerations involve the general openness of the web environment, remote access, and mobile data devices. Studies (Fulford and Doherty, 2003; Dhillon and Backhouse, 2001; and Hong et al., 2006) have also stressed the importance of information security mechanism(ISM) and further need for information security policies (ISP) to effectively tackle the information security issues in SCM. Hale et al., (2004) propose that “Information security is now a critical component of long-term company performance and should be directed strategically by top management.” The study defines the relationship between information and data security breaches, which are also applicable to the supply chain. It discusses as to how organizations should respond to information security threats. The authors observe that organizations must value their information assets, assess threats, and then evaluate the costs of securing those assets. “When companies are forced to take a reactive, ad hoc approach to information security rather than a proactive, strategic one, information remains vulnerable. Even more alarming is that critical information

may be attacked, accessed, copied, altered, or stolen without a company's knowledge.” It can be very dangerous for a company to only rely on a reactive strategy when dealing with information security issues, especially when the company may not even know what type of information breach has occurred. The implications for this in the context of the global supply chain are that it might be difficult for a company to determine where and when the information breach occurred if they don't have a comprehensive information security system in place.

Wagner (2003) considers that web security standards will face a long road to maturity as web services become more complex and involve interactions between multiple parties. Users will begin to require more versatile security. “Unfortunately, the progress towards establishing a set of web security standards that work together is being slowed by political battles between suppliers.” From the perspective of general strategy formulation, the supply chain must deal with disruptions of all types and there is a strong need for a business continuity plan with contingency planning, especially to maintain the efficiency of the supply chains (Reddy, 2004). This idea leads directly into the main topic of information flows. Information flow is critical to the efficiency of the entire supply chain. “Such information visibility requires at least two things: (1) event-driven data on supply chain operations, including security chain-of-custody information and (2) a tight integration of information systems across suppliers, manufacturers, logistics providers, and customers”(Lee et al., 2003). Murtaza et al., (2004) look at the major information security concerns of an online e-marketplace supply chain that include: confidentiality, industry-wide standards, and integration of the company's system with the e-marketplace. A few of the authors introduced information security issues raised with the new Radio Frequency Identification (RFID) technology. For example, “Information can be written to the devices at any point in the supply chain and the chips can transmit data to servers automatically”, asserts

Barry (2005). The RFID technology is also vulnerable when it is stored on the chip itself and also when it is written to, or read from the chip (Willoughby, 2004). A related information security topic concerns the data management issues associated with RFID technology in the supply chain and the subsequent increase in volume of data for the company (Angeles, 2005). The volume of data inflows needs to be addressed to ensure security of the information. A possible solution to the data volume management issue comes from companies that are searching for better ways to share and manage large amounts of data – example data grids. Forward-thinkers imagine data grid systems that connect large numbers of enterprises, entire supply chains, and customer bases in order to manage large amounts of information effectively (Thibodeau, 2004). The data management and volume management concerns relate to possible infrastructural issues with the increase in RFID data, and securing large amounts of information could be very challenging in the global supply chain. The general ideas, in Lee and Wolfe (2003), are that e-marketplaces are still in the early stages of their development life cycle. E-marketplaces are creating more complex supply chains that are requiring more complex information and data security across the chain. Securing information across the global supply chain is uncharted territory, but the need for it is gaining momentum and as more literature on the topic is coming to the forefront, organizations will be better able to understand the issues in protecting their information effectively.

Interorganizational information flows are a direct consequence of the ubiquitous use of the Internet and its communication protocols and the explosive growth in business to business (B2B) E-commerce. Clearly there is a significant gap in the research literature on inter-organizational information security. Given the current scenario where Information flows across a supply chain are far more distributed and less controllable by one organization. Power and control issues, local

mores, ethics, accounting practices, financial service rules, currency and stock markets, governmental control, privacy legislation, emergence of new information technology tools etc. are all likely to influence the supply chain. These and other parameters add many layers of complexity to the management of information flows in the trans-border supply chains of today, which are only likely to expand in the era of virtual organizations already on the horizon. The research literature does not appear to have dealt with the underlying area of inter-organizational information flows and the issues that drive the management of such flows, leave alone deal with the component issue of security in the context of inter-organizational information flows.

OBJECTIVE

It is clear from the literature survey, scant attention paid to issues relating to security of information flow between organizations, especially in the management of supply chain information security, at the corporate level. There is clearly a need for developing the procedures and protocols for establishing a strategy to secure information in the supply chain, which includes other organizations as well.

The main objective of the paper is to highlight the issues that demands attention for securing inter-organizational information flows in the global supply chain management (GSCM). A framework is suggested for the supply chain information security (SCIS) which emphasize the information security issues and concerns that needs to be understood in sharing information with its supply chain partners. The rest of the paper is structured as follows, in the next section framework for SCIS is presented, followed by the explanation of the same. Research issues and opportunities for future research, contributions of the study, its limitation are presented in the last section.

FRAMEWORK FOR SUPPLY CHAIN INFORMATION SECURITY (SCIS)

Broadly the SCIS in inter-organizational set-up can be classified into five main themes which form the framework. Figure 1 represents the framework. The framework captures the main facets that demands attention. The issues are mainly

1. infrastructural issues,
2. strategy development parameters and issues,
3. local protocols issues,
4. emerging technologies impacting the flow of information in the supply chain, and
5. power and control issues in inter-organizational systems.

{Figure 1 around here}

Infrastructural issues mainly deals with the organization structure, technology competence and training, organization learning and relationship with partners. Strategy development parameters and issues underline the need for well thought out strategy for securing information flow between organizations. Local protocol issues points out that accounting practices, culture issues might well eliminate or exacerbate security breaches. Emerging technologies like Blackberry, wireless enabled PDAs, ad-hoc networks, and RFIDs might introduce wide variation in both standards and infrastructure across organizations in the supply chain. This mandates the need for development of a SCIS strategy that includes the securing of information handled and flowing through emerging technologies. Power and control issues lay emphasis on different perspectives that might arise from different stakeholders in terms of who should control the security and underscores the importance of relationship management within the supply chain.

Next section discusses one by one, the issues related to information flows across corporate boundaries and its impact on information security, security of “transshipment” points of both data and materials, and security of accounting and financial transactions.

INFRASTRUCTURAL ISSUES

The supply chains of today are typically multi-organizational and across different countries. Even with a single organization involved in the area of information security, the infrastructure of the organization would be an issue in the securing of information. Not that this area is all that well studied in the research literature, it is more an imperative to study infrastructural issues in SCIS in the multi-organizational setting, on account of the stakes involved and the potential for massive disruptions spanning multiple organizations, and even nations.

{Figure 2 around here}

One aspect of infrastructure likely to affect SCIS in the multi-organizational context is the type of organizational structure that is to be found in the organizations across the supply chain. Hierarchical structures would appear to lend themselves more easily to control and, hence, security of information flows through the chain. The trend in most industrialized nations is, however, to have more of a matrix organization and even a flat organization, thus placing a premium on effective communication across the structural span. However, it is unlikely that organizational participants in the supply chain have similar organizational structures, let alone the same structure. Also, the level of technological sophistication and the ability to deal with disruptions and security breaches are likely to be all over the spectrum.

The flexibility of an organization, the learning orientation and responsiveness of its workforce to information flow disruptions in the supply chain are likely to be significant contributors to the

reliability and smooth functioning of the supply chain. The presence or absence of well-established communications protocols within the supply chain to handle information flow disruption would, surely, impact the supply chain's functioning. The human aspect is very critical in the securing of information flows.

Humans are likely to be the most important on both sides of this equation; namely, they are likely the perpetrators of SCIS violations and they have to be the ones to prevent it and/or fix these problems. The level of sophistication and trustworthiness and training required by organizations, in the supply chain, of their information processing employees, and their technical competence would all play a role in securing the information flows in the supply chain. Further, given the collective nature of the job of securing the information flows across organizational and national boundaries, well established mechanisms must be developed for information sharing across organizations in the supply chain and for promoting inter-organizational learning.

STRATEGY DEVELOPMENT ISSUES

It is questionable whether there exists a well thought out strategy for securing information flows even in a single organization setting. Often the operational practices put in place by the Information Technology infrastructure passes for "strategy" in this regard. Such a practice in the world of the global supply chain in securing information flows is not only bound to fail but also is likely to prove very perilous for ensuring the safety of both information and materials flowing through the supply chain. **{Figure 3 around here}**

We are talking about the need, here, for the formulation of a well thought out, multi-organizational, multilateral strategy for securing information flows in the global supply chain. One aspect of this area of strategy development is likely to be the development of a process for

diversifying SCIS strategy across the chain and bridge the gaps that would exist between and among the individual organization strategies, when set up, and the multilateral strategy needed.

This multilateralism is likely to evoke the specter of power and control in the supply chain. It would then become necessary, as part of the process of protocol development, to deal with power and control issues in an acceptable way for the sake of the larger good of the chain as a whole. This is likely to be a thorny problem, requiring much tact and diplomacy on the part of the leadership of the organizations in the supply chain, especially those, organizations and personnel that are considered the most influential.

One factor affecting the development and implementation of a strategy for SCIS would likely be finances. It is very unlikely that the financial burden of securing the information in the chain will be equally shared by all parties in the chain irrespective of their size, ability to pay, and gain from the extent of use of the information. Also, procedural and infrastructural individualities related to organization structure, cultural setting, governmental regulations, infrastructure, and size will all likely shape and mold SCIS strategy.

LOCAL PROTOCOL ISSUES

Study of information flow security in a trans-border, multi-organizational supply chain is a necessity stemming directly from the scope of such chains and the opportunities for its disruption based on a variety of factors. One such factor would be the protocols and practices local to the organization in its setting, typically abroad. **{Figure 4 around here}**

We have already alluded to the need for inclusion of financial aspects in SCIS strategy formulation. The financial practices that are local to the organization setting, in terms of expected ROI, cash flow requirements, debt service and ability to incur debt etc. will all play a role in determining both the operation and management of the information flows in the chain. Additionally, accounting standards differ widely across the world. Short of imposing a common, US like, FASB orchestrated standard, awareness and accommodation of the diversity of accounting practices becomes an imperative for securing, especially financial, information in the chain. In addition, there has to be responsiveness, in the SCIS strategy, to legislative mandates, such as Sarbanes-Oxley, in ensuring compliance at least in the countries with such legislative priorities.

Local cultural practices may eliminate or exacerbate security breaches. To an extent, the practice and management of information security is based on a trust no one attitude, which is likely to clash with the accepted cultural norms in some environments. Similarly, some locations in the chain are far more likely to be physically more secure than others. Clearly, physical security of information assets is a first step in ensuring overall SCIS. Since there are significant cost and capacity overheads that attend on practices such as encryption, the level of security through the chain is unlikely to be uniform and of a suitably high level. The challenge then will be to develop not only acceptable practices, but also to develop a strategy that is sensitive to local issues in ensuring that the weakest link does not end up compromising SCIS across the chain. The infrastructure, especially with regard to data communications, around the world and in different business organizations is far from uniform. Add to this the prevalence of ancient laws and modern regulations, and what we have is the making of a nightmare scenario of having

communication barriers within the chain for the sake of shoring up one or more weak links in the area of SCIS.

EMERGING TECHNOLOGIES ISSUES

The emergence of new wireless networking technologies such as Blackberry, wireless enabled PDAs, ad-hoc networks, and RFIDs has introduced a new twist into the dialog on information security that is becoming more urgent by the day. The frustrating aspect of dealing with securing these technologies is likely to be the wide variation in both standards and infrastructure across organizations in the supply chain. RFID technology, hailed as the next best thing to sliced bread, has been embraced with open arms without regard to the infrastructure needed to make information flows in this context secure. RFID tags are not tamper proof. Also, they can be removed and replaced by mischief minded hackers. Encryption would only partially prevent sabotage of RFID based information flows. **{Figure 5 around here}**

In this environment of rapidly changing technologies and expectations, it may be necessary to layer security systems and allow for layered handling of data and information in a secure fashion appropriate to the information being handled. The greatest challenge is likely to be the necessity to have all participants in the handling of information flows in the supply chain to have an acceptable level of security in the use of emerging technologies in the supply chain, even if they are not using them, as yet. This mandates the need for development of a SCIS strategy that includes the securing of information handled and flowing through emerging technologies.

POWER AND CONTROL ISSUES

Smooth functioning of a supply chain, and especially one that spans multiple organizations across national and cultural boundaries, is predicated on successful relationship management

within the chain. While individual organizations may emerge as leaders in the management of the supply chain, coercive practices are unlikely to work effectively in this environment. Securing information handling, and information flows, in this environment is but a piece of the overall relationship management puzzle, albeit a very important one. It is only now that researchers are beginning to turn towards relationship management issues in B2B E-commerce and, tangentially, the supply chain (Li et al., 2004). It is not clear that ones who control the relationship will or should automatically control SCIS. In the perspective of power and control of the supply chain relationships, SCIS would appear to play a role in the determination of the overall strategic posture to be adopted by organizations, individually and collectively, in managing the supply chain. It has to be that organizations, especially large and used to getting their way, have to become more flexible in the collaborative that is the supply chain, so as not to win many battles only to lose the war. **{Figure 6 around here}**

It is arguable whether the same parameters would attend relationship management irrespective of organization size and contribution to the chain. Further, given the diversity of locations and protocols, not to speak of legislation and legislative priorities, it is even more unlikely that one size would fit all, in terms of establishing either guidelines or checklists for successful relationship management and, hence, SCIS management.

There are many relationship layers within the supply chain. The issues that impact supplier-to-supplier relationships and SCIS management are likely to be different from those that impact vendor-supplier and vendor-vendor relationships. Infrastructural capabilities in these relationships are likely to be significantly skewed in favor of large vendors as opposed to small suppliers and, yet, the success of SCIS management is likely to depend on how well the skewed relationships are managed. It may be necessary to educate, on a continuing basis, the smaller,

seemingly less significant, players in the chain to the pitfalls of lax security along with the procedures, and the necessity there for, to avoid security compromises.

Again, the security system is going to be only as strong as the weakest link, and the mindset of the bigger players has to change to accommodate this reality to ensure smooth functioning of the supply chain.

CONCLUSIONS

Current information security trends include increase in the percentage of information security budgets among companies and a decrease in the records lost or damaged among companies. These trends show promise that securing information flows from a generic organizational perspective are gaining more attention from companies. Further, Compliance with regulations and standards is a concern that every organization must deal with and also whether or not the other members of the supply chain are adhering to them as well. Some examples of information security regulations for organizations to familiarize themselves with are: Sarbanes-Oxley, the Gramm-Leach Bliley Act, the European Data Privacy Directive, and the Basel II accord.

Though securing information flow in inter-organizational setup is gaining its importance, but the issues that demands attention for smooth flow of information among supply-chain partners has not been given its importance due. This paper tries to draw attention to information security issues that needs to be sorted out in the same context and suggest a framework for the same. Though there were isolated calls in SCM literature about the importance of secure information among supply chain members, we believe neither the issues related with it are discussed in wholesome way keeping the entire stakeholder in mind nor there exist any framework hinting the range of issues that needs serious consideration. By understanding the importance issues

associated with secure information flow in inter-organizational set-up, organizations could take informed decisions about analyzing the existing status of their information system and to improve on the same to avoid costly disruptions that may occur due to information security breach.

CONTRIBUTIONS

The main purpose of the paper is to bring into light the importance of secure information flow between organizations in global supply chain management and the issues that needs genuine attention mainly to avoid security infringement. The control of information flow and their security are of great importance to organizations participating in the global supply chain. Compromise of Information security puts off the functioning of the global supply chain. The abuse of the e-commerce interface for unauthorized access to sensitive organizational information is a primary security concern. In a global e-commerce environment with multiple organizations, intermediaries, and nations involved, information security is more critical. The stakes are high in having to maintain smooth flow of goods and services. Massive and costly disruptions can occur if information processing and information flows are compromised, especially due to security breaches.

Existing literature has stressed and has well recognized the importance of securing information within an organizational setting. However, information security in the context of securing critical information flows between and among organizations has received no attention and in particular; information security in the supply chain has received scant attention. To fill the gap, the study proposed a framework to include issues that need to be considered in dealing with information security issues in trans-border flow of data and supply chain partners. The study might well serve

as a starting point for future research paths in SCIS and tries to imbibe in the minds of practitioners and researchers alike to have a critical look in to the information security issues and fix the issues before it affects the firms' bottom line.

MANAGERIAL IMPLICATIONS

The framework suggested in this paper has several managerial implications. First Issues involved in ensuring secure information flow among the supply chain partners are complex and to reach a decent solution, the stakeholders concerned should establish well thought out standards, procedures and policies. Also the organizations should show commitment and adhere strictly to the documented principles to avoid security breaches of any kind. Second, it might not be possible to concentrate on several issues at the same time, since priority of issues to be dealt with might vary between and among supply chain partners. Hence it is necessary to bring the organizations concerned under common umbrella to prioritize issues to be tackled and act accordingly.

LIMITATIONS

The main limitation of the study is that, it is conceptual and needs either empirical or case study validation. Since the topic involves study on multiple organizations, involving multiple organization setting, culture and even different nations; hence data collection was difficult and could not be validated. Also due to the emergent nature of the phenomenon of SCIS and the issues encompassing it, implementation issues were not discussed much. Further, there could be some more issues that we have overlooked in terms of SCIS. Also it is possible that of all the issues that have been put forth in the paper, some of the issues might be more important and critical than the others, which we haven't taken into consideration or probably, could be analyzed

in further studies. Nevertheless the issues discussed in the study are of practical importance and needs genuine attention sooner or later before it blows out of proportion.

FUTURE RESEARCH

It is evident from even a cursory glance at the content of the previous sections that a vast array of unexplored researched areas exists on the topic of SCIS. Some of it, clearly, has to be dealt in tandem with the generic areas such as relationship management and some with the trans-border data flow areas. The typical research methodologies on business practices await business developments and are post-facto. What is needed, immediately, is fact-finding type of research that leads to the development of a conceptual model encompassing all aspects of the SCIS spectrum. This perspective leads us to suggest, chronologically, the following research steps in answering some of the salient research questions framed thus far in the article.

Develop case studies to identify examples illustrating the issues highlighted and organizational response, if any. Specifically, a) to examine the workings of global supply chains with a focus on identifying presence and absence of SCIS practices. Document consequences of action, inaction, and misaction, b) identify, in a case study setting, relationship management issues that impact SCIS, c) identify, through case studies, the security practices and security breaches in the handling of information flows by intermediate trans-shipment points on the Internet used by supply chains, d) identify, through case studies, the procedures or the lack thereof, in the area of strategy formulation, aimed at SCIS, e) identify trans-border parameters of impact in different supply chain environments, through case studies.

Also, case studies/field studies could be developed to identify infrastructure capabilities and limitations in handling security issues in inter-organizational information systems in the supply

chain. In particular, studies dealing with issues involving a) identification of multi-organizational data base security issues and responses, b) security of data communications in the supply chain across organizations, c) development of protocols and procedures for identification of and the upgrading of the weakest link in the inter-organizational supply chain, d) training and retraining of personnel dealing with the multi-organizational information and material flows, and e) organizational learning issues and development of monitoring mechanisms for securing information flows in the supply chain.

REFERENCES

Angeles, R, 2005, 'RFID Technologies: Supply-Chain Applications and Implementation Issues', *Information Systems Management*, pp 51 - 64

Barry, C, 2005, 'RFID tracks packages, 'speaks' to consumers: smart packages not only improve supply chain management- they ensure product security, authentication' *Emerging Technology*, Nov 18, http://www.findarticles.com/p/articles/mi_m0UQX/is_11_65/ai_812 Last accessed on: Dec 24, 2007.

Christopher, M, 2005, *Logistics & Supply Chain Management – Creating Value Adding Networks, 3rd ed.*, Harlow, Pearson Education Limited.

Coffee, P, 2004, 'Security is a moving target', *eWeek*, Vol. 21, No 50, Dec, pp D1- 4.

Dhillon, G, and Backhouse, J, 2001, 'Current directions in IS security research: towards socio-organizational perspectives', *Information Systems Journal*, Vol. 11, pp. 127-53.

Doherty, N.F. and Fulford, H, 2006, Aligning the information security policy with the strategic information systems plan', *Computers & Security*, Vol 25 , pp 55 – 63.

Entrust (Whitepaper), 2004, 'Protecting Your Most Important Asset: Information – How Data Security Mitigates Risk and Enables Compliance', *Entrust Publication*, September 10, <http://www.entrust.com>. Last accessed on: Jan 14, 2007.

Fawcett, S. E., Osterhaus, P., Magnan, G. M., Brau, J. C., and McCarter, M. W. 2007, 'Information sharing and supply chain performance: the role of connectivity and willingness.' *Supply Chain Management: An International Journal*, Vol 12, No 5, pp. 358–368.

Fulford, H. and Doherty, N.F, 2003, 'The application of information security policies in large UK-based organizations: an exploratory investigation', *Information Management & Computer Security*, Vol. 11 No. 3, pp. 106-14.

Hale, John C, Landry, Timothy D, and Wood, Charles M, 2004, 'Susceptibility audits: A tool for safeguarding information assets', *Business Horizons*, Vol. 47, No 3, May/Jun pp 59 – 66.

Hong, K, Chi, Y, Chao, Louis R. and Tang, J, 2006, 'An empirical study of information security policy on information security elevation in Taiwan', *Information Management & Computer Security*, Vol 14, No 2, pp 104-115.

Karkkainen, M., Laukkanen, S., Sarpola, S., and Kamppainen, K, 2007, 'Roles of interfirm information systems in supply chain management, *International Journal of Physical Distribution & Logistics Management* Vol. 37 No. 4, pp. 264-286.

- Kritzinger, E. and Smith, E, 2008, 'Information security management: An information security retrieval and awareness model for industry.' *Computers & Security*, Vol. 27, No 5/6, pp 224-231.
- La Londe, B.J, 2002, 'Security: the shipper speaks: results of a new survey show agreement and disagreement over security, point to an opportunity for business to assume a leadership role', *Supply Chain Management Review*, Vol. 6 , No. 6, pp. 9-12.
- Lee, H., So, K.C. and Tang, C.S, 2000, 'The value of information sharing in a two-level supply chain', *Management Science*, Vol 46 No 5, pp 626-43.
- Lee, Hau L, and Wolfe, M, 2003, 'Supply Chain Security without Tears', *Supply Chain Management Review*, Vol. 7, No 1, Jan/Feb pp 12 - 21
- Li, X, Kunnathur, Anand S, and Ragu-Nathan, T.S, and Jitpaiboon, T, 2004, 'Learning Capability, Supportive Leadership and Power in IOS Context,' Proceedings of the *National DSI Conference*, Boston (2004)
- Lia, J., Sikorab, R., Shawa, M. J. and Tanc, G.W, 2006, *A strategic analysis of inter organizational information sharing*, *Decision Support Systems*, Vol 42, pp. 251– 266.
- Mentzer, J.T, DeWitt, W. and Keebler, J.S, 2001, 'Defining supply chain management', *Journal of Business Logistics*, Vol 22 No 2, pp 1-25.
- Murtaza, Mirza B, Gupta, V, and Carroll, Richard C, 2004, 'E-marketplaces and the future of supply chain management: opportunities and challenges', *Business Process Management Journal*, Vol. 10, No. 3, pp 325-335

Norek, C.D, and Pohlen, T.L, 2001, 'Cost knowledge: a foundation for improving supply chain relationships', *International Journal of Logistics Management*, Vol 12, No 1, pp 37-51.

Raghunathan, S, 2001, 'Information sharing in a supply chain: a note on its value when demand is nonstationary', *Management Science*, Vol 47, No 4, pp 605-10.

Reddy, R, 2004, 'Without Safety Nets: Will Super-efficient supply chains take one beating and fail to keep on ticking?', *Intelligent Enterprise*, Nov 14, <http://www.intelligenteai.com/showArticle.jhtml?articleID=51201670>. Last accessed on: Sep 24, 2007.

Schary, P.B, and Skjott-Larsen, T, 2001, *Managing the Global Supply Chain, 2nd ed.*, Denmark, Copenhagen Business School Press.

Tan, K.C, 2001, 'A framework of supply chain management literature', *European Journal of Purchasing & Supply Management*, Vol 7, No 1, pp 39-48.

Thibodeau, P, 2004, 'Data finds a place on the grid', *Computer World*, Vol.38, No 14

Wagner, R, 2003, 'Secure the incompatible' *Computer Weekly*, Jan 19, Article Quicklink #00104. Last Accessed on: Jun 21, 2005

White, R. and Pearson, J, 2001, 'JIT, system integration and customer service', *International Journal of Physical Distribution & Logistics Management*, Vol 31, No 5, pp 313-33.

Willoughby, M, 2004, 'Securing RFID Information: Industry standards are being strengthened to protect information stored on RFID chips' *Computer World*, December.

APPENDICES – LIST OF FIGURES TO BE INCLUDED IN THE TEXT.

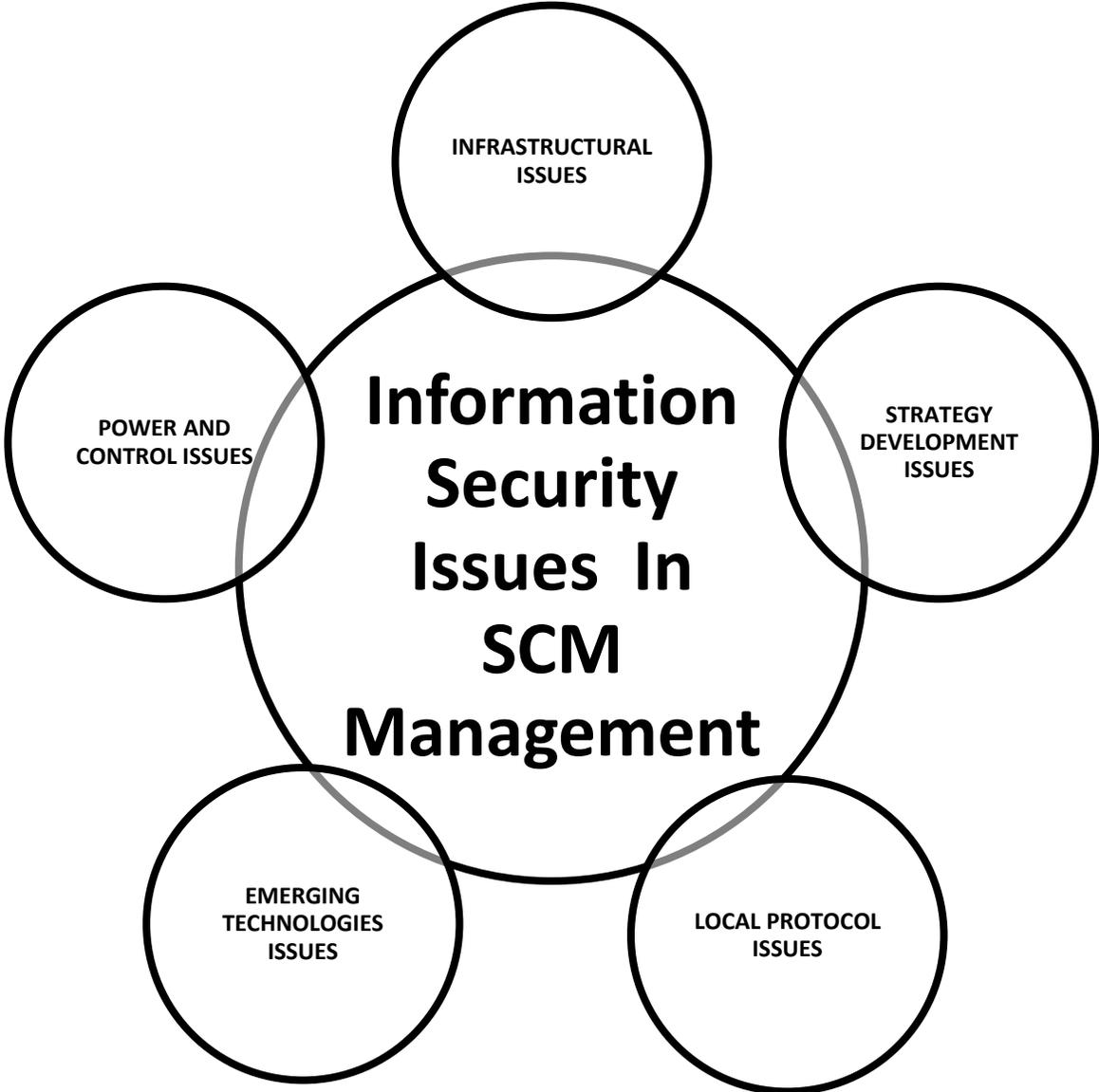


Figure 1: Framework for Information security issues in GSCM



Figure 2: Infrastructural Issues



Figure 3: Strategy Development Issues

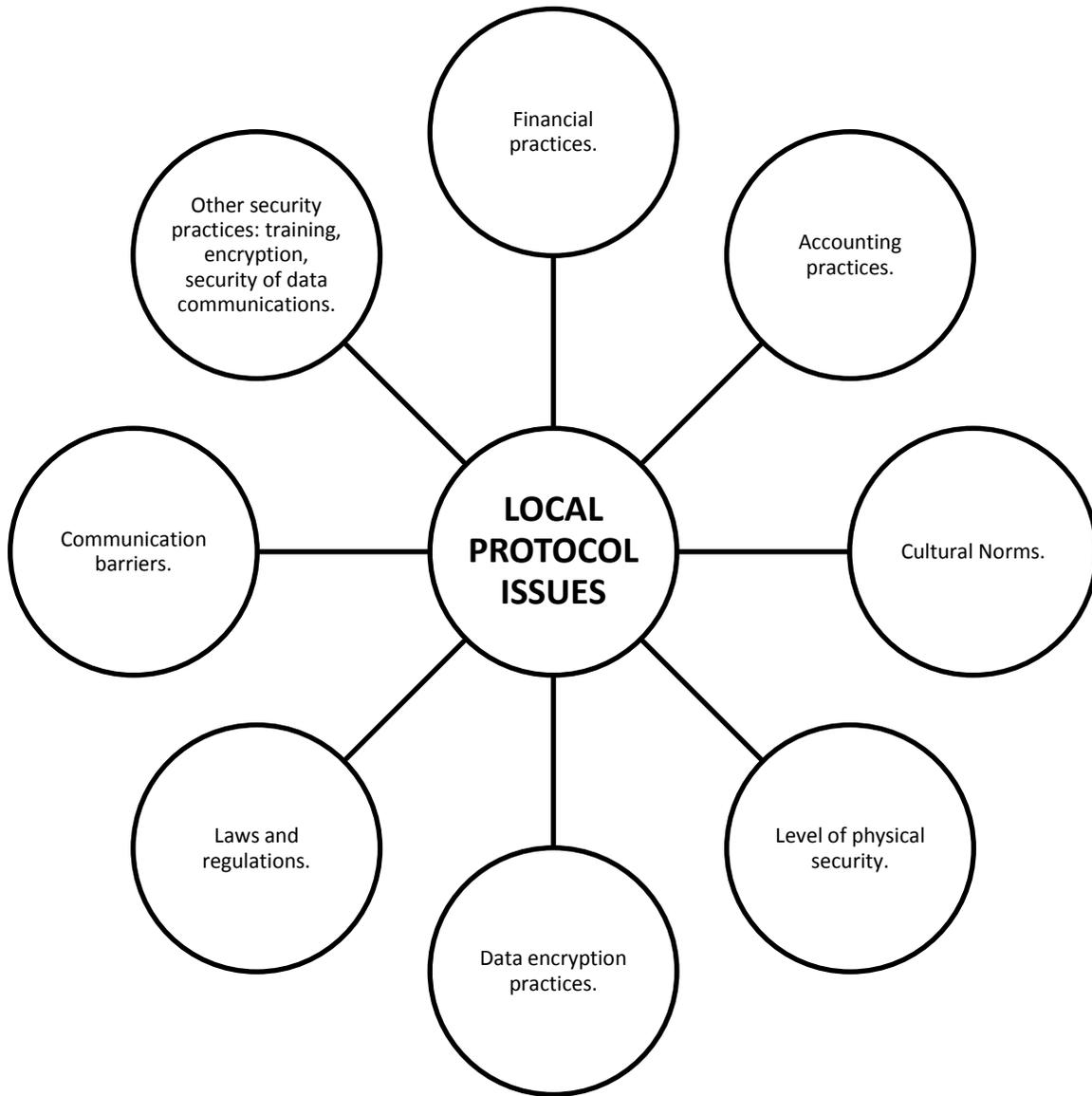


Figure 4: Local Protocol Issues

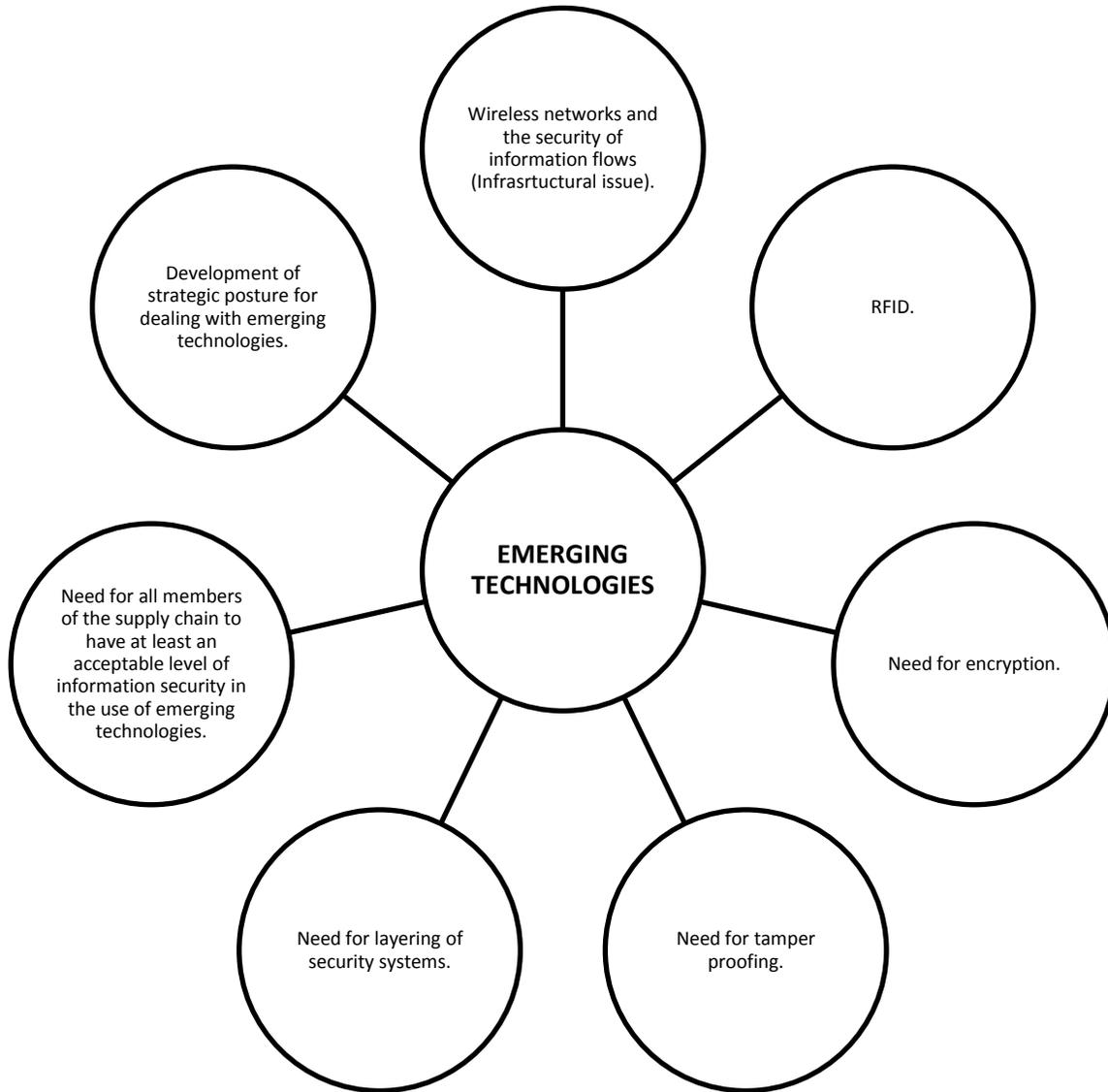


Figure 5: Emerging Technologies Issues

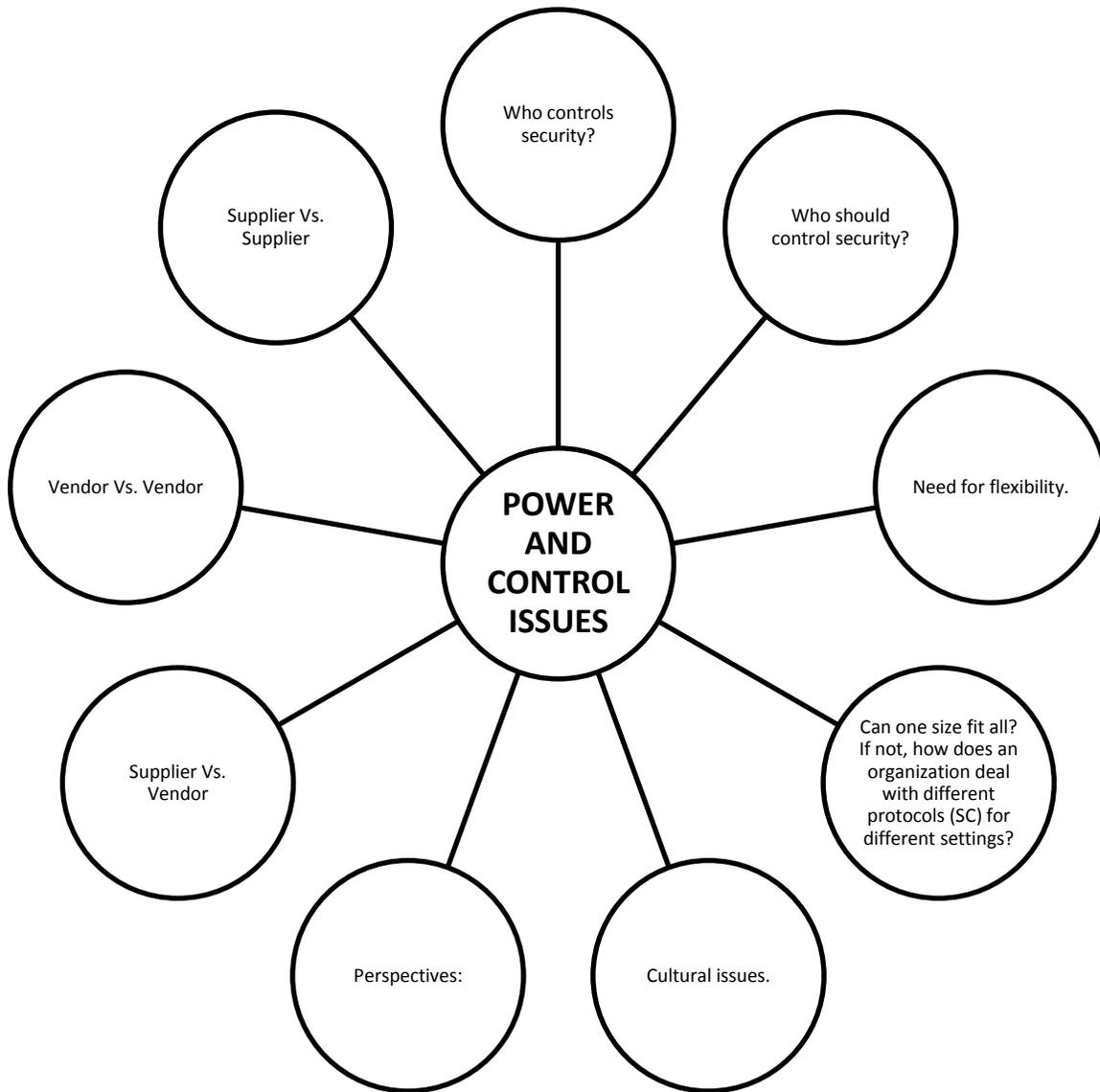


Figure 6: Power and Control Issues