1-1-2010

Critical Management Issues for Implementing RFID in Supply Chain Management

Bharatendu Srivastava
Marquette University, bharat.srivastava@marquette.edu

Published version. *International Journal of Manufacturing Technology and Management*, Volume 21, No. 3/4 (2010), DOI.

Critical management issues for implementing RFID in supply chain management

Bharatendu Srivastava

Department of Management,
Marquette University,
PO Box 1881, Milwaukee, WI 53201-1881, USA
E-mail: bharat.srivastava@marquette.edu

Abstract: The benefits of radio frequency identification (RFID) technology in the supply chain are fairly compelling. It has the potential to revolutionise the efficiency, accuracy and security of the supply chain with significant impact on overall profitability. A number of companies are actively involved in testing and adopting this technology. It is estimated that the market for RFID products and services will increase significantly in the next few years. Despite this trend, there are major impediments to RFID adoption in supply chain. While RFID systems have been around for several decades, the technology for supply chain management is still emerging. We describe many of the challenges, setbacks and barriers facing RFID implementations in supply chains, discuss the critical issues for management and offer some suggestions. In the process, we take an in-depth look at cost, technology, standards, privacy and security and business process reengineering related issues surrounding RFID technology in supply chains.

Keywords: supply chain management; radio frequency identification; RFID.

Reference to this paper should be made as follows: Srivastava, B. (2010) 'Critical management issues for implementing RFID in supply chain management', *Int. J. Manufacturing Technology and Management*, Vol. 21, Nos. 3/4, pp.289–307.

Biographical notes: Bharatendu Srivastava is an Associate Professor of Operations and Supply Chain Management at Marquette University. His research focuses on supply chain management, production planning and scheduling, RFID applications in SCM, flexible manufacturing systems and cellular manufacturing. His research has been published in journals such as *Annals of Operations Research*, *European Journal of Operational Research*, *IEEE Transactions on Robotics and Control*, *Journal of Operational Research Society*, *International Journal of Production Economics* and *Business Horizons*.

1 Introduction

Of all the emerging technologies in supply chains, none is likely to have a bigger impact than radio frequency identification (RFID). RFID tags attached to products are capable of providing real-time tracking information across the supply chain. Potentially, this information can be of significant value in terms of improving supply chain efficiencies and revenue generation (Angeles, 2005; Srivastava, 2004). Information sharing is often

considered the key to improving supply chain operations (Lee et al., 1997). Most of the foundation work for implementing RFID technology in supply chain was carried out by Auto-ID Center labs and its members. EPCglobal is responsible for developing and administering this technology.

With RFID initiatives from major retailers like Wal-Mart, Target, Mark & Spencer, Metro AG and Tesco likely to influence the whole retail industry, there is little doubt that RFID will become a pervasive technology in the future. Currently, several retailers utilise RFID tags to track shipment of goods through their distribution network. A number of studies forecast the market for RFID tags, products and services to increase sharply in the coming years (King, 2006; Liard, 2005). IDTechEX (2007), a technology research firm, estimates RFID business to jump from about $5 billion in 2007 to over $25 billion in 2017. All of this makes RFID one of the single biggest drivers of technology spending in supply chain management. Given the growing complexity of today's supply chains, RFID technology is also likely to be one of the biggest technological undertakings for most firms.

Despite this general trend, there are several fundamental questions and challenges that companies face when assessing, planning and implementing RFID projects. Several pilot projects involving the EPCglobal technology have produced somewhat disappointing results (McWilliams, 2007), most companies are adopting RFID because they have to (The Economist, 2007; Schuman, 2006). While RFID systems have been around for several decades, the technology for supply chain management is still emerging. Several barriers related to cost, global standards, system integration, information technology (IT) infrastructure, privacy and security are seriously hindering the widespread deployment of RFID in supply chains. Excessive promises and hype about the benefits of RFID (often by RFID vendors and consulting companies) have also created a cloud of uncertainty and misconceptions. As pointed out by Lee and Özer (2007), there is a serious credibility issue with several reports generated by the industry with respect to the rate of return on investment.

While some companies are taking a cautious wait-and-see approach, many others are doing just the minimum (such as placing the tag at the distribution centre just before shipping the products to retailers) to comply with mandates (Schuman, 2006). While this practice fails to yield any significant supply chain benefit, it is not surprising – firms when forced to adopt a technology by the dominant partner in the supply chain, often do not implement the technology in the best possible way (Riggins and Mukhopadhyay, 1994). Ideally, tags should be placed as early as possible in the supply chain. Many supply chain benefits can only be realised with widespread item level tagging at the industry level, which still seems several years away for most companies. Consequently, bar code and RFID technologies will co-exist for many years to come, adding to supply chain cost, complexity and in some cases even confusion. With a rapidly evolving technology, current implementations and outlays on RFID technology may need complete replacement in the future, making integration an overwhelming task. Already, there are suppliers of RFID technology stuck with unsold inventory of products based on first-generation standards (The Economist, 2007).

RFID lacks the technical maturity and financial affordability necessary for a technology to be of any practical value in today's global supply chain. Impediments are slowing down the adoption rate. RFID in supply chains is an example of a system with network externality where the value of the technology increases with an increase in the number of firms implementing RFID in their supply chains. Both Wal-Mart and the US

Department of Defense have significantly scaled back their initial optimistic forecasts. The intent of this paper is to discuss the critical issues necessary for RFID implementations to succeed in supply chain management. We take a comprehensive look at questions concerning cost, technology, standards, privacy and security and business process reengineering, factors considered important for meaningful RFID implementations in the consumer products good industry and retail organisations (Bolotnyy and Robins, 2007). *It is hoped that stakeholders may find opportunities to influence these factors in future developments*.

2 Cost

By far, the biggest obstacle RFID faces is the cost. In the past, cost has been found to be a significant barrier in the adoption of many interorganisational systems like electronic data interchange (Premkumar and Ramamurthy, 1995). For a typical Wal-Mart supplier, estimates of total investment required for the RFID mandate vary significantly between $9–$25 million depending on the scope of the project (Overby, 2004; Shutzberg, 2004). Most of the RFID related costs become interdependent over the supply chain, often involving hundreds of businesses. While the US Department of Defense is willing to bear all the RFID related expenditure, major retailers are against any such cost sharing arrangements related to tagging and tags. Forcing major costs onto the suppliers does not provide for a fair and conducive situation. Many suppliers consider their RFID investment as a waste of resources with no immediate return. Major cost of a RFID system is due to tags, readers, network infrastructure and hardware to print and apply the labels, middleware to manage data flow, integration of RFID technology with other business processes, consulting and finally training and change management.

2.1 Tag cost

Tag cost is a significant component of total cost of RFID implementations (Bolotnyy and Robins, 2007). Even though the prices have come down within the last few years, still at 10–40¢ a tag, most companies are still hard pressed to justify the investment (The Economist, 2007; Schuman, 2006). At these prices, not only do the applications get limited, but just the tag cost can run into millions of dollars each year for a manufacturer. A price of 5¢ a piece was often cited as a tipping point for item level tagging (Sarma, 2001). A 5¢ a tag is a possibility once the annual demand reaches tens of billions and with wider adoption (a trillion tags a year) tag price is likely to drop to a penny. Other factors affecting the cost of a tag are chip type, antenna design and the technology. About 60–80% of the total tag cost is due to the silicon chip. Reducing chip size (ultra small chips) reduces cost, but makes assembly more expensive. Nonetheless, chip manufacturers are developing novel assembly techniques such as fluidic self assembly (FSA) which when used with very large production volumes will bring down the cost of a tag considerably.

With respect to chip type (material) and antenna design parameters, there is a price and performance trade-off. Typically, the RFID chip (a silicon integrated circuit) is joined to the antenna (typically made of laminated copper substrate) and then set as an inlay between layers in a pressure sensitive assembly. The inlays can then be placed on a polymer tape substrate and delivered to manufacturers in reels where the pre-made inlays

are converted into labels. This is an expensive and time consuming process to manufacture a tag. A promising low-cost alternative to the silicon tag is the chipless technology (Das, 2006). Instead of silicon, a chipless tag utilises technologies based on different materials such as polymers, fibres, thin films and specially formulated inks for printing. It is easier to apply these tags to metal or products containing liquids, whereas the chip-containing tags are somewhat problematic in such situations. Printed electronics can also be utilised for producing the tag's antenna instead of the commonly used copper. Ultimately, printed electronics could be utilised to print the complete RFID tag directly on the products and packages. While chipless tags have the potential to offer huge price advantage over the silicon based tags, current designs offer limited functionality in terms of storage capacity, reading ranges and reliability required for supply chain applications. Another recent development with applications to low cost disposable RFID tags is the paper based transistors in which both sides of the paper are coated with metal oxides (Fortunato et al., 2008). What is unique about this development is the use of paper both as a flexible substrate and as a dielectric layer. *Clearly, major technological breakthroughs and innovation in the design and production of low cost tags are crucial before RFID deployment moves into the realm of economic feasibility*.

2.2 Reader cost

Tracking individual items in the supply chain will require a large number of RFID readers. These units will have to be located at several strategic locations such as in manufacturing, shipping, sorting and retailing to provide the needed visibility. Often multiple readers are necessary at each gateway to ensure 100% read rates. A reader can cost anywhere from $800–$2,000, though the price is expected to decline as tag production picks up in the coming years, with the prediction of it dropping to $100–$200 with widespread RFID adoption (Trebilcock, 2007). A variety of different reading systems and technologies exist today such as handheld, fixed location, doorway, forklift, multi-protocol, multi-frequency. The new generation of electronic product code (EPC) compliant readers called 'agile reader', incorporates radio, computing and networking capabilities. These units use modular architecture and offer the flexibility needed to operate with different tag protocols and to protect against future obsolescence. In the EPCglobal Network (EPCglobal's RFID infrastructure), companies may be required to handle multiple tag protocols in the future. Agile readers can be upgraded and reconfigured as frequency, protocol and other requirements change. In addition, these units are scalable and have the ability to turn off the tags that have already been read. A full deployment of RFID throughout the supply chain will require hundreds of readers and will be a major investment.

2.3 Data management cost

Another major area of expenditure is the software and the related services to handle data from the RFID readers. RFID middleware is a key part of this software and manages the data flow from the readers to applications software by consolidating, purging, filtering and formatting the tag data so that it can be processed by systems like enterprise resource planning (ERP), advanced planning and scheduling (APS), warehouse management system (WMS) and transport management systems (TMS). Most RFID middleware applications include an edge server for managing the RFID readers and an application

programming interface (API) for integration with enterprise applications. Like many other RFID components, middleware costs also vary over a wide range, from $25,000 to several thousands for an enterprise wide system (Shutzberg, 2004). The cost also depends upon the number of edge servers or the number of readers in the system. RFID middleware is going through rapid development and as its capabilities improve, it is expected the costs will also increase.

Integrating all the databases with various enterprise applications and reengineering the business processes will require a lot of consulting services. These fees could quickly add up to become a significant portion of the RFID deployment. As was witnessed during the ERP implementations, consulting is not cheap and it quickly adds up to become a significant component of total cost. In the case of RFID implementations, consulting expenditure is likely to be spread over several years. Finally, most large projects of this magnitude have a history of often finishing late, over budget and generally fail to deliver the expected benefits.

3 Technology

While significant advances have been made in RFID technologies during the past few years, its implementation in supply chain still faces some major technological problems. Foremost among them are problems pertaining to signal distortion, reader accuracy and scalability all of which can lead to imprecise tracking of products in the supply chain. A perfect read rate (or close to it) is necessary for two important reasons. First, it is required before they can be used to replace the bar codes (accuracy of more than 99%) and second, most supply chain benefits are directly linked to the precise real-time tracking of the products in supply chain (Srivastava, 2004). Many ongoing pilots have been plagued by poor read rates with read accuracy ranging from as high as 99% for pallets to as low as 66% for cases on a pallet (Ferguson, 2007; Loebbecke, 2007). Inconsistent performance and reliability have been major issues since the beginning of the RFID experiments in supply chain, additionally, getting validation from recent pilots is also getting more difficult (Schuman, 2006; Ferguson, 2007).

Poor read rates are due to many factors. Ultra high frequency radio waves are deflected and/or absorbed by many liquids and metals making the accurate reading of the tags on many products a technical challenge. The magnitude of interference from liquids depends upon its viscosity. In such situations, companies have devised a workable solution by repositioning the tags on the products. For example, tags on bottles containing liquid products are placed on the plastic caps or near the top of the bottle where the interference is the least. In the case of metals, insulators are inserted between the tag and the metal surface on which the tag is to be mounted.

Each frequency range is susceptible to different types of interference. Low and high frequency tags work better on products containing liquid or metal, however, the focus of EPCglobal is on ultra high frequency tags. In simple terms, the space around the antenna can be divided into two regions, a near field (magnetic) and a far field (electromagnetic). Low and high frequency systems are short range systems and utilise the near field, whereas ultra high frequency and microwave systems are long range systems and utilise the far field (Nikitin and Rao, 2007). A near field ultra high frequency RFID system addresses many of the short comings of item level tagging due to liquids and metals. It is an area that is being investigated for supply chain applications. Another way to improve

reliability is to put multiple tags on an item. Bolotnyy and Robins (2007) found that placing multiple tags on an object improved read reliability significantly. It is important to underscore that fundamentally, the physics of RFID technology doesn't permit for 'one-size-fits-all' approach.

Being able to read multiple tags quickly is very desirable; however, it can also cause collision. Tag collision occurs when several tags respond to the reader at the same time. This happens when there are many tags present in a relatively small area. Likewise, collision also occurs when a signal from a reader interferes with signals from other readers. This interference is called reader collision. When this happens the tag is unable to respond to simultaneous queries by multiple readers. Collision also results in degraded performance. Anti-collision algorithms enable the readers to separate multiple tag signals and do it fairly well (Jain and Das, 2006). However, it still does not guarantee 100% read rates and usually delays the response.

An IBM study on the Wal-Mart deployments discovered that RFID systems can easily be disrupted by interference from walkie-talkie, forklift, electric motors, computing equipment, high frequency machine noise, wireless networks, cell phone towers and even lighting fixtures (Sullivan, 2004). This type of disturbance is often present in several places where RFID systems are going to be installed such as factory floors, warehouses, distribution centres and retail stores. Other factors such as temperature, humidity, ambient radio noise, object density and placement geometry can also adversely affect read rates (Bolotnyy and Robins, 2007).

RFID tags and readers along with other EPCglobal Network infrastructure are prone to failures. In fact, in their study of multiple tagging, Bolotnyy and Robins (2007) discovered several defective tags (due to manufacturing or transportation) during the programming phase of their experiments. Additionally, they also discovered significant differences in performance among identical tags. Tag performance also degrades after every read attempt. As RFID deployments grow, there are several scalability questions related to the system architecture. Limitations may be due to hard constraints built into the system or simply the negative effect of an overwhelming number of tags and readers in the system on the network and software applications. Many ongoing pilots have limited scalability.

While a viable solution to circumvent many of the above problems can certainly be devised on a situational basis, clearly, RFID technology lacks the robustness necessary for heterogeneous open supply chains that span through several regions of the world, carrying a variety of products made from different materials and passing through range of diverse facilities. There is ongoing research in this area to understand and overcome the current shortcomings of the RFID technology.

4 Standards

Creating a set of open global standards is a fundamental issue facing RFID implementation in supply chains. Standards are required for several elements of a RFID system such as tag specifications, allocation of frequencies, communication equipment, middleware, back-end processes, data handling and specifications for business process integration. Many RFID systems in use today are based on the vendor's own proprietary systems. Proprietary implementations lead to protocol incompatibility between various systems. This can be detrimental to the widespread acceptance of the technology and may

ultimately limit the level and scope of RFID deployments. Lack of standards also slows down the development of new products and systems and makes planning a difficult task. As noted by Curtin et al. (2007), standards will play a major role in RFID adoption and benefits. Standards bring transparency and are a prerequisite for technical maturity and affordability. Ideally, standards should be open, global, non-proprietary and built on sound scientific/engineering principles, with reusable components. Standards should not impede competition; rather it should promote innovation, growth and expanded access. Once developed, the standards need to be adopted rapidly by the trading partners to enable seamless flow of data across the supply chain.

4.1 EPCglobal and RFID standards

In an era of global manufacturing and sourcing, differences in radio regulations around the world make it difficult for companies to have a uniform RFID infrastructure across the world. Definition of UHF spectrum in the USA is different from the one in Europe and in some other countries. This undermines the effectiveness of the technology and increases the complexity and cost of the RFID system. Basically, there are two parts to this issue, the allocation of the radio frequency spectrum by the governments and the standardisation of RFID communication systems (such as power levels for tags). Global interoperability is EPCglobal's key charter. It is developing and promoting open global standards for RFID technology in supply chains and coordinating it closely with several organisations and countries worldwide.

Incorporating the EPC standards into the International Standards Organization (ISO) is essential to make the standards truly global. For example, in the past, UHF Class 0 and Class 1 specifications ignored global operability and could only be sourced from a handful of suppliers. In 2006, ISO approved EPC Generation 2 Class 1 UHF standard as ISO 18000-6C to ensure global interoperability. In the future, EPCglobal will likely expand generation 2 tags to include higher classes of tags. In general, a number of standards already exist or are at the developmental stage. Standards such as ISO 18000 (air interfaces), ISO 15962/15961 (readers and data protocol standards) have already been published, whereas standards like ISO 24791 (software system infrastructure) and ISO 24753 (air interface commands) are in the developmental stage. EPCglobal has also ratified the electronic product code information services (EPICS), a standard that provides a common language for exchanging data recorded on RFID tags.

4.2 Intellectual property

Related to the standards is the intellectual property (IP) rights issue. Over the years, several companies (including EPCglobal members) have invested heavily in the development of RFID technologies and products, which are often protected by one or more patents. Initially, EPCglobal required its members to license the use of specifications to which they have contributed on a royalty-free basis. While this is a very worthwhile policy, nevertheless it has raised several questions and led to lawsuits involving patent infringements. EPCglobal strongly discourages standards based on IP that is not available on a royalty-free basis. Under this policy, the standards may often turn out to be less than ideal or may involve considerable work designing around the patents. In light of recent litigations and in an effort to create more advanced and cost effective standards, EPCglobal now allows standardising on patented technology that is

not available on a royalty-free basis. It has modified its IP policy to include licensing of patented technology on a fair, reasonable and non-discriminatory (RAND) basis. This policy is not unusual for standard setting organisations and is consistent with ISO's IP policy. In any case, EPCglobal needs to articulate a more coherent IP policy or it risks getting mired in time consuming proceedings which may delay the development of standards and undermine innovation. Interoperability between different manufacturers is essential and this may require cross licensing or similar agreements. It is worth noting within the last decade, the role and the management of IP in the IT and telecom industry has undergone a fundamental shift. Lastly, the pace of technological development puts added pressure on EPCglobal as new RFID technology is being designed and tested as much as it is being selected for standardisation.

4.3 Global implications

A number of countries like China, Korea and Japan are working towards developing national RFID standards and in doing so, are collaborating with international organisations. The level of interoperability between different standards remains to be seen. For example, if countries have already designated certain frequencies for other uses, it cannot be easily changed or taken back. In China, the frequency bandwidth designated for RFID systems is utilised for wireless telecommunication, radio broadcasting and aerospace communications (Bremner, 2006). China is also keen on developing its own RFID standards and is somewhat reluctant to pay royalties to enterprises outside China on a technology that will have such a ubiquitous presence in its trade (Harmon and Downey, 2005). It has already developed its version of the EPC numbering system called the national product code (NPC) and intends to develop its own product-information registry which organisations like EPCglobal can access for a fee. A proliferation of standards could mean a serious setback for global implementation of RFID technology. Certification of international standards is of utmost importance if RFID has to be effective in global supply chain management, unfortunately it is also quite time consuming. As standards evolve from emerging to enabling, one is likely to see many changes taking place in the existing RFID infrastructure.

5 Privacy and security

Without any safeguards in place, RFID technology has the potential for compromising consumer privacy and security. The uniqueness of the electronic product code erodes the ability of consumers to remain anonymous. Information on the tag could also be linked to personal identity. On the privacy front, the main concern centres around the possible misuse of RFID collected data and fears of surveillance after the purchase, as the tag may continue to emit signals (if interrogated) containing information. Companies can get valuable insights into the buying habits of the consumer by mining the data collected over a period of time. This information could be subjected to scrutiny or be traded to other parties. Moreover, by matching this information with other databases a much more comprehensive consumer profile can be constructed. Tagged products on a consumer can also be used by criminals to identify possible targets or by agencies to identify and track the whereabouts of certain citizens. For retailers, in-store monitoring of consumers with tagged products provides added insights into consumer behaviour and permits more

direct marketing at customers as they walk through the store. Although, it seems that in some way, it is our civil liberties that are under threat, currently, almost all of our personal data and buying patterns are accessible through credit cards and various loyalty card programs. Moreover, in certain parts of the world, mobile phones, GPSS technology and CCTV systems make it possible to track individuals virtually anywhere and the general public doesn't seem to mind.

In the past, some of the leading proponents of RFID technology are known to have clandestinely conducted RFID pilots in the retail stores. In their book *Spychips*, Albrecht and McIntyre (2005) discuss some alarming patent filings that threaten consumer privacy. There have been several protests worldwide from consumer groups forcing many companies to scale back their RFID deployments. A number of consumer groups like Consumers against Supermarket Privacy Invasion and Numbering (CASPIAN) have been fairly active in bringing these issues to the forefront. While some of the consumer fears are genuine, others may be related to a consumer's perception of RFID technology, poor communication and lack of trust.

The tags likely to be used in supply chains do not contain a lot of information. However, the low cost nature of the EPC tags limits the computing power and hence is unsuitable for sophisticated encryption or any other meaningful security measure. Tags can only be read from a few metres, thus tracking consumers over a wide geographical region is a not a possibility, at least in the foreseeable future. However, even tags with cryptographic protection, emit unique identifiers on interrogation and are vulnerable to a variety of clandestine threats. RFID readers would be easy to come by and are small enough to be hidden in a cell phone. Currently, the only true protection that EPCglobal offers against privacy is the ability to kill the tag at the point of sale. However, this also limits the potential uses of the tags after the sale such as after-sales-service or returns.

Privacy issues relate to many RFID applications. However, most are associated with item level tagging, widespread adoption of which is still several years away. With the current focus on pallet and case level tagging, privacy and security issues are not what businesses are struggling with. The Electronic Privacy Information Center (www.epic.org) classifies privacy in four areas: information, bodily, communication and territorial. In someway, RFID impacts all four of them. Globally, the legal and regulatory standards on privacy differ widely between countries. Both the European Union and EPCglobal have created advisory groups within their organisations with the objective of initiating a public dialogue on this topic. The European Union through its data protection directive has some of the toughest privacy and data protection laws, which are also applicable to RFID applications. Historically, privacy laws have almost always been enacted in response to technological developments (Regan, 1995). In 'An RFID Bill of Rights', Garfinkel (2002) strongly suggests that the industry should not indulge in any surreptitious activity where consumer privacy is compromised. Adherence and promotion of the privacy guidelines by various stakeholders will go a long way in preventing costly mistakes.

RFID is an evolving technology and new developments create new privacy concerns. Though still in the early stages of development, wireless sensor networks could potentially have a big impact on RFID technology in the future (Warneke et al., 2001). These networks (also known as motes and smart dust) are a collection of chips that communicate wirelessly with each other and often self-organise after being deployed in an ad hoc manner. These chips can also be RFID tags which can then communicate with each other. From a privacy perspective, the network can then be used to track people with

RFID tagged products over a wide geographical area. Whether new developments become practical or not is a different matter, the policy makers definitely need to keep themselves abreast of it.

5.1 Counterfeiting and other security concerns

RFID tags are also vulnerable to counterfeiting and theft. Scanning the RF signals from the tags and then simulating the behaviour of these tags using RFID simulation devices can be done. A team of researchers at John Hopkins University and RSA Laboratories were able to expose a security weakness in the cryptographically enabled RFID tags used widely in securing vehicles against theft and in ExxonMobil's SpeedPass system designed to prevent fraudulent transactions (Garfinkel et al., 2005). The team was able to successfully simulate the tags by breaking the 40 bit cryptographic code found on them. Research into a number of security measures such as encryption, tag passwords, pseudonyms and blocker tags is underway to address some of the privacy and security concerns (Kharif, 2006). A blocker tag prevents unauthorised scanning of a tag by transmitting more data than the reader is capable of handling – an equivalent of a denial-of-service attack. A group of researchers in Amsterdam have created a device called RFID Guardian (a handheld device) that can prevent RFID tags from being read (a firewall for the tags) (Rieback et al., 2006).

The global and networked nature of today's supply chain exposes the EPCglobal Network to various threats and attacks by various criminals including malicious hackers making them highly vulnerable. A single breakdown in one network can cascade through and between the networks causing major disturbances throughout the EPCglobal Network. The wireless nature of the technology adds to its vulnerability in terms of malicious security attacks such as eavesdropping, intercepting and modification of the transmitted data. RFID tags can also be infected with a virus which can then spread to other areas of the system (Rieback et al., 2006). Globally securing the critical RFID infrastructure and providing a secure mode to collaborate and exchange data is a major undertaking, it is also a basic prerequisite for RFID technology.

5.2 Data-sharing risk

RFID systems will gather and store vast amounts of data, keeping it secure at all levels is an enormous undertaking. Seamless integration of business processes allows for flow of critical business information across the supply chain. These systems also penetrate the critical processes of supply chain partners such as WMS, ERP and TMS. There is considerable risk from the amount of data that is going to be shared across the EPCglobal Network and stored in several hubs/locations around the world. Corporate espionage through product tracking or information gathering is a real possibility. Implementing RFID technology requires significant business process reengineering which by its inherent nature carries security risks. It is of utmost importance that EPCglobal develop sound security and data protection measures. What makes this a difficult task is determining the security risks that the EPCglobal Network will be exposed to in the future and how to mitigate them. Identifying and quantifying the security risks in supply chains will be the key to developing effective risk management strategies to mitigate the threats. EPCglobal should document and track all the security breaches in the network and share the information with other companies (probably anonymously). This

information can also be used for security benchmarking, etc. Overall, it is important to make the EPCglobal Network as secure as possible – major security breaches can lead to serious setbacks and problems including litigation and legislation.

5.3 Security lessons from e-commerce

Many of the techniques deployed in the internet for security purposes (such as encryption, firewalls, intrusion detection, virtual private networks and authentication) can also be used for RFID technology. However, even some of the so called 'secure systems' have found themselves less than impervious to such attacks. In a major attack on key computers that manage the flow of global internet traffic, hackers were able to overwhelm the computers with enormous amount of data that threatened to choke the flow of data (Bridis, 2007). Surprisingly, the attacks were fairly powerful and lasted for 12 hours. Cukier et al. (2006) report that hackers typically use a 'dictionary script' that run through a list of commonly used usernames and passwords to break into thousands of computers connected to internet at a time. Hacked computers are then setup to become a part of botnet (a collection of hacked computers) that can be run remotely by the hacker to commit other frauds.

The new breed of criminals is involved in a variety of criminal activity including phishing, network sabotaging, threatening a web site with denial of service attack unless it pays a ransom and surreptitiously installing a spyware on the computers to secretly obtain the passwords and account details. The speed with which the stolen information is converted into monetary gains points to the emergence of an elaborate infrastructure of sophisticated cyber criminals, interested more in profiting from their crimes than in simply creating havoc on the internet like the earlier hackers. These criminals have also added a global dimension to their activities.

Security is an ongoing issue and should be evaluated frequently, regular certification and compliance should be strictly enforced. Poor compliance is often the reason for laptops containing sensitive data being stolen or backup tapes gone missing. The *Wall Street Journal* reported that a key hash function routinely used in encrypting sensitive information (credit card numbers, social security numbers, etc.) in online transactions is less resistant to attacks by hackers than had been originally thought (Forelle, 2005). Increasingly, the hacking community is developing malicious software (malware) that is hard to detect and remove from computers/networks (Vijayan, 2006). Techniques such as code mutation evade detection by signature-based malware blocking tools. Once installed on a system, these programs split themselves into several co-dependent fragments where each fragment keeps track of others. When an attempt is made to remove a component, other fragments combine to reinstall it. Several spyware programs also use sophisticated methods such as kernel-level drivers and process blocking routines to prevent anti-spyware routines from running.

Security measures need to be designed carefully. In an effort to limit copying of its CDs, Sony Corporation embedded copy-protection software XCP on its CDs. However, the software has had several disturbing lapses. XCP creates a way for viruses to go undetected into the computer's operating system. XCP constantly monitors the CD-ROM drive making the computer more prone to crashes (Graham, 2005). A similar security flaw was again discovered in a Sony product, this time in its micro vault USB memory sticks (Sanders, 2007). As a result, the company had to phase out this product line.

While no amount of safety can fully guarantee the security of a system, minor breaks in security are likely to occur over a period of time in a complex network like the EPCglobal Network. Herrmann and Herrmann (2006) describe a useful framework called $MoSS_{BP}$. It specifies the security requirements for business processes, repositories of various mechanisms enforcing security requirements and a collection of reference models and case studies enabling the modification of the business processes.

6 Business process reengineering

Clearly, adopting the RFID system will be disruptive to many of the existing business processes. RFID technology brings real-time data, speed and connectivity to supply chains. Companies that share and process information in real-time across the supply chain are in a better position to respond to changes in the marketplace (Barratt, 2004; Cachon and Fisher, 2000). This also mitigates the impact of bullwhip effect in supply chains (Lee et al., 1997). However, utilising real-time data requires reengineering the supply chain processes. In fact, the accuracy, the speed and the reliability of RFID collected data directly impacts some of the critical areas targeted by many companies for improvement such as demand management, planning and forecasting and order management. Reengineering the supply chain is also an opportunity to carry out some major process improvements and boost profits by as much as 150–250% (Handfield and Nichols, 2002).

More than 85% of the senior executives responding to a survey said that improving supply chain performance is one of their top priorities (Cook and Hagey, 2003). For most companies, realising gains through supply chain improvements in the extended enterprise is largely untapped. In a survey of key challenges in manufacturing by BearingPoint (2007), less than 25% of the respondents rated their firm's capabilities in critical supply chain areas (such as logistics, transportation, warehousing, purchasing, supply chain planning) as very good to excellent. One of the reasons for this rather disturbing finding is the fact that supply chain processes have simply not evolved with changing needs of the marketplace. Poorly performing supply chains pay a hefty price in terms of shareholder value and profitability. Hendricks and Singhal (2002) show that on an average supply chain disruptions lead to a 107% decrease in operating income, 7% lower sales growth, 11% increase in cost, a 14% increase in inventories and a 33–40% decline in stock returns over a three-year period. It is therefore essential that companies meet these challenges in ways that continue to increase value for their stakeholders.

Often reengineering and IT are closely linked together. The last 15 years have seen significant BPR in supply chain management largely because of technological developments. IT has enabled major collaborative supply chain ventures like collaborative planning forecasting and replenishment (CPFR), vendor managed inventory (VMI) and customer relationship management (CRM). Such ventures are also fraught with challenges for they are complex, expensive and inherently risky as they often require significant changes in business processes (Clark and Lee, 2000). Over time, many reengineering projects have fallen short of expectations; Hammer and Champy (1993) claim that 70% of the companies fail to realise any benefits from their reengineering projects. In another study conducted by Booz Allen and Hamilton, nearly 45% of the respondents said that IT in supply chain has failed to live up to its expectations (Heckmann et al., 2003). Despite such discouraging facts and statistics, technology

continues to have an enormous impact on supply chain management and RFID is one of them.

6.1 Issues in reengineering RFID supply chains

Lately, BPR is again gaining momentum – this time to improve the coordination in global supply chains by integrating and optimising business processes across organisations. In principle, this effort is similar to the reengineering work required to integrate RFID technology in supply chains. However, several factors complicate BPR as never before. Many companies are jumping into RFID applications before fully understanding the cost implications, technology roadmaps and business requirements both internal and external to the organisation. BPR efforts will inevitably be hampered by a lack of understanding and commitment to support changes in the supply chain. Some of these are discussed next.

The presence of disparate information systems and diverse business practices across organisational and geographical boundaries make BPR a very labour intensive and expensive undertaking. Internally, supply chains with fragmented logistical and distribution networks lack the basic infrastructure and readiness required for transferring and sharing data in an extended enterprise (Prahalad and Krishnan, 1999). One of the biggest challenges that managers find in reengineering supply chains is the integration of dissimilar IT systems and processes (BearingPoint, 2007). In a supply chain with global dimensions, the presence of multiple disparate systems with limited connectivity is common.

Despite its importance and its positive relationship with improved performance, collaboration among supply chain partners continues to face plenty of resistance. Sharing critical and confidential data across organisational boundaries requires trust and a fundamental shift in the relationship amongst the supply chain partners. In a survey by Kurt Salmon Associates (2002) for Grocery Manufacturers of America, retailers expressed a fundamental lack of trust in developing a true partnership with their vendors. Clark and Hammond (1997) echo a similar opinion and point to the existence of an 'adversarial win-lose' relationship in supply chains. Lack of trust can lead to communication delays, inconsistent information, high administrative costs and ultimately poor decision making. CPFR projects were delayed by several years, in part due to the unwillingness of companies to exchange critical data and construct joint business plans. It is no secret that managers charged with implementing such projects encounter numerous obstacles both internal and external to their organisations. As outsourcing grows, trust, commitment and good supplier relationships are essential for supply chain to be competitive (Morgan and Hunt, 1994). Trust is central to any long-term collaborative relationship where risks, uncertainty, shifts in power and fears of opportunism are present.

Reengineering RFID technology in supply chain management will require a paradigm shift in attitudes towards collaborative endeavours. Many highly regarded companies still have a lot of work to do in developing a truly collaborative partnership. Strategic alliances and partnerships are pursued on a very selective basis (Fawcett and Magnan, 2002). Furthermore, unlocking the potential of RFID technology requires firms to deepen the integration process and carry out BPR in ways that facilitates collaboration across multiple domains and supply chain networks. In many ways, this requires the support of

the entire industry and complicates BPR both from a technical and a practical standpoint. On the other hand, it will end up making collaborative technology more efficient.

In an effort to help firms in their BPR endeavours, EPCglobal should develop a roadmap based on the assessment of the current landscape of global supply chains in terms of maturity of business processes, IT and technological capabilities and organisational needs and capabilities of trading partners. The roadmap must set the scope of supply chain integration, identify the path to the future, the technological advances and the barriers likely to be encountered. The technological capabilities of RFID systems are dependent upon a host of other systems where the technology and even the standards are still being developed. Not only is RFID technology in supply chain an evolving technology, software applications which support BPR and form the foundation of an integrated supply chain are in the early stages of development and testing. RFID implementations and its reengineering are likely to be phased out over several years. All of this creates a lot of uncertainty. Projects of this nature are fraught with unforeseen problems, delays, technical glitches and unexpected expenses.

BPR should be carried out in a way that the RFID infrastructure is capable of expansion and assimilating new developments in the future. Developing flexible and responsive systems will be the key to enabling different supply chains processes to work together in an era of globalisation, industry mergers and rapid technological innovation which may be disruptive at times. There will be huge technological challenges in terms of security, scaling, application interfaces, data access and support. Many new applications and systems would have to be developed, supported and maintained over time. In large scale RFID deployments, standardisation of processes across enterprises in supply chains will go a long way in developing efficient and robust RFID systems on a global basis. It will also help EPCglobal at a later time as it attempts to expand the scope of RFID technology, either in the context of supply chain management or in serving other related markets.

Adopting leading edge techniques in integrating business processes across multiple supply chains can bring significant analytical rigor to BPR. A methodology based on critical success factors as investigated by Quesada and Gazo (2007) can be used for identifying critical business processes that need to be mapped out and reengineered first. In constructing process maps of supply chain networks, one needs to consider workflow merge and methods for merging business processes across firms. Examples of merge methods include sequential, parallel, conditional and iterative. A framework suggested by Sun et al. (2006a) can help managers perform simulations to visualise different merges for business processes. This can help in creating flexible processes and planning merges that allow for software agents to share process knowledge. Their work also includes algorithms for grouping merges. Accurate workflow modelling and analysis requires syntactically correct process sequence and anticipated data-flow specifications. Data-flow anomalies (such as missing data, redundant data or potential data conflicts) can be detected using the methodology suggested by Sun et al. (2006b).

6.2 BPR lessons from VICS, SCOR and RosettaNet

As EPCglobal looks at these and other challenges, it can draw upon the motivation, experience and lessons from other interorganisational supply chain implementations such as Voluntary Inter-industry Commerce Standards Association (VICS), Supply Chain Council (SCC) and RosettaNet.

In 1998, VICS set up a committee to identify a set of business processes and design guidelines for CPFR – a major supply chain initiative in recent years to improve the collaboration between customer demand and replenishment strategies across the supply chain (www.vics.org). The committee developed a generic CPFR process model based on a successful collaborative project between Wal-Mart and Warner-Lambert with assistance from Surgency, SAP and Manugistics. The proposed guidelines for CPFR are designed to facilitate the reengineering of the replenishment process between the trading partners. It includes details on supporting technology, process definitions, data content and format, metrics, communications systems, security procedures and a roadmap for implementing CPFR along with change management issues. VICS's involvement and development of the CPFR process model has been a key to CPFR's success. It continues to be the leading methodology for CPFR implementations. In the past, VICS was also involved in developing standards for bar codes and EDI.

The supply chain operations reference (SCOR) model developed by SCC can also be used as a basis for configuring and integrating business processes across the supply chain (www.supply-chain.org). SCOR combines elements of BPR, benchmarking and leading practices into a single framework. It is built around five core business processes: plan, source, make, deliver and return and covers key supply chain activities from the supplier's supplier to customer's customer. Each of these processes is further examined in detail at three levels during the reengineering exercise. The model contains standard descriptions of business processes, a framework of relationships among the processes, metrics to measure the performance and best practices. It also provides a roadmap for managing supply chain projects. SCOR has been used by several companies such as IBM, HP, Coca-Cola, Intel and Siemens to evaluate their supply chain processes. Imation, the technology spun off from 3M, has used both CPFR and SCOR together to improve its collaborative supply chain processes (Lohse and Ranch, 2001). Companies like SAP have started incorporating the SCOR model and metrics in their supply chain software. In fact, the SCOR model has been an impetus to companies to create similar processes in areas such as product development, customer relationship management, finance, accounting and human resource management (Davenport, 2005). One of the biggest implementations of SCOR is at the US Department of Defense.

RosettaNet (www.rosettanet.org), a consortium of major electronics and telecommunications companies, is working since 1998 to create and implement industry-wide e-business standards for aligning supply chain processes between various links in the supply chain, including manufacturers, distributors, resellers and customers on a global basis. RosettaNet standards provide for standardised business content and processes to improve supply chain reliability, flexibility and responsiveness. Standards include data dictionaries, implementation frameworks, business message schemas and process specifications for e-business standardisation. Business processes are aligned through partner interface processes (PIPs) which allow for automated exchange of real-time data between trading partners. Each PIP specification includes a business document and a detailed business process that includes interaction, data transmission, security and error-handling requirements. PIPs are tested and voted on by the consortium members before releasing it for general use. Implementing PIPs requires BPR, as PIPs specify processes only at the interface between trading partners. Deriving full benefit requires aligning the internal processes as well. Since its introduction, RosettaNet enabled e-business standards have led to significant improvements in operational efficiencies across many high-tech supply chains.

A detailed study of these three interorganisational systems should provide valuable lessons and opportunities to improve RFID implementations in supply chains.

7 Conclusions

With all the hype surrounding RFID, the focus of this paper has been to highlight the level of 'readiness' of RFID technology by underlining the major issues facing many companies. The push to implement RFID technology appears to be driven more by major retailers and government and not by consumer goods manufacturers. While there is no doubt that RFID technology presents new opportunities to improve retail supply chains, given the present state of technology and knowledge, it is highly unlikely that many of the RFID benefits are realisable in the near future. In the short-term, firms may end up adopting RFID technology out of strategic necessity. The technology needs to be viewed with a caution. Many shortcomings and risks are often overlooked when trying to compress the time schedule, thereby increasing the odds of making mistakes and ill-informed decisions. It has the potential to disrupt the functioning of a well-run company in the short-term. From a managerial perspective, the critical task facing many companies is how to begin systematising and implementing RFID technology. Companies should carefully assess the viability, risk, potential benefits and the impact of RFID technology on the industry and supply chain management. Often, managers fail to take prudent measures in assessing and managing risks associated with major IT projects. It is therefore imperative that RFID projects be prioritised, closely monitored and key deliverables be clearly identified. Good communications and a shared understanding of the technological landscape between the trading partners are essential for RFID to succeed in supply chain management.

References

Albrecht, K. and McIntyre, L. (2005) *Spychips: How Major Corporations and Government Plan to Track your Every Move with RFID*, Thomas Nelson, Nashville, Tennessee.

Angeles, R. (2005) 'RFID technologies: supply-chain applications and implementation issues', *Information Systems Management*, Vol. 22, No. 1, pp.51–65.

Barratt, M. (2004) 'Unveiling enablers and inhibitors of collaborative planning', *International Journal of Logistics Management*, Vol. 15, No. 1, pp.73–91.

BearingPoint (2007) *Vision 2007: Key Challenges in Manufacturing*, available at http://www.bearingpoint.com/Documents/StaticFiles/c3908_Vision2007_execsum.pdf.

Bolotnyy L. and Robins, G. (2007) 'The case for multi-tag RFID systems', *Proceedings of International Conference on Wireless Algorithms, Systems and Applications*, Chicago, IL.

Bremner, B. (2006) 'Radio-frequency ID: Asian impediments', *BusinessWeek Online*, 9 October.

Bridis, T. (2007) 'Hackers attack key net traffic computers', *The Washington Post*, 6 February.

Cachon, G. and Fisher, M. (2000) 'Supply chain inventory management and the value of shared information', *Management Science*, Vol. 46, No. 8, pp.1032–1048.

Clark, T.H. and Hammond, J. (1997) 'Reengineering channel reordering processes to improve total supply chain performance', *Production and Operations Management*, Vol. 6, No. 3, pp.248–265.

Clark, T.H. and Lee, H.G. (2000) 'Performance, interdependence and coordination in business to business electronic commerce and supply management', *Information Technology and Management*, Vol. 1, No. 1, pp.85–105.

Cook, M. and Hagey, R. (2003) 'Why companies flunk supply-chain 101', *Journal of Business Strategy*, Vol. 24, No. 4, pp.35–42.

Cukier, M., Berthier, R., Panjwani, S. and Tan, S. (2006) 'A statistical analysis of attack data', *Proceedings of Annual IEEE/IFIP International Conference on Dependable Systems and Networks*, Philadelphia, PA.

Curtin, J., Kauffman, R.J. and Riggins, F.J. (2007) 'Making the 'most' out of RFID technology: a research agenda for the study of the adoption, usage and impact of RFID', *Information Technology and Management*, Vol. 8, No. 2, pp.87–110.

Das, R. (2006) 'Chipless tags: the future of RFID', *Manufacturing Business Technology*, Vol. 24, No. 5, p.59.

Davenport, T.H. (2005) 'The coming commoditization of processes', *Harvard Business Review*, Vol. 83, No. 6, pp.1–8.

Fawcett, S.E. and Magnan, G.M. (2002) 'The rhetoric and reality of supply chain integration', *International Journal of Physical Distribution & Logistics Management*, Vol. 32, No. 5, pp.339–361.

Ferguson, R.B. (2007) *RFID Adoption is Lagging*, available at Eweek.com, (accessed on 8 January).

Forelle, C. (2005) 'Crack in computer security code raises red flag', *The Wall Street Journal*, 15 March, p.A1.

Fortunato, E., Correia, N., Barquinha, P., Pereira,L., Goncalves, G. and Martins, R. (2008) 'High performance flexible hybrid field-effect transistors based on cellulose fiber paper', *IEEE Electron Device Letters*, Vol. 29, No. 9, pp.988–990.

Garfinkel, S.L. (2002) 'An RFID bill of rights', *Technology Review*, Vol. 105, No. 8, p.35.

Garfinkel, S.L., Juels, A. and Pappu, R. (2005) 'RFID privacy: an overview of problems and proposed solutions', *IEEE Security and Privacy*, Vol. 3, No. 3, pp.34–43.

Graham, J. (2005) 'Sony to pull controversial CDs, offer swap', *USA Today*, available at http://www.usatoday.com/money/industries/technology/2005-11-14-sony-cds_x.htm, (accessed on 4 November).

Hammer, M. and Champy, J. (1993) *Reengineering the Corporation: A Manifesto for Business Revolution*, Harper Collins, London.

Handfield, R.B. and Nichols, E.L. Jr. (2002) *Supply Chain Redesign*, Prentice Hall PTR, Upper Saddle River, New Jersey.

Harmon, C. and Downey, L. (2005) 'RFID: will China throw a monkey wrench?', *BusinessWeek Online*, 12 September.

Heckmann, P., Shorten, D. and Engel, H. (2003) *Supply Chain Management at 21 – The Hard Road to Adulthood*, Booz Allen Hamilton, New York.

Hendricks, K.B. and Singhal, V.R. (2002) 'How supply chain glitches torpedo shareholder value', *Supply Chain Management Review*, Vol. 6, No. 1, pp.18–33.

Herrmann, P. and Herrmann, G. (2006) 'Security requirement analysis of business processes', *Electronic Commerce Research*, Vol. 6, Nos. 3–4, pp.305–335.

IDTechEx (2007) 'RFID is poised for a change', available at http://server2.idtechex.com/products/en/articles/00000771.asp.

Jain, S. and Das, S.R. (2006) 'Collision avoidance in a dense RFID network', *Proceedings of First ACM International Workshop on Wireless Network Testbeds, Experimental Evaluation and Characterization*, pp.49–56.

Kharif, O. (2006) 'What's lurking in that RFID tag?', *BusinessWeek Online*, 16 March.

King, R. (2006) 'Radio shipment-tracking: a revolution delayed', *BusinessWeek Online*, 9 October.

Kurt Salmon Associates (2002) *Survey of Supply Chain Effectiveness*, Grocery Manufacturers of America.

Lee, H.L. and Özer, Ö. (2007) 'Unlocking the value of RFID', *Production and Operations Management*, Vol. 16, No. 1, pp.40–64.

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

Liard, M.J. (2005) *The RFID Business Planning Service*, Venture Development Corporation, Natick, MA.

Loebbecke, C. (2007) 'Piloting RFID along the supply chain: a case analysis', *Electronic Markets*, Vol. 17, No. 1, pp.29–38.

Lohse, M. and Ranch, J. (2001) 'Linking CPFR to SCOR Imation's experience', *Supply Chain Management Review*, Vol. 5, No. 4, pp.56–62.

McWilliams, G. (2007), 'Wal-Mart's radio-tracked inventory hits static', *The Wall Street Journal*, 15 February, p.B1.

Morgan, R.M. and Hunt, S.D. (1994) 'The commitment-trust theory relationship marketing', *Journal of Marketing*, Vol. 58, No. 3, pp.20–38.

Nikitin, P.V. and Rao, K.V.S. (2007) 'An overview of near field UHF RFID', *IEEE RFID Conference*, Grapevine, TX, available at http://www.ee.washington.edu/faculty/nikitin_pavel/papers/RFID_2007.pdf.

Overby, C.S. (2004) *RFID at What Cost*, 1 March, Forrester Research, Cambridge, MA.

Prahalad, C.K. and Krishnan, M.S. (1999) 'The meaning of quality in the information age', *Harvard Business Review*, Vol. 77, No. 5, pp.109–118.

Premkumar, G.K. and Ramamurthy, K. (1995) 'The role of interorganizational and organizational factors on the decision mode for adoption of interorganizational systems', *Decision Sciences*, Vol. 26, No. 3, pp.303–336.

Quesada, H. and Gazo, R. (2007) 'Methodology for determining key internal business processes based critical success factors: a case study in furniture industry', *Business Process Management Journal*, Vol. 13, No. 1, pp.5–20.

Regan, P.M. (1995) *Legislating Privacy: Technology, Social Values and Public Policy*, University of North Carolina Press, Chapel Hill, NC.

Rieback, M.R., Gaydadjiev, G.N., Crispo, B., Hofman, R.F.H. and Tanenbaum, A.S. (2006) 'A platform for RFID security and privacy administration', *Proceedings of Large Installation System Administration Conference*, pp.89–102, available at http://www.rfidguardian.org/papers/lisa.06.pdf).

Riggins, F.J. and Mukhopadhyay, T. (1994) 'Interdependent benefits from interorganizational systems: opportunities for business partner reengineering, *Journal of Management Information System*, Vol. 11, No. 2, pp.37–57.

Sanders, T. (2007) 'Sony halts production of Rootkit USB sticks', *ITNEWS*, 3 September, available at http://www.itnews.com.au/News/60374,sony-halts-production-of-rootkit-usb-sticks.aspx.

Sarma, S. (2001) 'Towards the five-cent tag', *Technical Report, MIT-AUTOID-WH-006*, Auto-ID Labs.

Schuman, E. (2006) 'Major RFID hurdles ahead', available at http://www.eweek.com/article2/0,1895,1990814,00.asp (accessed on 20 January).

Shutzberg, L. (2004) *Scoping Out the Real Costs of RFID*, available at InformationWeek.com (accessed on 1 November).

Srivastava, B. (2004) 'Radio frequency ID: the next revolution in SCM', *Business Horizons*, Vol. 47, No. 6, pp.60–68.

Sullivan, L. (2004) *IBM Shares Lessons Learned from Wal-Mart RFID Deployment*, available at InformationWeek.com (accessed on 15 October).

Sun, S., Kumar, A. and Yen, J. (2006a) 'Merging workflows: a new perspective on connecting business processes', *Decision Support Systems*, Vol. 42, No. 2, pp.844–858.

Sun, S.X., Zhao, J.L., Nunamaker, J.F. and Sheng, O.R.L. (2006b) 'Formulating the data-flow perspective for business process management', *Information Systems Research*, Vol. 17, No. 4, pp.374–391.

The Economist (2007) *Radio Silence*, available at http://www.economist.com/science/tq/displaystory.cfm?story_id=E1_JNQJNSR (accessed on 7 June).

Trebilcock, B. (2007) 'Bringing down the cost of RFID infrastructure', *Modern Materials Handling*, available at http://www.mmh.com/article/CA6445606.html (accessed on 22 May).

Vijayan, J. (2006) *Mutating Malware Evades Detection*, available at PCAdvisor.co.uk (accessed on 11 November).

Warneke, B., Last, M., Liebowitz, B. and Pister, K.S.J. (2001) 'Smart dust: communications with a cubic-millimeter computer', *IEEE Computer*, Vol. 34, No. 1, pp.44–51.