Sharing and Guarding Information: Managing Data Security in Supply Chain Networks

Darian Unger and Rajni Goel

Abstract

Companies must frequently balance the benefits and security threats of sharing information with suppliers. This paper broadly surveys and summarizes several recent cases of network hacking, compromised bidding systems, competitive business theft, and the inadvertent transformation of suppliers into competitors. We develop a general framework that categorizes these information threats and maps them to specific information technology (IT) and business policy solutions, including more stringent security procedures, enhanced software technology, and improved vetting. Depending on the specific threat, companies can purchase or implement distinct countermeasures as part of a larger strategy for IT security. Companies and supply chain experts can use our review and proposed framework to better understand information threats and improve their information sharing procedures.

Introduction

In this era of systems-based design and complex manufacturing, companies must share their product information with suppliers to benefit from improved supply chain management (SCM) systems. Companies often employ networked supply chains to share necessary data with partners and suppliers. Firms balance the need to share information with their need to limit information exchange and protect data security. Protecting security and privacy creates barriers that, although sometimes necessary, prevent companies from sharing complete information in a supply network. Existing literature and practices suggest a need for a clear framework for balancing security and information-sharing in SCM systems. This research defines such a framework by using a case study methodology to identify and categorize threats faced by different companies.

Our work contributes to the field by examining information-sharing problems in the supply chains of several large organizations. Our cross-industry research includes interviews with company managers and recent published revelations about supply chain security breaches. We categorize the various supply chain threats and match them to IT security mechanisms and business solutions that can improve SCM.

We begin by acknowledging the literature describing the benefits and advantages of information-sharing in SCM. We then define and identify actual case-based threats of information sharing, including data theft, data inference, compromised bidding and reverse-auction systems, and hacking. Much of the current literature focuses on security threats from hacking attacks from outside the company network; however, companies are frequently exposed to insider threats such as the loss of competitive information from people within their own network of suppliers and partners. Our research includes both insider and outsider vulnerabilities to proprietary information and intellectual property.

We use business case studies to classify SCM threats into three major categories. The first category is the technical loss of proprietary information to rivals. This can lead a company to forfeit its competitive advantage. Technical loss of information can occur through competitive business theft, hacking, poor information security, inference by suppliers, or the transfer of information by personnel. The second category of threat, system malfunction of supply chain information technology (IT), causes both delays and ordering mistakes. The third category, compromised bidding systems, can lead to significant cost increases due to artificially high bids from suppliers. We use these cat-

egories to develop a new framework for balancing information sharing and information security in SCM. The framework is a potentially useful tool for managers who decide which security mechanisms to deploy, how to share information, and how to maintain competitive advantage. The research also provides practitioners and academics with a protocol for improved information sharing that balances supply chain efficiency with information and intellectual property security.

Literature Review

Existing literature and industry practices have established the value of sharing information with suppliers. For example, companies frequently invite several potential suppliers to bid for purchases in reverse-auctions. Increasing the information available to those suppliers, including physical specifications or demand forecasts, allows the suppliers to discern their own forecasts accurately before making bids, thus encouraging a healthy supplier rivalry and reduced costs. Dell and Ford Motor Company are often cited as examples of companies that share a great deal of information with suppliers in order to reduce overall product cost (Akasie, 2000; Jacobs, 2003; Kapuscinski, 2004). Other advantages and examples of sharing information with suppliers are well-documented, especially with the expansion of e-procurement, collaborative commerce, and the use of radio frequency identification (RFID) tags and other IT systems to reduce companies' operation costs (Fortescue, 2004; Laudon 2004). Together, these methods of sharing information with suppliers can lead to competitive advantage (Kaufman and Carter, 2004).

Despite these advantages, companies sharing information with suppliers should remain aware of the threats that accompany the distribution of production data and methods. To sustain competitive advantage, companies must not only release information but control its flow (Prasad, 2003). Simply increasing the level of sharing may increase supply chain speed, but selective sharing will increase the effectiveness. Companies that would otherwise freely exchange information to raise productivity should worry about exploitation by competitors and the appearance of collusion that might violate antitrust regulations. These concerns necessitate an intelligent system that controls the degree of information sharing.

Controls are necessary because of many significant information threats (Stedman, 1999). According to the 2003 CSI/FBI Computer Crime and Security Survey (2003), theft of proprietary information was the largest category for losses, totaling 35% of the total financial loss reported in that survey. However, existing research on IT breaches is not always linked to supply chain management, nor does it establish that such breaches are harmful. Challenging the importance of this data theft threat, Teece (1998) points out that merely gaining information does not constitute a large threat because many additional steps are necessary to capitalize on the information gained. Hurdles include competence, complementary assets, and "sensemaking" of data. Firms seeking to protect their competitive advantages should erect as many such hurdles as possible to inhibit rivals and potential new competitors. Although Teece applies his findings to innovation management, we seek to extend this work and apply it to SCM as well.

Porter (1987) has long suggested the potential threat from suppliers. This threat has traditionally been understood as the ability of suppliers to raise their prices, resulting in increased costs. Dangers from suppliers can also include the actual loss of market share to suppliers who become direct competitors as they gain market knowledge, often with the unwitting help of the purchasing company. (Ulrich, 1989).

Several other articles instead focus on the benefits of information sharing among nodes in a global supply chain (Lee and Whang, 2000; Alade, 2004). Agarwal (2001) and Kolluru (2001) also offer practical information on information sharing and supply chains. Both stress the utility of sharing information with suppliers, but include only limited analysis of the threats of such sharing. Agarwal limits analysis to databases, while Kolluru only considers threats from known attacks by outsiders, such as hacking and identification spoofing.

Existing literature offers broad consensus on the opportunities afforded by greater information sharing

Table 1

Different SCM and IT threats faced by organizations

Company/Organizations	Informations/SCM security threat
Reebok	Lack of speed until implementation
Siemens-Westinghouse Power Generation (SWPG), Ellery Systems	Direct theft of design data
Sony, Burger King	Direct hacking attack
Baxter/AHS	Indirect supplier inference and takeover
CNN, Amazon	Direct denial of service attack
Microsoft, CRX	System Down
Nike	Poor SCM software implementation
U.S. General Services Administration (and Bidding government contractors)	Compromised bidding system

with suppliers; however, analyses of the commensurate threats tends to be narrowly focused on specific media or types of information (Durfee, 2000). Companies are left with the vexing question of how to share data in order to reduce supply chain costs without also revealing or losing valuable information.

Findings

Our findings focus on the threats and problems that companies have faced while using IT to share information with suppliers and other companies. We define information to include orders, shipments, products, designs, demand forecasts and inventory data in any form or media. A summarized list of cases is shown in Table 1, which lists companies and the problems they faced. Some of these problems, such as Nike's difficulties in implementing its i2 SCM software, are identified through several existing case studies. Others, such as Westinghouse' data thefts, are based on direct interviews with company managers in an effort to identify specific SCM information threats. We also incorporate recent revelations about security breaches at Sony and Amazon.

Table 1 displays a range of SCM and IT problems that are representative of threats companies often encounter in their supply chains. Some companies, such as Siemens-Westinghouse and Ellery Systems, have fallen victim to the direct theft of information even though the companies are in different industries. Baxter and AHS, both provide medical equipment, yet faced two markedly different SCM and information-sharing problems.

Initial interviews with supply chain managers from Reebok confirmed previous findings on the utility of sharing information and provided further demonstrations of how sharing information with suppliers can reduce both cost and time to market. For example, when Reebok started sharing sensitive ordering and manufacturing data with East Asian leather and rubber suppliers, the company benefited from a more rapid supply chain. This resulted in heightened productivity and increased competitiveness; products were available to the American and European markets several months sooner than they would have been if Reebok had continued using more restrictive information-sharing procedures.

Useful patterns and categorizations emerge as the Reebok case study and other findings are aggregated. We find that sharing information electronically leads to three distinct yet overlapping threats. The first major threat is the loss of sensitive, proprietary data to either competitors or potential competitors. The second threat is that of compromised bidding systems, which can lead to high supply costs. The third threat is the

potential malfunction or freeze of a supply chain system due to IT system error. Each category has several potential causes, some of which are shared. For example, computer hacking can be an avenue for both direct information loss and compromised bidding systems, eventually resulting to the loss of competitive advantage, customers, market share, and stock value. The threats and mechanisms are described in the text and industry cases and shown graphically in Figure 1.

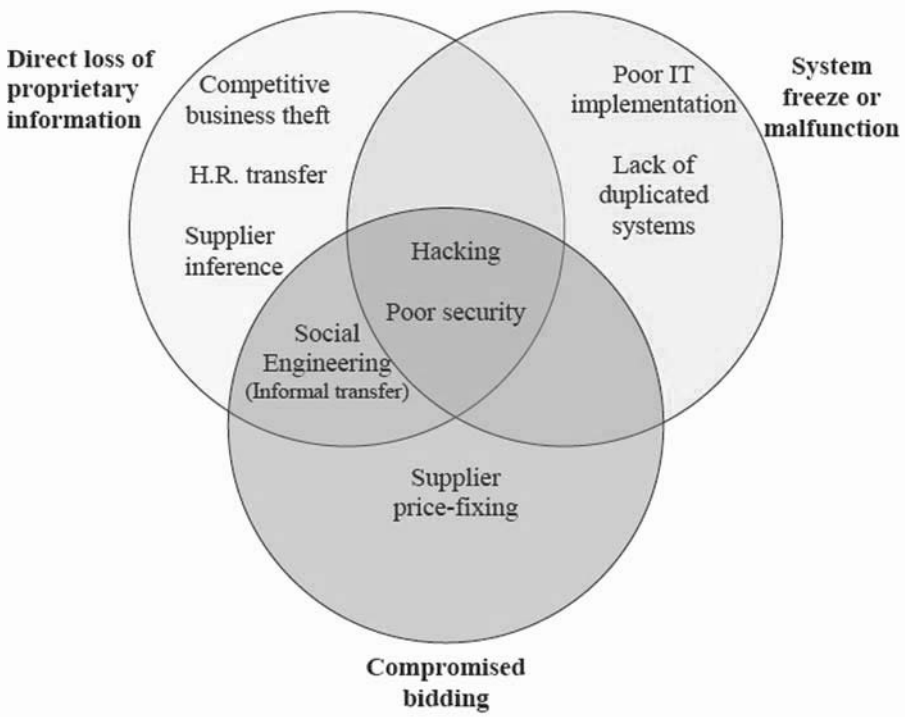
Direct Loss of Proprietary Information

Companies have historically guarded their proprietary data for competitive advantage. A company could irretrievably lose competitive advantage if it shared sensitive design data with a supplier, which in turn released that data to an intra-industry rival. The loss could be compounded if the original company lacked patent protection. Such loss of proprietary information to intra-industry rivals can occur either through competitive business theft, poor information security, the transfer of information by personnel, accidental communication, or hacking. Competitive business theft is exemplified by numerous cases of industrial espionage where one company is able to view or glean sensitive technical data directly from its rivals. Such theft is relatively common, especially in industries in which products have relatively long lead times and in which information is already packaged for the convenience of suppliers. (Mixson, 1977; Whitney, et. al. 1996; Creswell, 2004).

Theft and poor information security procedures can also cause loss of proprietary information. In the late 1990s, Siemens-Westinghouse Power Generation (SWPG), partnered with rival companies in an effort to reduce costs and expand its overseas markets. Interviews and discussions with company engineers and managers indicate that SWPG intended, and indeed needed, to share information with its rival-partners. However, SWPG failed to appropriately limit the information shared. The rival, once granted access to some internal documents, had virtually free reign among SWPGs proprietary collection of detailed designs, some of which were then copied. SWPG employees later found that unauthorized viewers had

Figure 1

Potential threats from supply chain information sharing



accessed some designs, but they detected the infraction too late. Proprietary data had been stolen, with potential losses of over $1 million.

Supplier inference occurs when companies accidentally allow their own suppliers to become direct competitors. There are several examples of suppliers who have taken over markets from their one-time customers, including Baxter-Travenol Laboratories, a medical equipment company, which used to be a supplier to American Hospital Supply (AHS). Baxter became so good at anticipating its customers' orders and needs that it was able to predict the market better than AHS itself. Armed with this knowledge and market success, Baxter began supplying hospitals directly, first bypassing, then taking over, and eventually completely acquiring AHS (Barkhotz, 1985; Rublin, 1986; Ulrich, 1989).

Data inference also occurred when SWPG attempted to reduce costs by creating additional suppliers in China. Manufacturing costs of necessary machine parts were much lower overseas, but the Chinese suppliers needed to be trained in order to ensure acceptable quality. During the training, one supplier was able to infer enough about the power turbine market to become a direct competitor to the company it was supposed to supply. Nor is outsourcing to China unique; an executive from Wipro, one of India's top technology companies, summarized the potential problem for purchasing or outsourcing companies when he said, "You go from solving my problem to serving my business to knowing my business to being my business" (Friedman, 2005, emphasis added).

Inference by suppliers is different from the general loss of proprietary information because it may involve neither theft nor proprietary data. Inference is learning, not stealing. Furthermore, the information learned is often useful, but general and neither patented nor proprietary. This occurs when suppliers log all information communicated from other companies in their supply chain. The supplier can then use widely available mining tools to mine the data (including responses to questions, direct statements or quantitative information) for patterns. From this aggregated data, inferences are derived which otherwise would not be evident from any one individual piece of information. Upstream companies may unwittingly assist in this endeavor by over-sharing information that is not relevant to production, or by not recognizing that production information itself may offer useful insights to suppliers regarding expected sales.

Human resource transfers constitute a third avenue by which companies can lose proprietary information to rivals. The relatively commonplace practice of "poaching" occurs when one company attempts to hire employees of a rival company specifically because of their knowledge. Some of this knowledge is experience and training, but some may also be proprietary. Companies attempt to limit this type of information loss by having employees sign nondisclosure or noncompetitive contracts that employees may hold employees liable for providing information to rivals, but these precautions are not failsafe. For example, in 1993, a former General Motors employee defected to Volkswagon bringing sensitive design, purchasing, and sales information with him and causing tens of millions of dollars in damages (Denning, 1999). Similarly, Apple filed a civil suit in 2002 against a former contractor for stealing company trade secrets by publicly posting schematic drawings, images and engineering details of an unannounced Apple product (Wilcox, 2002).

Even current employees can leak proprietary information. This problem of social engineering, or "loose lips," occurs when information is leaked inadvertently or pried out of an employee by a seemingly friendly party (Rusch, 1999; Mixson, 1977). Social engineering is the attempt to garner information from direct communication with purchasers' insiders who unwittingly provide information due to lack of caution, poor negotiation skills, or because they fall victim to outright deception (Harl, 1997). If the information is leaked intentionally or for a price, it is a form of competitive business theft. For example, in 1994, a "highly trusted employee" of Ellery Systems in Colorado transferred $1 million worth of software to a competing Chinese firm. A recent American Society for Industrial Security survey suggested that trusted insiders are among the greatest threats to corporate intellectual property (Denning, 1999). Supply chain

partners and their employees can frequently qualify as insiders, who are defined as people who have been vetted and explicitly granted privileges authorizing use of a particular system (Neuman, 1999).

Companies also lose supply-based or general proprietary data through generalized hacking; computer penetration is a serious threat. Integrated SCM requires a broad sharing of data and the commensurate expansion of databases and information systems. Broad, inter-industry information systems are considerably more open to attack than smaller, better-protected files that companies keep internally on LANs. As a result, large-scale information sharing may expose a company to considerably more hacking attempts. These incursions differ from earlier examples in this section because generalized hacking may not be motivated by any attempt to steal information. Furthermore, hackers are frequently not even rival companies, but instead relatively disinterested third parties that may cause damage or loss of data with no theft at all. Examples of hacking attacks include those on Sony Records (Warren, et. al. 2000), Amazon, and Burger King, which suffered either website damage, denial of service, or both (Garg, et. al. 2003). Together, these examples demonstrate that the direct loss of proprietary data can occur in several ways.

Compromised Bidding Systems

Compromised bidding systems constitute a second major information threat because they allow suppliers to charge artificially high prices. For example, if two suppliers are competing for a contract in a silent reverse auction or bidding contest, each supplier has an interest in knowing the bid of its rival. Such knowledge can allow the first supplier to bid only slightly lower than its rival, reducing true competition and increasing the buyers' costs.

A recent example of a compromised bidding system occurred on eOffer, a website and system belonging the U.S. General Services Administration (GSA). As the federal agency responsible for government procurement, the GSA is the world's largest contracting organization. It introduced eOffer in 2004 to simplify the bidding system and allow contractors to provide online information and offers. In December 2005, the Inspector General received a report of a security flaw that allowed contractor fraud. The flaw, which allowed one authenticated bidder to potentially access and even change the bids of rival contractors, forced the GSA to shut down eOffer for almost a week. Until the flaw was repaired, bid tampering was possible, and one entrant could see and theoretically alter the bids of rivals, major government contractors such as Boeing, Lockheed Martin, Dell, Gateway, and hundreds of other companies. GSA is still investigating possible irregularities because it does not yet know whether or how much bid tampering may have occurred. Although the acquisition system was online for less than two years, it had data from over nine years of government purchasing contracts and 1,200 companies (Weiss, 2006; Markoff, 2006).

Compromised bidding also occurs if, instead of knowing at which price a rival supplier is willing to sell, a supplier knows at which price a customer is willing to buy. Unfortunately for purchasers with compromised or broken systems, either or both pieces of information may be available to a supplier. If such information is available to several suppliers, then supplier price-fixing is also possible. Suppliers can gain unauthorized access to bidding data in two ways. Suppliers can breach a purchaser's (or rival suppliers') information system, thus compromising the bidding system, or untrustworthy suppliers can gain restricted information through social engineering.

System Freeze or Malfunction

A final threat of SCM information sharing using networked IT systems is potential system failure, which can cause stoppage or mis-orders. Manufacturers must fulfill customer orders rapidly and inexpensively to remain competitive. Losses may occur if any component of the supply chain information system is non-functional. This was illustrated by athletic shoe industry leader Nike, which encountered major difficulties in implementing i2 forecasting and supply chain software. The results, mainly in the form of poorly-placed orders to East Asian suppliers, cost the company almost 100 million (Koch, 2004; Laudon, 2004).

In another major supply chain example, cyber threats to digitally-operated railways can disrupt any supply chain infrastructure that depends on rail transport. For instance, CSX rail transportation was forced to shut down its central control dispatching center in 2002 because of a computer virus. The company shut down crossing signals in 23 states and had no way to track the location of its trains (King, 2003). This breach of the main IT system adversely affected the transport of goods in many supply chains. The potential threat against the rail infrastructure is of great concern; several studies have demonstrated successful attacks on control systems. Hacker activity includes the ability to break into wireless networks and degrade or disrupt system availability (GAO, 2004; Chittester and Haines, 2004; Presidential Report, 2003).

Like rail transport, e-procurement and digital transactions are now necessary components of efficient supply chains. Yet these systems are also vulnerable. For example, in 2003 the "Blaster" computer virus invaded Microsoft, flooding its product support web site with millions of update requests, causing systems to fail (Smith, 2004). This attack affected not only Microsoft, but many of its business customers to whom Microsoft supplied critical product support. The total losses included supply chain disruptions as well as the costs of virus detection, isolation and removal. Thus, organizations seeking to remain competitive must invest in security mechanisms that protect IT systems by providing detection, deterrence and recovery capabilities. Together, these three threats, and their numerous subcategories, pose risks to companies seeking to improve their supply chain with increased information sharing.

Research Applications: Policies to Combat Information-sharing Threats

The findings above organize the case studies into overlapping categories of information-sharing threats. The results can be useful to supply chain and information security managers who need to identify and control information flows. Figure 1 shows that many root disruption mechanisms are concentrated in the loss of proprietary information category, indicating an area of particular sensitivity. The case studies and recent literature reports confirm that many of the most serious information concerns deal with the direct loss of sensitive information to suppliers or competitors and the potential gaming of supply chain bidding systems. The root risks common to all three categories of threat include hacking and poor security. Informal sharing and social engineering risks are common to both direct information loss and compromised bidding. Information security managers looking to address threats in the most efficient way possible may choose to address these risks first. We now address potential solutions and map them to the specific threats determined above.

We developed the following framework to help protect and facilitate information sharing. A combination of existing technologies and business policies can address practical security needs for sharing supply chain information. Security mechanisms and designs have been developed for protecting the confidentiality, integrity and availability of information in computer systems. Technologies such as intrusion detection systems, encryption, firewalls and application software can address issues of access controls, authentication, and data protection. Other countermeasures include access control policies, stringent human resource (HR) security policies, and a deliberate vetting of data and distribution partners. Table 2 provides a summary map of the threats, proposed solutions and cost of proposed solution implementation.

Information Technology Remedies

Information technology advances have reduced the risk of hacking attacks, theft, and poor security in SCM while enhancing the ability to share information. The challenge is to minimize the damage of the attack or threat. Potential security tools include access controls, firewalls, encryption, intrusion detection systems and authentication.

Table 2

Threats matched to information-sharing solutions

IT/SCM threat mechanism	Threat category	Solutions	Cost of countermeasures
Competitive business theft	Direct info loss	• ID security • HR policies	• Additional IT costs • Monitoring and employee relations
Poor IT security	All	• Encryption • Access control	• Additional IT costs
Personnel/HR transfer	Direct info loss	• HR policies • Nondisclosure agreements • Misuse detection systems	• Inexpensive implementation, but challenging enforcement
Hacking	All	• Firewalls • Encryption • Digital signatures • Location signatures • Intrusion detection	• Additional IT costs • Employee relations
Social engineering	Direct info loss and compromised bidding	• HR policies	• Monitoring and employee relations
Supplier inference	Direct info loss	3rd party authentication and vetting	• Additional IT costs • Management time and effort in reviewing trust levels
Poor IT implementation	System freeze/malfunc.		
Lack of redundant systems	System freeze/malfunc.	Backup or redundant system	Extra system and transition costs

Access controls ensure that only authorized users view or edit stored information in the computer system. Access control solutions authenticate the requester of information and verify if this requester is authorized to view and edit data. Critical controls may employ strong identification mechanisms, such as smartcards, personal identification numbers, and secure IDs. Other access controls may employ less expensive, but weaker mechanisms, such as passwords, and may use simple encryption to store this data. Once identified, role-base access controls are implemented and validate authority to view specific information. This controls the granularity of the view of information, allowing different people in the supply chain to review only the specific information necessary for their job function. Access control limits direct loss of proprietary information and secures against unauthorized disclosure.

Firewall software for SCM should be designed to be friendly to information requests, since the goal is to share across distributed, networked, and integrated supply chains. Firewalls are poor determinants or managers of trust levels between companies and suppliers, and should not be used for this purpose. Rather than trying to bar unauthorized users or investigate inquiries already authenticated by the other IT tools de-

scribed earlier, firewalls should be used mainly to detect and stop viruses, worms, and hackers. Since only authorized supply chain partners can enter a firewall-secured system, loss of information becomes controllable and traceable. This monitoring also ensures the integrity of bidding systems.

Encryption, or the scrambling of the data according to a secret transformation key (symmetric or asymmetric), secures supply chain partners from malicious tampering and information loss. It is crucial because internet and LAN traffic is particularly vulnerable to eavesdroppers who deploy packet sniffers. Digital signatures use the public key infrastructure, and verify the identity of the sender of information, whereas hash signatures validate the integrity of data. Encryption adds confidentiality and integrity to data being sharing across the network, while also protecting data that are stored on computer systems.

Misuse and intrusion detection systems (IDS) operate on the principle that it is not feasible to prevent all information leaks, (particularly those caused by insiders) but that such attacks follow identifiable patterns or deviate from normal usage in identifiable ways. By monitoring system behavior, either from audit records or in real time, a profile of the user or system is created using statistical or nonstatistical methods. Components, as network-based, host-based and application layer IDS can be installed for prevention of system entry, outside intrusion, and misuse by even authorized persons. These methods deter hacking and reduce the risk of compromised bidding systems.

Finally, improved authentication technologies are another useful tool in SCM. Authentication deters impersonation of legitimate users and controls access to sensitive information. Authentication mechanisms can include knowledge requirements through passwords, possession of secure IDs, or even biometrics to verify the identity of a user, an agent external to the protection system, or other entities, even on networked computers.

Despite the five tools described above, sharing data is often restricted by widespread privacy concerns. Securely integrating data from multiple sources has been a heavily researched arena in the information security community. Some information, such as point-of-sale data, may be kept private, while the information actually needed by a supplier can be communicated by using new privacy-preserving data exchange algorithms. For example, privacy-preserving data mining algorithms modify the original data so that the private data and knowledge remain private even after the mining process. These techniques also help deter the database inference problem. Heuristic techniques (classification, association rule discovery and clustering), as well as cryptographic, statistical, and reconstruction-based techniques, are alternative approaches to sharing information while preserving the privacy of sensitive data.

These algorithms provide solutions to the problem of sharing the minimal amount of information necessary across databases and provide results to queries without revealing additional information. Accurate correlations among various sets of data become difficult, especially when they are shared with different partners. This difficulty combats the inference threat described earlier, allowing companies to maintain their competitive advantages.

Human Resource and Business Policy Solutions

Improved HR policies are also crucial to SCM control. Company policies frequently include nondisclosure contracts with employees to prevent industrial espionage, but these are not failsafe and may be dependent on uncertain and expensive litigation. Nondisclosure agreements, although useful, can be supplemented with a variety of other tools more suitable for use with current, rather than former, employees and supply chain partners.

HR policies may include both holistic evaluation and individual monitoring. Holistic evaluation can include the establishment of a SCM or information manager who evaluates information in two ways. First, the manager guards against the direct loss of proprietary or sensitive data by vetting the trustworthiness of SCM partners before allowing more general access to information. Second, the manager can establish guards to monitor whether a supplier is garnering enough knowledge by inference to become a competitor. If necessary, process or product information can

be parsed and dispersed among different suppliers to prevent over sharing with one partner.

Individual monitoring can include monitoring either of or by employees in the company or partners in the supply chain. Monitoring by employees is far less controversial because it involves training in which each employee or SCM partner employee is taught that information security is a responsibility within their job description. Monitoring of employees, on the other hand, can include email screening, communication monitoring, and other enforcement mechanisms that may provide security but often infringe on employee privacy and working conditions.

Trust is an inherent aspect of supply chain performance, yet it is difficult to embed in a security policy or mechanism. A trusted third party authentication system provides the trust necessary to allow the distribution of information across supply chains. Two companies needing to exchange information give data to a "trusted" third party-which is completely trusted with respect to intent and competence against security breaches-that authenticates each company's information and also ensures that this information does not reach malicious hands. Authentication provides the ability to reliably establish the identity of the communicating parties, regardless of whether they are partners or individuals.

Supply chain partnerships are heterogeneous, so companies should deal with different partners, agents, and data unequally. Security policies on data sharing and access should vary based on multilevel security considerations. One key tenet in efficient information sharing is need-to-know usage of information. People should be using the information for exactly what it was intended and required, but no more. Thus, internal access, security, and privacy mechanisms should ensure that each insider who accesses a company system only uses the information as required by his or her assigned duties.

Weighing Threats and Solutions

Companies must decide how much to invest in the SCM security mechanisms and business policies described above. IT remedies and protective policies can mitigate the risks of sharing data with suppliers, but their costs include restrictions on sharing information and tangible IT investments. To make investment decisions, companies should balance the risk of information sharing threats against the costs of implementing solutions. Risk analyses can serve as useful tools in this balancing act.

The individual threats addressed in section three do not all constitute large risks because risk is a function of both probability and consequence. A threat of high probability, such as a hacking attack, may be of low risk if the consequence of the hack is small. For example, a hacking attack is of little concern if it only slows down company servers over a short or low-traffic period when losses are minimal. Similarly, an improbable threat, such as the reneging of a trusted supplier on a confidentiality agreement, may be of low risk even though the potential consequences are significant. Our proposed framework is a useful resource in understanding the inherent risks of SCM information sharing and the potential costs of IT or security solutions. Companies can use the framework to identify current risks and evaluate or implement appropriate countermeasures.

Conclusions

Companies must share information with suppliers to reduce supply chain costs, but sharing information introduces risk. Our review and summary of industrial cases reveals different categories of threats that stem from sharing information, including loss of information, compromised bidding systems, and system failure. Many threats can be mitigated or prevented by IT advances and improved HR or information-sharing policies that address specific business threats. These countermeasures, including improved vetting, security software, authentications, and employee training, allow for a wider flow of information and more efficient SCM.

Because overall 'blanket' solutions to information sharing threats consume resources, companies need specific solutions to address each threat. Our categorization of threats and mapping of potential solutions provides a framework for improved information sharing that balances supply chain efficiency with informa-

tion and intellectual property security. The proposed framework can be used by businesses and researchers to improve supply chain efficiency, reduce business threats, manage trust with suppliers, and identify policies that reduce information loss.

References

Agarwal, R. et. al. (2001) *Supply Chain Agent Decision Aid System (SCADAS)*, Proceedings for the 2001 Winter Simulation Conference.

Akasie, J. (2000) "Ford's Model E," *Forbes*, New York: Jul **17**, pp. 30–34.

Barkholz, D. et. al. (1985) "Hospitals Expect to Gain Benefits from Baxter-American Merger/Wall Street Hails Baxter Victory/HCA Continues Expansion Efforts in Wake of Failed American Merger," *Modern Healthcare*. Chicago: Aug 2, Vol. 15, Iss. 16; p. 16.

Chittester and Haines (2004) "Risks of Terrorism to Information Technology and to Critical Interdependent Infrastructure", *Journal of Homeland Security and Emergency Management*, Vol. 1, Iss. 4.

Computer Security Institute (CSI) and the FBI (2003) *Computer Crime and Security Survey*. `http://www.security.fsu.edu/docs/FBI2003.pdf`

Creswell, J. (2004) "Boeing plays defense," *Fortune*, New York: Apr. 19, Vol. 149, Iss. 8; p. 91.

Denning, D. (1999) "Industrial Espionage: Who's Stealing Your Information?" *Information Security*.

Durfee, G. and Franklin, M. (2000) *Distribution Chain Security*, ACM, Athens.

Fortescue, S. (2004) "Courts' IT purchasing goes online," *Supply Management*, Sept. 23,, p. 8.

Friedman, T.L. (2005) "Bangalore: Hotter and Hotter," *The New York Times*, June 8th.

Garg, A., Curtis, J. and Halper, H. (2003) "Quantifying the financial impact of IT security breaches," *Information Management and Computer Security*, 11/2, pp. 74–83.

Government Accounting Office (GAO), (2004) "Critical Infrastructure Protection Challenges and Efforts to Secure Control Systems", Testimony Before the Subcommittee on Technology Information Policy, Intergovernmental Relations and the Census, United States House Committee on Government Reform, March 30.

Harl, (1997) "People Hacking: The Psychology of Social Engineering," Talk at Access All Areas II Conference, May 7, `http://www.noblit.com/docs/people-hacking.html`.

Jacobs, D. G. (2003) "Anatomy of a supply chain," Transportation & Distribution. June, Vol. 44, Iss. 6; p. 60

Kaufman, L. and Carter, C. "Deciding on the Mode of Negotiation: To Auction or Not to Auction Electronically," *The Journal of Supply Chain Management*, Spring 2004, pp. 15–26.

Kapuscinski, R. et. al. (2004) Inventory Decisions in Dell's Supply Chain, *Interfaces*. Linthicum: May/June, Vol. 34, Iss. 3, p. 191.

King, L. (2003) "Computer virus hits CSX," Destination Freedom Newletter, Vol. 4, No 34.

Koch, C. (2004) "Nike Rebounds: How and Why Nike Recovered from its Supply Chain Disaster," *CIO Magazine*, June 15.

Kolluru, R. and Meredith, P. (2001) *Security and trust management in supply chains*, Information Management & Computer Security; Vol. 9, No. 5.

Laudon, K. and J., (2004) Management *Information Systems, 8th ed*. NJ: Prentice Hall, pp. 132–134.

Lee, H. L. and Whang, S. (2000) "Information sharing in a supply chain," *International Journal of Technology Management*, **20**(3/4), pp. 373–387.

Markoff, J. (2006) "Web Site Of Agency Is Called Insecure," *The New York Times*, Jan. 13, p. C1, Col. 6.

Mixson, P. (1977) "Loose Lips Sink Sales," *S & MM - Sales & Marketing Management*, New York, Vol. 118, Iss. 2; p. 37.

Neumann, P.(1999) "Risks of Insiders," *Communications of the ACM*, December 1999, Vol. 42, No. 12.

Rublin, L. (1986) "Just What the Doctor Ordered: Baxter Plus American Hospital Equals a Robust Com-

petitor," *Barron's National Business and Financial Weekly*, Boston, Vol. 66, Iss. 48; p. 13.

Porter, M. (1987) "From Competitive Advantage to Corporate Strategy," *Harvard Business Review*, pp. 43–59.

Prasad, S. and Sounderpandian, J. (2003) "Factors influencing global supply chain efficiency: implications for information systems," *Supply Chain Management: An International Journal*, Vol. 8, No. 3, pp. 241–250.

Presidential Report, President's National Security Telecommunications Advisory Committee Wireless Task Force Report "Wireless Security" (2003) January.

Rusch, J.J. (1999) "The 'Social Engineering' of Internet Fraud," Internet Society, INET 1999 Proceedings, San Jose, California, June.

Smith, T. (2004) "Information Risk: A New Approach to Information Technology Security," Sys.Con Media, Nov. 29,.

Stedman, C. (1999) "Race heats up for e-supply chains," *Computerworld*, Framingham. Vol. 33, Iss. 45, p. 1.

Teece, D. J. (1989) "Capturing Value from Knowledge Assets," *California Management Review*, Vol. 40, No. 3, pp. 55–79.

Ulrich, D. et. al. "(1989) Why Baxter Moved Quickly to Absorb American Hospital," Mergers and Acquisitions, Philadelphia, Vol. 24, Iss. 1; p. 54.

Warren, M. and Hutchinson, W. (2000) "Cyber attacks against supply chain management systems: a short note," *International Journal of Physical Distribution & Logistics Management*, Vol. 30, No. 7/8, pp. 710-716. (Sony)

Weiss, T. R. (2006) "GSA's vendor Web site closed to fix security flaw; Flaw could allow applicants to see and change data on other vendors." *Computerworld*, Jan. 13, Government section.

Whitney, M. and Gaisford, J. (1996) "Economic espionage as strategic trade policy," *The Canadian Journal of Economics*, Malden, Vol. 29, Part 2, p. S627.

Wilcox, J. (2002) "Apple sues former contractor," CNET News.com, December, 11.

ABOUT THE AUTHORS

Darian Unger is an Assistant Professor at the Howard University School of Business. He received his Ph.D. from the Massachusetts Institute of Technology (MIT) in engineering systems management and policy, and his M.S. in technology policy. He received B.A. and B.S. degrees from Swarthmore College. His areas of specialization and industrial experience include supply chain management, technology management, and energy infrastructure development.

Rajni Goel is an Assistant Professor in the Information Systems and Decision Sciences Department in the School of Business at Howard University. She holds a Ph.D. (IT) from George Mason University, an M.S. (Mathematics) from George Mason University and a B.A. (Mathematics) from Millersville University. Dr. Goel's areas of specialization and research include information security, privacy, enterprise security, profiling/data-mining, grid computing and security, high performance computing and security curriculum development. She is an active member of the Center of Applied High Performance Computing and has served as an Adjunct Professor of Mathematics.