3

The Role of RFID Technology in Supply Chain Risk Management

May Tajima
The University of Western Ontario
Canada

1. Introduction

Supply chain risks come in a variety of forms: disruptions to material flows, product quality problems, information systems breakdowns, and economic instability (Chopra & Sodhi, 2004; Zsidisin et al., 2000). The recent literature in supply chain management recognizes the importance of managing such risks in the age of global supply chains. Various researchers have discussed firms' increasing exposure to risks and the resulting, potentially severe negative impact on the firms' financial performances (e.g., Hendricks & Singhal, 2005).

One such risk to the supply chain, disruption of supply flows, can occur suddenly due to a number of unpredictable events. Even more unpredictable, however, is the ripple effect caused by the disruption. For example, the September 11th terrorist attacks of 2001 in New York and Washington, D.C., originally disrupted many supply chains on the United States (U.S.) East Coast, one of which was the Ford Motor Company's parts supply chain. The disruption eventually forced not one but five of Ford's assembly plants to cease production within a week of the incident (Zakaria, 2001). While Ford was experiencing parts shortages, Quanta Computer, a Taiwanese contract manufacturer for Dell and others, faced a pile-up of finished products when the U.S. airspace closed due to the attacks (Einhorn, 2001). One logistics service company in Europe estimated that the attacks cost the company £5 million (Parker, 2002). In this example, the ripple effects were extensive, affecting businesses in North America, Asia, and Europe. This high degree of impact clearly illustrates the importance of managing ripple effects as a part of supply chain risk management. In the first of two parts, this research shows that Radio Frequency Identification (RFID) technology, a relatively new development in supply chain management, holds great promise for managing supply disruptions and for containing their harmful ripple effects.

RFID — a wireless technology that uses transmitted radio signals to tag an item in order to track and trace its movement without human intervention — has superior capabilities over bar codes and promises many supply chain benefits, such as reductions in shrinkage, efficient handling of materials, increased product availability, and improved asset management (Angeles, 2005; Li & Visich, 2006; Taghaboni-Dutta & Velthouse, 2006). RFID has many applications in retail, healthcare, logistics, records management, and more, but so far its use in risk management has not been explored in the literature. To fill that gap, this research first addresses the following question:

Is RFID applicable in supply chain risk management; in particular, how is it useful for managing supply disruptions?

Based on RFID's technological capabilities, this research identifies three areas in which this technology could be utilized in the management of supply disruption risk: (i) monitoring for a disruption, (ii) responsiveness to the disruption, and (iii) the quality of decision-making involved in choosing corrective actions. Each of these three areas is discussed with a particular focus on how RFID could help to reduce the harmful ripple effects that are generated from supply disruptions. In order to provide support for these uses of RFID in risk management, this research presents case studies that originated from newspaper, magazine, and journal articles.

The discussion on RFID's risk management capabilities considers RFID as a source of advantages for firms that adopt the technology. However, the unprecedented level of supply chain visibility that is possible by the use of RFID can also be a source of risk. The literature has identified a number of concerns about this high degree of RFID-enabled visibility into supply chain activities. The concerns include consumer privacy invasion, corporate system security concerns, and industrial espionage (e.g., Juels, 2006; Shih et al., 2005). The second question in this research draws its motivation from the need to look at the other side of the same coin in order to gain a full understanding of RFID technology within the context of supply chain risk management:

What are the specific risks associated with RFID-enabled supply chain visibility, and how can these risks be mitigated?

The concerns associated with RFID's capability to provide supply chain visibility represent a timely and important research topic because similar concerns have been raised for other technologies that are capable of collecting, storing, and accessing huge amounts of data on individual items or people. For example, the Quit Facebook Day event in 2010 demonstrated Facebook members' concern for the privacy breach by the world's largest social networking website (CNN, 2010), which is capable of generating an unprecedented level of visibility into personal relationships. In the second part of this research, a review of the literature is conducted to identify specific risks associated with RFID's capability to provide supply chain visibility, and the research goes on to examine the existing mitigation approaches for dealing with RFID's visibility-related risks. Finally, the management implications are provided for the use of RFID in supply chain risk management based on both advantages and risks of its use.

The remainder of this chapter is organized as follows. Section 2 provides a review of the background literature. Section 3 presents the first part of this research, which focuses on RFID as a source of advantages in supply chain risk management, and Section 4 presents the second part, which focuses on RFID as a source of risks. Section 5 concludes the chapter with a summary of research contributions, limitations, and directions for future research.

2. Background

This section provides background information for this research. Two areas of the literature are particularly relevant: Section 2.1 reviews the capabilities and applications of RFID technology, and Section 2.2 reviews those risk management elements that are associated with supply disruptions.

2.1 RFID capabilities

RFID is an automatic identification technology that identifies specific items and gathers data on them without human intervention or data entry (Wyld, 2006). Item identification occurs

when a reader scans an RFID tag that is tuned to the same frequency as that of the reader. Fundamentally, RFID technology can be summarized by the following characteristics: (a) RFID is wireless, (b) it provides unique identification to an object, and (c) it traces and tracks objects (Kärkkäinen & Holmström, 2002). Each of these fundamental characteristics leads to an advantage over the existing bar code technology and allows RFID to possess three distinct capabilities: (i) advanced process automation, (ii) closed-loop tracking, and (iii) supply chain visibility (Tajima, 2007). These capabilities and their related applications are discussed in turn, below.

First, RFID's wireless characteristic eliminates the need for product positioning that is associated with bar-code scanning. This allows for the contents of mixed pallets to be identified simultaneously without undoing the packaging. Hence, compared to bar codes, RFID can support a higher degree of automated material inspection and handling (McFarlane & Sheffi, 2003). This process-automation capability provides many benefits in the management of warehouses and logistics by reducing material handling time and human errors in operations, such as receiving, inventory counting, data entry, put-away, routing for cross-docking, and custom clearance for cross-border shipments (Rutner et al., 2004; Zebra Technologies, 2004).

Second, RFID's ability to provide a unique identifier to an object comes from the fact that an RFID tag has a higher data capacity than does a bar code. This higher data capacity provides RFID with advanced record keeping and retrieval capability, through which RFID enables closed-loop tracking of individual items and assets, an action that is not possible with bar codes, which refer only to a class of products (Wyld, 2006). Recently, a wide range of applications has been identified for RFID's closed-loop tracking, including the tracking of medical devices within a hospital; paper documents within a law firm; gaming chips in casinos; media players for rental cars; and flower-growing operations from seeds to blooms (RFID Update, 2006c, 2007a, 2007b, 2007d, 2008b).

Third, RFID's ability to track and trace objects provides supply chain-wide, real-time visibility of individual items. When combined with other real-time locating technologies, such as Global Positioning Systems (GPS), RFID can be used to capture product information such as a detailed description of the product, its manufacture and expiration dates, the time of its departure and arrival at various facilities, and the address and telephone number of its manufacturer (EPCglobal, 2004). RFID-generated product information can provide an unprecedented level of visibility in the supply chain when shared among supply chain partners, a level of visibility that is simply not obtainable from bar codes. In the retail industry, where inaccuracy of inventory data is a major problem (Raman et al., 2001), one of the major applications of RFID is to improve inventory visibility. RFID can also increase the visibility into shipment data, which can in turn improve demand visibility (Lapide, 2004; McCrea, 2005). Automatic replenishment using "smart shelves" is another application in the retail industry and is considered valuable by, for example, German retailer METRO and Finnish apparel manufacturer NP Collection (RFID Update, 2007c, 2007e). For the pharmaceutical industry, the degree of supply chain visibility provided by RFID is considered critical for anti-counterfeiting measures and product recall management (Wicks et al., 2006; Wyld & Jones, 2007).

As shown above, RFID technology has applications in a wide range of industries and settings, but it has not yet found a place in the area of risk management.

2.2 Supply chain risk management

As mentioned in the Introduction, supply chain risks come in a variety of forms. To limit the scope of discussion, however, this research focuses solely on supply disruptions. In this research, supply disruptions are, as defined in Craighead et al. (2007), the disruptions of the normal flows of goods and materials within a supply chain that are caused by unplanned and unanticipated events. These disrupting events come in the various forms, such as natural disasters, labor disputes, wars, power failures, supplier contract breaches, and infectious diseases (Chopra & Sodhi, 2004; Haksöz & Kadam, 2009; Tang, 2006). For the purpose of this research, a ripple effect of a disruption is defined as any other supply disruptions that occur at different locations and/or at later dates due to the original disruption.

Typical risk management consists of four elements: (i) risk source/driver identification, (ii) risk consequence and likelihood assessment, (iii) risk mitigation and treatment, and (iv) risk monitoring. For risk source identification, Helferich (2002) indicated that supply disruptions could occur from interruptions in production facilities, supplier networks, transportation networks, communication infrastructure, and electricity and water services. Global sourcing is particularly vulnerable to supply disruptions because it generally involves greater distance, longer transit time, limited transportation mode, and complex security protocols for border crossings (Prater et al., 2001; Zsidisin, 2003). The just-in-time system is also susceptible to supply disruptions because it operates under fast-cycle procurement and lean inventory (Aichlmayr, 2001).

For risk assessment, Haksöz and Kadam (2009) studied ways to assess the supply disruption risk that results from supplier contract breaches. In their study, a tool to assess the financial impact of contract breaches was developed.

Risk mitigation focuses on ways to avoid, reduce, eliminate, buffer, or hedge against risk. A variety of operational strategies for mitigating supply disruptions have been examined in the literature. Chopra and Sodhi (2004) discussed having redundant suppliers, adding capacity, and increasing responsiveness as possible mitigation strategies. Sheffi (2001) proposed a multiple sourcing strategy that allocates the bulk of the procurement volume to inexpensive offshore suppliers but also gives a fraction of the business to local suppliers as insurance against supply disruption. Prater et al. (2001) identified a number of advantages in using local logistics operators, such as their knowledge of regional transportation routes and their familiarity with the border-crossing procedures. Babich et al. (2007) studied a hedging strategy based on the pricing and ordering policies of multiple suppliers.

Some authors studied inventory-related strategies for mitigating supply disruptions. For example, Sheffi (2001) discussed the emergency designation for safety stock in order to discourage its use for day-to-day fluctuations. Martha and Subbakrishna (2001) suggested increasing safety stock for critical items only, such as those coming from a single international source or those whose shortage quickly leads to plant shutdowns. When transfer or production of goods is not possible within a reasonable time frame, a marketing strategy may be used to steer customers toward substitutes. This strategy was exercised by Dell in response to the September 11th terrorist attacks (Rocks, 2001): Dell salespeople searched online to see which configurations of computers were available and then steered customers accordingly. Finally, Craighead et al. (2007) identified two key capabilities for mitigating supply disruptions: the capability to detect and disseminate information pertaining to the disruptive event, and the capability to respond quickly and effectively to the disruption.

The next section, which presents the first of two parts in this research, highlights RFID's usefulness in supply chain risk management by demonstrating that RFID can improve some of the risk-mitigation strategies mentioned above.

3. RFID as a source of advantages

Is RFID applicable in supply chain risk management, and in particular, how is it useful for managing supply disruptions? This section addresses this research question by showing that an understanding of RFID's technological capabilities can lead to the discovery of RFID's risk management capabilities.

3.1 Methodology

First, it is shown that RFID's technological capabilities of closed-loop tracking, process automation, and supply chain visibility yield three specific risk management capabilities: increased monitoring capacity, increased response speed, and higher decision-making quality. Then, case studies are presented for all three risk management capabilities in order to provide support for their validity. As shown in Section 2.1, RFID application that is specific to the area of risk management has not yet been explored. Hence, any related case studies that could highlight the potential use of RFID in risk management were searched from newspaper, magazine, and journal articles. Below, RFID's three risk management capabilities are discussed in turn.

3.2 Monitoring capacity

Risk monitoring, as discussed in Section 2.2, is one of the typical elements in risk management, and it plays an important role in the management of unexpected supply disruptions. With an ability to monitor for and detect a disruption as it happens, corrective actions can begin sooner, the escalation of the disruption can be avoided, and the impact of the disruption, direct or indirect, can be reduced. Craighead et al. (2007) identified risk monitoring as one of the key capabilities needed for mitigating supply disruptions. It is shown below that closed-loop tracking, one of RFID's technological capabilities, can increase a firm's risk monitoring capacity.

As discussed in Section 2.1, the data capacity of RFID tags is higher than that of bar codes, and this higher data capacity allows for the closed-loop tracking of individual items and assets. RFID can be used to monitor not only cases and pallets but also individual raw materials, work-in-process inventories, and finished products. It can also monitor the use and condition of equipment and reusable assets. Therefore, with its closed-loop tracking capability, RFID can increase a firm's monitoring capacity by increasing the level of details that can be monitored.

The following case studies provide support for RFID's ability to increase a firm's monitoring capacity. At Nestlé, a large global food company, RFID was used to track the cleanliness of product trays (Bear, Stearns & Co. Inc., 2003). Such RFID-enabled tracking of reusable assets would extend Nestlé's capacity for detecting poor product quality to include the work-in-process items in addition to finished products. At the Wynn Hotel and Casino in Las Vegas, poker chips imprinted with RFID were used to monitor game play for possible cheating or gambling addiction (Wyld, 2008). In this case, RFID would increase the casino's capacity to detect problematic gaming behavior from the table/station level to the individual player.

RFID's closed-loop tracking capability can also increase a firm's risk monitoring capacity by providing the firm with an ability to monitor huge volumes of assets. RFID has already

successfully managed a variety of assets with huge volumes. For example, a casino tracked 80,000 uniforms through the laundry process, and a beer company tracked three million beer kegs using RFID (Bear, Stearns & Co. Inc., 2003; Byrne, 2004). Byblos Amoreiras, a Portuguese book retailer, used RFID to track 150,000 books, periodicals, CDs, and other merchandise in its store (RFID Update, 2008a).

By increasing a firm's risk monitoring capacity, RFID can assist the firm with the identification of critical items. In Section 2.2, some risk mitigation strategies, such as an increase of safety stock and multiple sourcing, were discussed for critical items (Martha & Subbakrishna, 2001). With the use of RFID, firms could quickly identify critical items, such as those that run out first or those whose shortage causes a plant shutdown. Also, RFID's capability to monitor huge volumes of items can assist firms with the collection of historical data at the individual item level. These data would be useful in improving a firm's risk assessment in terms of estimating and updating the severity and likelihood of various supply disruptions.

3.3 Response speed

The previous section focused on RFID's ability to detect a disruption at the level of individual items and assets. Once detected, a firm's ability to respond quickly to the disruption becomes important in the containment of the ripple effects. Responsiveness has been identified as one of the key capabilities for managing supply disruptions in the literature (Chopra & Sodhi, 2004; Craighead et al., 2007). Another of RFID's technological capabilities, process automation, can increase a firm's response speed.

As discussed in Section 2.1, when compared to bar code technology, RFID's wireless characteristic allows for a higher degree of automation in the processes, such as material inspection and handling (McFarlane & Sheffi, 2003). For LCWaikiki, one of the largest apparel retailers in Turkey, the replacement of bar codes with RFID technology has resulted in the merchandise transfer from the back room to the shop floor being performed 70% faster and the merchandise receiving being performed 60% faster (RFID Update, 2008d). For Bloomingdale's, a large U.S. department store, an RFID pilot study resulted in a 96% reduction of cycle counting time for the store's inventories (RFID Update, 2009). For American Apparel, a large U.S. clothing manufacturer and retailer, with the use of RFID, the time required for store-level inventory count dropped from 120 work-hours to 15 work-hours (Avery Dennison Corporation, 2010). These case studies support RFID's ability to speed up some of the common responses to a supply disruption, such as recounting inventories, adjusting shipment data, and sending invoice reconciliations.

In reality, the response to a supply disruption cannot begin until key personnel within a firm are notified of the disruption. Once notified, these individuals can then authorize the start of corrective actions. In this leg of the process, RFID's process automation capability can increase a firm's response speed by facilitating the real-time alert for notifying key personnel in the event of a supply disruption. Throttleman, a Portuguese fashion retailer, has set up a real-time alert system using RFID in its distribution center (RFID Journal, 2007). Upon arrival at the distribution center, the contents of a box are automatically identified using RFID without opening the box. The captured contents are then compared to the items listed in an advance shipping notice that has been electronically sent by the garment manufacturer. If the received contents do not match with the advance shipping notice, then an alarm goes off for the center's personnel to physically deal with the discrepancy. In

another instance, a real-time alert system has been implemented at several U.S. hospitals to notify staff immediately when a piece of equipment becomes misplaced (Emrich, 2008). Also, at Lincoln University, a Pennsylvania liberal arts college, valuable audio-visual equipment was tracked using RFID, and an alert notified the IT department as soon as a piece of equipment left its predetermined zone (RFID News, 2008). These case studies support RFID's ability to increase a firm's response speed by setting up a real-time personnel alert system.

3.4 Decision-making quality

Upon notification of a supply disruption, key personnel need to assess the extent of the disruption and decide on the appropriate risk mitigation strategies before corrective actions can actually begin. The quality of these strategic decisions can have a significant impact on the outcome of the corrective actions. For example, Hurricane Mitch in 1998 caused a supply interruption for two major banana producers in Central America, Dole and Chiquita (Martha & Subbakrishna, 2001). Dole's business suffered from this supply disruption, with the subsequent ripple effect lasting longer than a year. Chiquita, on the other hand, had a significantly different outcome: it was able to arrange alternative supply sources, and its revenue actually grew during the last quarter of 1998.

In general, management decisions are often made based on incomplete or old data (Lin et al., 2006). Therefore, an overall increase in information accessibility has significant potential to improve the quality of management decisions, including the ones that must be made in response to supply disruptions. As discussed in Section 2.1, compared to bar codes, RFID promises an unprecedented visibility into supply chain operations. Supply chain-wide visibility provides information such as inventory levels, shipment data, locations of stockpiles, and alternative suppliers throughout the extended enterprise. Such information is critical in providing a firm with the ability to redirect its inventories within its supply chain, or to steer customers toward substitute products based on informed decision-making, rather than based on incomplete or untimely data. Hence, the third of RFID's technological capabilities, supply chain-wide visibility, can improve the quality of a firm's decision-making in the selection of risk mitigation strategies by increasing the completeness and timeliness of information available for the decision-makers.

Several case studies provide support for RFID's ability to improve the quality of a firm's risk mitigation decisions. In the retail industry, electronic article surveillance (EAS) devices provide retailers with the knowledge of timing when something is stolen from a store, but it cannot reveal which item has been taken (RFID Journal, 2009). RFID, on the other hand, can provide the retailers with more complete information. At Sony Europe, a combination of RFID, EAS, and a video surveillance system was implemented in its largest European distribution warehouse, located in the Netherlands (RFID Journal, 2009). The system was designed to deter employee or professional theft by giving Sony as much information as possible on each theft: which item is stolen, when it is stolen, and who may be doing the stealing. In another case, the additional data obtained through RFID allowed one retailer to successfully link multiple thefts over a period of time to a single person (Arnstein, 2010). Moreover, RFID-generated data can support a targeted and cost-effective security strategy that provides different security levels for different products within the same store, such as a silent alarm for expensive items and an audible alarm for inexpensive ones (Arnstein, 2010). These case studies support RFID's ability to improve the quality of a firm's risk mitigation decisions by increasing the completeness of the information available for the decision-makers.

As discussed in Section 2.1, when combined with other real-time locating technologies, such as GPS, RFID is capable of capturing product information within a supply chain on a real-time basis. Hence, in addition to the increase in completeness of information, RFID-enabled supply chain visibility can increase the timeliness of information available for the decision-makers in a firm. For example, through the use of RFID, Dole Food Company, the world's largest producer and marketer of fresh fruits and vegetables, was able to initiate a voluntary, pre-emptive recall of packaged salads that were suspected of E. coli bacteria contamination *before* any consumers were reported ill (Uldrich, 2007). When the recall announcement was made, Dole also knew that a total of 5,058 bags of salad were most likely to have been exposed to the bacteria, of which 528 bags were distributed in Canada and 4,530 bags were distributed within eight U.S. states. The value of RFID in providing timely information was also discussed in a simulation study conducted by Kim et al. (2010). Their study showed that an RFID-based, vehicle-tracking system could significantly decrease the overall transfer time of finished vehicles from an automobile assembly plant to its shipment yard by providing the real-time availability of parking spots. The yard operators were then able to use real-time information to make their decisions more efficiently and effectively. Without RFID, the status of parking availability could be updated only periodically through a manual reporting process, and therefore, the yard operators had to make their decisions based on untimely data.

All the related case studies presented above support RFID's ability to improve a firm's risk management capabilities in terms of its monitoring capacity, response speed, and decision-making quality. As a result, this section clearly demonstrates RFID's applicability in supply chain risk management and its usefulness in managing supply disruptions.

4. RFID as a source of risks

The previous section focused on RFID as a source of advantages for firms that adopt the technology and use it for supply chain risk management. However, the use of RFID can also be a source of various risks in and of itself. Within the literature, numerous articles have discussed RFID-enabled supply chain visibility as a source of security and privacy risks. The concerns surrounding these risks are a timely and important research topic, from both industry and society perspectives.

From a society perspective, a general feeling of anxiety exists toward technology-enabled information visibility. As mentioned in the Introduction, the Quit Facebook Day event in 2010 stands out as a high-profile example of people's concerns for the breach of users' personal information. Another example concerns Google's Street View, which provides panoramic views of streets all over the world, as captured by a fleet of vehicles that are equipped with high-tech cameras and scanners. The main concern for this technology stems from the fact that these panoramic images are publicly accessible from the Google website and may contain personally identifiable details, such as people's faces, belongings, and cars on the driveways with visible license plate numbers, all matched to easily identifiable street addresses (Bradley, 2010). Digital medical records represent another high-profile example of the public's concerns for technology-enabled information visibility. On one hand, electronically accessible medical records offer many benefits, including the reduction of duplicate diagnostic testings and medical errors. On the other hand, medical records consist of highly personal information, from prescription records to family-health histories, and may even include DNA information in the future (Fox News, 2010). A concern exists among

physicians in terms of how to protect such private, sensitive, and massive data from potential hacking. As can be seen from these examples, the concerns for technology-enabled information visibility are not unique to RFID, and at present, no absolute solutions or countermeasures exist to deal with these concerns.

From an industry perspective, the risks associated with RFID-enabled supply chain visibility constitute a timely and important research topic for RFID vendors, potential users, and corporate and public policy-makers mainly because RFID is still a developing technology (RFID Update, 2008c), whose industry adoption may easily be hindered by any risk related to its use. With other established supply chain technologies, such as bar codes, electronic data interchange (EDI), and enterprise resource planning (ERP), information sharing and the resulting visibility have not posed any serious issues since the scope of visibility has rarely been extended to involve individual items or consumers. Consequently, within the context of supply chain technologies, RFID has no obvious precedence to follow regarding how to deal with the risks related to information visibility, and this makes an understanding of these risks critical for RFID technology's future growth.

What, then, are the specific risks associated with RFID-enabled supply chain visibility, and how can these risks be mitigated? The remainder of this chapter focuses on addressing this research question.

4.1 Methodology

A review of published literature is provided on possible risks associated with RFID-enabled supply chain visibility. Two databases, ProQuest and Scholars Portal, were used to search relevant articles. The chosen search terms utilized various combinations of: RFID, risk, security, and privacy. The search dates were restricted to the years between 2003 and 2010. Due to insufficient resources for translation, the review was also restricted to English-language articles only. The search produced over 100 articles, covering more than 50 different journals from a variety of disciplines, such as business, engineering, information systems, economics, law, electronic commerce, marketing, production, and healthcare. Therefore, although the search was not exhaustive, the search range was considered sufficiently comprehensive in terms of the variety of articles, and further searches from other databases were deemed unnecessary.

Based on the articles found in the search described above, Section 4.2 provides the first result: an overview of two main categories of RFID's supply chain visibility risks, which are security risks and privacy risks. Section 4.3 then provides the second result: a classification of the existing mitigation approaches for dealing with RFID's supply chain visibility risks. Finally, Section 4.4 discusses the management implications of the use of RFID in supply chain risk management based on its advantages as well as risks.

4.2 Supply chain visibility risks

In the RFID literature, a variety of risks associated with the use of RFID have been discussed. For example, a risk to patients' health that might result from the altering of the chemical composition of a medication was discussed in the context of using RFID for pharmaceutical products (Symbol Technologies, 2006). A risk to the environment was discussed in relation to the disposal of non-biodegradable RFID tags (Li & Visich, 2006). A risk to the corporate information system was also discussed in terms of the vulnerability of RFID to computer viruses (RFID Update, 2006b). This section, however, focuses on

providing an overview of the risks that are specifically associated with RFID-enabled supply chain visibility: security risks and privacy risks.

Security risks. Security risks in the RFID literature are often discussed as attacks against organizations by their competitors, opponents, or criminals. Various types of attacks are possible with the use of RFID. One type is referred to as "data eavesdropping," which is the interception of communications between RFID tags and readers. Through data eavesdropping, a military security breach may occur if enemy forces detect troop locations and monitor their movements by tracking RFID tags within a military supply chain (Juels, 2006; Zuo, 2010). Corporate espionage is also possible through data eavesdropping. For example, by tracking RFID tags through the retail supply chain, competitors may spy on one retailer's sensitive business data, such as sales trends, pricing trends, stock selections, and stock turnover rates (Juels, 2006; Li & Visich, 2006; Shih et al., 2005). A seller organization may also attempt to gain visibility into the downstream of the supply chain by monitoring RFID tags on the sold items after the seller no longer has physical access to the items (Kapoor et al., 2009).

Another type of attack against organizations is referred to as "data corruption," which erases or modifies RFID tag contents. If the tag contents include price information, then, through data corruption, hackers could lower the price of expensive retail items, and then use an RFID-enabled self-checkout counter to avoid detection by store employees (Li & Visich, 2006). Spoofing, another type of attack, involves the retrieval of confidential information by impersonating authentic readers (Shih et al., 2005). Spoofing can lead to, for example, counterfeiting of retail products by falsely authenticating fake products using stolen authentication information. Finally, denial of service is a type of attack that renders RFID tags temporarily or permanently incapacitated (Zuo, 2010). Denial of service can cause a loss of business data and operational disruptions to an organization.

Privacy risks. While security risks typically affect organizations and result in financial losses, privacy risks affect individuals and result in ethical issues. The literature discusses three main issues that are specifically related to RFID's ability to provide supply chain visibility that includes end-consumer information.

The first issue relates to the collection of personal data without an individual's knowledge or consent. This concern stems from the fact that the size of RFID tags can be as small as grains of sand, making it possible to inconspicuously attach the tags on products. Also, the scanning of RFID tags is a wireless process that cannot be detected by human eyes or ears. Hence, a retailer is technically able to conduct market research, for example, by tracking RFID tags on pre-sale items inside the store without the knowledge or consent of the consumers (Jones et al., 2004).

The second ethical issue relates to the infringement on individual anonymity. In the context of supply chain management, RFID tags are traditionally associated with product information but not with consumer information. However, since an RFID tag is capable of providing a unique identifier to a product, any association between the product and an individual can in turn become the unique identifier of the individual. For example, a female customer with a previously purchased item carried in a purse can be identified as a returning customer if the tag on the item is read upon her return to the store. Even if the retailer does not possess full information on her identity, the anonymity of this customer can still be infringed upon since it is possible to build a personal profile based on information such as the frequency of the store visit, the time and day of the visit, and the history of other purchases made by this customer (Wasieleski & Gal-Or, 2008). Such consumer profiles could

then be exploited for price differentiation strategies or could be sold to third parties (Jones et al., 2004; Peslak, 2005). Moreover, if the item in question was, for example, a prescription drug bottle being carried by an individual, then the product information itself could represent a piece of sensitive personal data.

The third ethical issue, the surveillance of individuals, also stems from the association made between a product and an individual by the use of RFID. By tracking RFID tags on products that are owned by individuals, people may be tracked in the stores, on the streets, and even in people's homes (Jones et al., 2004; Rutner et al., 2004). This issue is often discussed in relation to the idea of "Big Brother," where the authority monitors civilians' every move.

All the ethical issues discussed above have been fueling an opposition to RFID from various consumer advocacy groups, such as Consumers Against Supermarket Privacy Invasion and Numbering (CASPIAN), the American Civil Liberties Union, the Privacy Rights Clearinghouse (PRC), all of which are generally against the use of RFID (Barut et al., 2006; Jones et al., 2004).

4.3 Risk mitigation approaches

The actual occurrence of security and privacy risks is still not common due to the limited and fragmented use of RFID, and the literature discusses these issues as potential risks of RFID. However, as mentioned previously, any risk related to RFID's use may negatively affect the growth of this technology. How, then, can these risks be mitigated? This section presents a classification of the existing mitigation approaches for dealing with RFID's supply chain visibility risks. An examination of the RFID literature revealed that four general treatments currently exist: technology-based countermeasures, business policies, consumer education, and legal measures. Each of these approaches is discussed below.

Technology-based countermeasures. In order to reduce the likelihood of the occurrence of security and privacy risks, some technology-based countermeasures have been proposed in the literature. One group of countermeasures is designed to protect RFID tags from unauthorized scanning, including: tag killing, to make tags permanently inoperative when the tags receive a "kill" command from a reader; tag sleeping, to make tags temporary inactive unless "woken" by authorized users; tag relabeling, to give tags different identifiers periodically; tag encryption, to use cryptography to encrypt tag data or identifiers; and hash locks, to make tags respond to data queries with only limited information when "locked" (e.g., Juels, 2006; Shih et al., 2005; Zuo, 2010). By protecting the tags, these countermeasures are intended to prevent security attacks, such as data corruption, spoofing, and denial of service; they can also prevent the surveillance of individuals.

Another group of technology-based countermeasures is designed to protect communications between RFID tags and readers. Most of these countermeasures are based on developing protocols for the search and authentication procedures that occur between the tags and readers (Zuo, 2010). Another approach to protect the tag-reader communication is to limit the tag-reading area, which can be accomplished by tag clipping, a process that shortens the antenna in a tag to reduce its read range (Kapoor et al., 2009), or by shielding the tag-reading area with metal screens to prevent the unauthorized scanning from outside (Swartz, 2007). The protection of communications between tags and readers would certainly be useful for the prevention of attacks that involve data eavesdropping and spoofing.

Another group of technology-based countermeasures focuses on informing individuals about unauthorized scanning. For example, a watchdog tag is supposed to be carried by an individual to monitor for any unsolicited scannings against the individual (Juels, 2006). A

read-write tag, also carried by an individual, keeps a log of unauthorized scannings (Li & Visich, 2006), and a blocking tag on an individual is supposed to block any unsolicited scannings (Juels, 2006). By alerting individuals about the practice of unauthorized scanning, these countermeasures give consumers an opportunity to, for example, look for a suspicious reader or walk away from the area in question, therefore, helping to alleviate the risks, such as data eavesdropping, collection of personal data without the individuals' knowledge or consent, and the surveillance of individuals.

Business policies. The use of business policies offers another general approach for dealing with RFID's supply chain visibility risks. While technology-based countermeasures address both security and privacy risks, the business policies discussed in the literature focus on dealing with privacy risks. Common policies on the use of RFID include making RFID tags clearly visible to consumers, making tags easily removable by placing them on the product packaging or on price tags, and disabling tags at the point of product purchase (Jones et al., 2004; Li & Visich, 2006; Taghaboni-Dutta & Velthouse, 2006). As an example, H.D. Smith, a major pharmaceutical product distributor, officially requested that its customers (i.e., pharmacies and hospitals) remove RFID tags upon receipt of shipments from H.D. Smith (Downey, 2006). Business policies may also include statements about a firm's data-collection practices. For example, Pfizer, a large pharmaceutical manufacturer, made a public statement that it would not collect any patient information using RFID (RFID Update, 2006a). Such policy statements are used by firms mainly to reassure consumers that the subject firms intend to use RFID responsibly, thereby minimizing the privacy risks associated with its use.

Consumer education. Another general approach for dealing with RFID's supply chain visibility risks comes in the form of consumer education. As with the business policy approach, consumer education focuses on dealing with privacy risks. In 2004, a survey of 1,000 North American consumers showed that only one in four knew what RFID was (Jones et al., 2004). A study on the consumer attitude toward RFID revealed that, the less consumers were educated about RFID, the more hesitant they were about the use of RFID in businesses (Razzouk et al., 2008). In light of a general lack of consumer understanding regarding RFID, an industry group, the Association for Automatic Identification and Mobility (AIM), has recognized the need to convey accurate information about the technology to the community (Peslak, 2005). Information on RFID's technical capabilities, as well as its limitations and comparisons of RFID to other wireless technologies, could educate consumers on the likelihood of privacy risks. Moreover, consumers could be further educated on the likelihood of privacy risks through access to information on whether an RFID tag is embedded in a product, when the tag is read, and whether the tag is removed or deactivated upon purchase (Pottie, 2004).

Legal measures. The final approach that is discussed in the literature as a way to deal with RFID's supply chain visibility risks is the legal approach. This approach mainly focuses on the protection of information privacy, which is the right of an individual to retain control over the collection and use of personally identifiable information (Kelly & Erickson, 2005). In 2004, California passed a bill prohibiting the use of RFID to collect, store, use, or share personal information unless certain legal conditions were met (Taghaboni-Dutta & Velthouse, 2006). A proposal to extend the Fair Information Practices, originally promoted by the Federal Trade Commission in the U.S. to protect online privacy, has also been put forth for the use of RFID (Peslak, 2005). Fair Information Practices include business practices such as notifying consumers of the collection of personal information; giving consumers

options concerning how information is used; giving consumers access to the collected information; providing security over the collected data; and providing penalties for non-compliance. The European Union does not have RFID-specific regulations. However, its existing regulations — the Data Protection Directive of 1995, the Electronic Commerce Directive of 2000, and the Privacy and Electronic Communications Directive of 2002 — do apply to the personal data collected by the use of RFID (Slettemeås, 2009). By establishing and enforcing the laws on RFID-generated data, the legal approach is intended to deter the occurrence of security and privacy risks and to provide individuals with a means of recourse in the case of a privacy breach.

4.4 Management implications

The first part of this two-part research demonstrated that RFID could be a source of tremendous advantage for firms that adopt the technology and use it for managing supply disruptions. The second part of this research, however, showed that RFID could also be a source of security and privacy risks, and attacks on the RFID system, such as data corruption and denial of service, may actually cause supply disruptions through a loss of business data or the disruptions to internal operations. Hence, from a management perspective, the use of RFID in supply chain risk management requires careful consideration of the risks in and of RFID itself. The security attacks in general may be alleviated by the use of technology-based countermeasures. However, the management must be aware that various shortcomings have been documented for these countermeasures. For example, tag killing can eliminate the security risks, but it also eliminates many post-sale benefits of having RFID tags on products, such as efficient warranty processing, easy handling of returns, and goods authentication (Juels, 2006). The use of cryptography may be computationally infeasible when RFID tags are employed on a mass scale (Zuo, 2010), and a security protocol is secure only until its loopholes are discovered (Kapoor et al., 2009).

Privacy risks associated with the use of RFID may not cause supply disruptions, but they may negatively influence the consumer attitude towards RFID (e.g., Slettemeås, 2009), thereby hindering the growth of RFID adoption. Hence, the management needs to address the privacy risks in general, but it must be aware that the mitigation of the privacy risks is a complex subject that requires a multi-faceted solution, for none of the existing mitigation approaches provides an all-encompassing solution on its own. Technology-based countermeasures, as mentioned above, come with various shortcomings. Business policies and consumer education do not actually prevent the incidence of unauthorized scanning. With the legal approach, the burden is placed on the plaintiff to prove that a privacy breach has taken place and it resulted in a high degree of shame, humiliation, mental illness, and so on (Willey, 2007).

A further examination of the privacy risks reveals that, when a firm considers the use of RFID in supply chain risk management, the collection of personal data without an individual's knowledge or consent and the surveillance of individuals may not be the first risks that the firm needs to address since the data utilized in the context of risk management are mostly inventory, shipment, equipment, asset, and supplier data, but not consumer data. On the other hand, since a unique product identifier given by an RFID tag can turn into a unique personal identifier as discussed previously, the infringement on individual anonymity should be addressed whenever a firm uses item-level information. In terms of risk mitigation, all of the current approaches focus on when or how to stop the collection of

personal data, but none of them effectively address the infringement on individual anonymity since they do not focus on what to do with the data that are already collected.
Based on this research, two suggestions are made for mitigating the infringement on individual anonymity when firms consider the use of RFID for supply chain risk management. First, the firms can utilize the consumer education approach to clearly communicate specific benefits for consumers resulting from the better management of supply disruptions. Based on the three risk management capabilities of RFID discussed previously, the consumers can expect benefits such as fewer and shorter business disruptions experienced by the consumers and increased public safety in certain cases (e.g., food recalls). Second, in addition to the business policies on whether or not certain data will be collected, the firms should consider adding policies on how they intend to utilize the collected data in order to come across as the responsible users of RFID in the eyes of consumers. For example, a firm may state that it will collect item-level product data via RFID for the purpose of detecting and mitigating supply disruptions.

5. Conclusion

The first part of this research demonstrated that RFID's three risk management capabilities — monitoring capacity, response speed, and decision-making quality — were applicable and useful in the management of supply disruptions. The second part of this research showed that the security and privacy risks were associated with RFID-enabled supply chain visibility, and that four general mitigation approaches exist at present: technology-based countermeasures, business policies, consumer education, and legal measures. Together, the two parts of this research provided a comprehensive understanding of the use of RFID in the context of supply chain risk management.
The main limitation of this research is that some practical issues related to the use of RFID in a real-life setting were not included in the discussion. One such issue is that a firm's corporate information system may not be capable of supporting the increased monitoring capacity that is promised by the use of RFID. A general increase of data processing needs has been discussed as one of the challenges associated with RFID implementation (Angeles, 2005). Another issue arises with the design of a real-time alerting system. The alerting of top personnel should ideally be reserved for severe supply disruptions only. This implies that the alerting system must recognize different levels of the disruptions in order to alert different levels of personnel. However, a firm may not have sufficient data on the actual supply disruptions with varying degrees. Also, as RFID improves the completeness and timeliness of information available for the key decision-makers, information overload may become an issue in general. Having abundant information may lead to the generation of many options for the decision-makers to assess, and consequently, it may slow the response to a supply disruption. Future research must address such practical issues in order to make RFID-based risk management a reality.
In conclusion, this research provided valuable insight into a novel application of RFID technology in the area of supply chain risk management. This insight was built from the balanced understanding of RFID as a source of advantages as well as a source of risks.

6. Acknowledgment

The author wishes to acknowledge Lelanya Perryman for her assistance in this research as a research assistant, whose work was funded by the Start-Up Research Grant at The University of Western Ontario.

7. References

Aichlmayr, M. (2001). The future of JIT – time will tell. *Transportation and Distribution*, Vol. 42, No. 12, pp. 18-22

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

Arnstein, L. (2010). How to serve the multi-channel consumer. *Material Handling Management*, December 1

Avery Dennison Corporation. (2010). American Apparel RFID case study: the challenges. Date of access, March 21, 2011, Available from: www.ibmd.averydennison.com/solutions/american-apparel-rfid-challenges.asp

Babich, V., Burnetas, A., & Ritchken, P.H. (2007). Competition and diversification effects in supply chains with supplier default risk. *Manufacturing and Service Operations Management*, Vol. 9, No. 2, pp. 123-146

Barut, M., Brown, R., Freund, N., May, J., & Reinhart, E., (2006). RFID and corporate responsibility: hidden costs in RFID implementation. *Business and Society Review*, Vol. 111, No. 3, pp. 287-303

Bear, Stearns & Co. Inc. (2003). Supply-chain technology: track(ing) to the future. Equity research report, Date of access, September 10, 2006, Available from: www.bearstearns.com/bscportal/pdfs/research/supplychain/technology_rfid.pdf

Bradley, T. (2010). Google Street View raises privacy concerns again. In: *PCWorld*, Date of access, February 18, 2011, Available from: www.pcworld.com/printable/article/id,190279/printable.html

Byrne, P.M. (2004). RFID: not just for Wal-Mart anymore. In: *Logistics Management*, September 1, Date of access, September 10, 2006, Available from: www.logisticsmgmt.com/archive

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

CNN. (2010). Some quitting Facebook as privacy concerns escalate, In: *CNN Tech News*, Date of access, February 18, 2011, Available from: http://articles.cnn.com/2010-05-13

Craighead, C.W., Blackhurst, J., Rungtusanatham, M.J., & Handfield, R.B. (2007). The severity of supply chain disruptions: design characteristics and mitigation capabilities. *Decision Sciences*, Vol. 38, No. 1, pp. 131-156

Downey, L. (2006). An Interview with RFID Trailblazer H.D. Smith. *RFID Update*, August 21, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

Einhorn, B. (2001). Laptop king; in a year that's decimated high tech, Taiwan's unstoppable Quanta is posting double-digit sales growth. *Business Week*, No. 3756, p. 48

Emrich, A.B. (2008). Wireless RFID product tracks hospital assets. *Grand Rapids Business Journal*, Vol. 26, No. 50, p. 14

EPCglobal. (2004). The EPCglobal Network and the Global Data Synchronization Network (GDSN). Date of access, September 10, 2006, Available from: www.epcglobalinc.org/news/position_papers.html

Fox News. (2010). WikiLeaks breach raises concern about privacy of electronic medical records. In: *Fox News*, Date of access, February 18, 2011, Available from: www.foxnews.com/politics/2010/12/07

Haksöz, Ç., & Kadam, A. (2009). Supply portfolio risk. *The Journal of Operational Risk*, Vol. 4, No. 1, pp. 59-77

Helferich, O.K. (2002). Securing the supply chain against disaster. *Distribution Business Management Journal*, Vol. 2, No. 3, pp. 10-14

Hendricks, K.B., & Singhal, V.R. (2005). An empirical analysis of the effect of supply chain disruptions on long-run stock price performance an equity risk of the firm. *Production and Operations Management*, Vol. 14, No. 1, pp. 35-52

Jones, P., Clarke-Hill, C., Hillier, D., Shears, P., & Comfort, D. (2004). Radio frequency identification in retailing and privacy and public policy issues. *Management Research News*, Vol. 27, No. 8/9, pp. 46-56

Juels, A. (2006). RFID security and privacy: a research survey. *IEEE Journal of Selected Areas in Communications*, Vol. 24, No. 2, pp. 381-394

Kapoor, G., Zhou, W., & Piramuthu, S. (2009). Challenges associated with RFID tag implementations in supply chains. *European Journal of Information Systems*, Vol. 18, No. 6, pp. 526-533

Kärkkäinen, M., & Holmström, J. (2002). Wireless product identification: enabler for handling efficiency, customization and information sharing. *Supply Chain Management: An International Journal*, Vol. 7, No. 4, pp. 242-252

Kelly, E.P., & Erickson, G.S. (2005). RFID tags: commercial applications v. privacy rights. *Industrial Management and Data Systems*, Vol. 105, No. 6, pp. 703-713

Kim, J., Ok, C.S., Kumara, S., & Yee, S.T. (2010). A market-based approach for dynamic vehicle deployment planning using radio frequency identification (RFID) information. *International Journal of Production Economics*, Vol. 128, No. 1, pp. 235-247

Lapide, L. (2004). RFID: what's in it for the forecaster? *Journal of Business Forecasting Methods and Systems*, Vol. 23, No. 2, pp. 16-19

Li, S., & Visich, J.K. (2006). Radio frequency identification: supply chain impact and implementation challenges. *International Journal of Integrated Supply Management*, Vol. 2, No. 4, pp. 407-424

Lin, D., Barton, R., Bi, H., & Freimer, M. (2006). Challenges in RFID enabled supply chain management. *Quality Progress*, Vol. 39, No. 11, pp. 23-28

Martha, J., & Subbakrishna, S. (2001). When just-in-time becomes just-in-case. *Wall Street Journal*, October 22, p. A18

McCrea, B. (2005). Reliable Foods lives up to its name. In: *Logistics Management*, July 1, Date of access, September 10, 2006, Available from: www.logisticsmgmt.com/archive

McFarlane, D., & Sheffi, Y. (2003). The impact of automatic identification on supply chain operations. *International Journal of Logistics Management*, Vol. 14, No. 1, pp. 1-17

Parker, R. (2002). Just-in-time freight plans survive 11 September crisis. *Supply Management*, Vol. 7, No. 5, p. 8

Peslak, A.R. (2005). An ethical exploration of privacy and radio frequency identification. *Journal of Business Ethics*, Vol. 59, No. 4, pp. 327-345

Pottie, G.J. (2004). Privacy in the global e-village. *Communications of the ACM*, Vol. 47, No. 2, pp. 21-23

Prater, E., Biehl, M., & Smith, M.A. (2001). International supply chain agility: tradeoffs between flexibility and uncertainty. *International Journal of Operations and Production Management*, Vol. 21, No. 5/6, pp. 823-839

Raman, A., DeHoratius, N., & Zeynep, T. (2001). Execution: the missing link in retail operations. *California Management Review*, Vol. 43, No. 3, pp. 136-152

Razzouk, N., Seitz, V., & Nicolaou, M. (2008). Consumer concerns regarding RFID privacy: an empirical study. *Journal of Global Business Technology*, Vol. 4, No. 1, pp. 69-78

RFID Journal. (2007). Throttleman adopts item-level tagging. In: *RFID Journal*, Date of access, January 19, 2011, Available from: www.rfidjournal.com/article/print/3580

RFID Journal. (2009). Retail theft is up – can RFID help? In: *RFID Journal*, Date of access, January 19, 2011, Available from: www.rfidjournal.com/blog/entry/5372

RFID News. (2008). Schools using RFID for security enhancement. In: *RFID News*, Date of access, January 19, 2011, Available from: www.rfidnews.org/2008/09/09/schools-using-rfid-for-security-enhancement

RFID Update. (2006a). Pfizer Shipping RFID-Tagged Viagra. In: *RFID Update*, January 9, Date of access, March 21, 2011, Available from:www.rfidupdate.com /articles/home.php.

RFID Update. (2006b). Study: RFID vulnerable to viruses and worms. In: *RFID Update*, March 15, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2006c). Dutch casino operator bets on RFID chips. In: *RFID Update*, December 8, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2007a). RFID blooms for Dutch flower tracking. In: *RFID Update*, July 18, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2007b). Hospital manages thousands of patient files with RFID. In: *RFID Update*, August 1, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2007c). Why METRO's item-level RFID deployment matters. In: *RFID Update*, September 24, Date of access, September 24, 2007, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2007d). RFID file tracking is heating up. In: *RFID Update*, November 29, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2007e). Finnish retailer gets quick ROI on item-level RFID. In: *RFID Update*, November 16, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2008a). World's largest item-level RFID application launches. In: *RFID Update*, Date of access, January 19, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2008b). RFID helps kids take Dora the Explorer on road trips. In: *RFID Update*, March 10, Date of access, March 21, 2011, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2008c). RFID market on target to reach $5.3B in 2008. In: *RFID Update*, June 12, Date of access, June 12, 2008, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2008d). Turkish retailer plans big item-level RFID expansion. In: *RFID Update*, Date of access, August 11, 2008, Available from: www.rfidupdate.com/articles/home.php

RFID Update. (2009). Bloomingdale's tracks strong results from RFID pilot. In: *RFID Update*, Date of access, January 19, 2011, Available from: www.rfidupdate.com/articles/home.php

Rocks, D. (2001). The Net as a lifeline; a tough economic environment makes the Web even more important for companies attempting to cut costs, generate new revenues, and better serve customers. *Business Week*, No. 3755, p. EB16

Rutner, S., Waller, M.A., & Mentzer, J.T. (2004). A practical look at RFID. In: *Supply Chain Management Review*, January/February, Date of access, September 10, 2006, Available from: www.manufacturing.net/scm/

Sheffi, Y. (2001). Supply chain management under the threat of international terrorism. *The International Journal of Logistics Management*, Vol. 12, No. 2, pp. 1-11

Shih, D.H., Lin, C.Y., & Lin, B. (2005). RFID tags: privacy and security aspects. *International Journal of Mobile Communications*, Vol. 3, No. 3, pp. 214-230

Slettemeås, D. (2009). RFID–the "next step" in consumer-product relations or Orwellian nightmare?: challenges for research and policy. *Journal of Consumer Policy*, Vol. 32, No. 3, pp. 219-244

Swartz, N. (2007). NIST issues RFID guidelines. *Information Management Journal*, Vol. 41, No. 4, p. 8

Symbol Technologies (2006). A prescription for RFID success in the pharmaceutical industry. Date of access, March 21, 2011, Available from: www.symbol.com/assets/files/rfid_uhf.pdf

Taghaboni-Dutta, F., & Velthouse, B. (2006). RFID technology is revolutionary: who should be involved in this game of tag? *Academy of Management Perspectives, Vol. 20, No. 4, pp. 65-78*

Tajima, M. (2007). Strategic value of RFID in supply chain management. *Journal of Purchasing and Supply Management*, Vol. 13, No. 4, pp. 261-273

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

Uldrich, J. (2007). Dole: let us thank RFID technology. In: *The Motley Fool*, Date of access, February 17, 2011, Available from: www.fool.com/investing/value/2007/09/rfid-saves-the-dole.aspx

Wasieleski, D.M., & Gal-Or, M. (2008). An enquiry into the ethical efficacy of the use of radio frequency identification technology. *Ethics and Information Technology*, Vol. 10, No. 1, pp. 27-40

Wicks, A.M., Visich, J.K., & Li, S. (2006). Radio frequency identification applications in healthcare. *International Journal of Healthcare Technology and Management*, Vol. 7, No. 6, pp. 522-540

Willey, L. (2007). RFID and consumer privacy: let the buyer beware. *Journal of Legal, Ethical and Regulatory Issues*, Vol. 10, No. 2, pp. 25-37

Wyld, D.C. (2006). RFID 101: the next big thing for management. *Management Research News*, Vol. 29, No. 4, pp. 154-173

Wyld, D.C., & Jones, M.A. (2007). RFID is no fake: the adoption of radio frequency identification technology in the pharmaceutical supply chain. *International Journal of Integrated Supply Chain Management*, Vol. 3, No. 2, pp. 156-171

Wyld, D.C. (2008). Radio frequency identification: advanced intelligence for table games in casinos. *Cornell Hospitality Quarterly*, Vol. 49, No. 2, pp. 134-144.

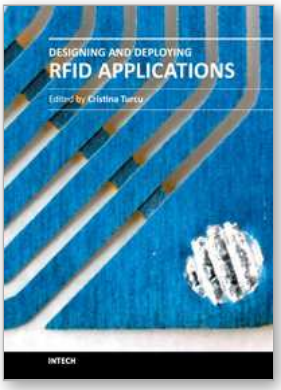
Zakaria, F. (2001). Time to save "just in time". *Newsweek*, Vol. 138, No. 20, p. 38

Zebra Technologies. (2004). RFID: the next generation of AIDC. Date of access, September 10, 2006, Available from: www.integratedlabeling.com/rfid/white_papers/11315Lr2RFIDTechnology.pdf

Zsidisin, G.A. (2003). Managerial perceptions of supply risk. *The Journal of Supply Chain Management*, Vol. 39, No. 1, pp. 14-25

Zsidisin, G.A., Panelli, A., & Upton, R. (2000). Purchasing organization involvement in risk assessments, contingency plans, and risk management: an exploratory study. *Supply Chain Management: An International Journal*, Vol. 5, No. 4, pp. 187-197

Zuo, Y. (2010). Secure and private search protocols for RFID systems. *Information Systems Frontier*, Vol. 12, No. 5, pp. 507-519



Designing and Deploying RFID Applications

Edited by Dr. Cristina Turcu

ISBN 978-953-307-265-4
Hard cover, 384 pages
Publisher InTech
Published online 15, June, 2011
Published in print edition June, 2011

Radio Frequency Identification (RFID), a method of remotely storing and receiving data using devices called RFID tags, brings many real business benefits to today world's organizations. Over the years, RFID research has resulted in many concrete achievements and also contributed to the creation of communities that bring scientists and engineers together with users. This book includes valuable research studies of the experienced scientists in the field of RFID, including most recent developments. The book offers new insights, solutions and ideas for the design of efficient RFID architectures and applications. While not pretending to be comprehensive, its wide coverage may be appropriate not only for RFID novices, but also for engineers, researchers, industry personnel, and all possible candidates to produce new and valuable results in RFID domain.

How to reference

In order to correctly reference this scholarly work, feel free to copy and paste the following:

May Tajima (2011). The Role of RFID Technology in Supply Chain Risk Management, Designing and Deploying RFID Applications, Dr. Cristina Turcu (Ed.), ISBN: 978-953-307-265-4, InTech, Available from: http://www.intechopen.com/books/designing-and-deploying-rfid-applications/the-role-of-rfid-technology-in-supply-chain-risk-management

INTECH
open science | open minds

InTech Europe
University Campus STeP Ri
Slavka Krautzeka 83/A
51000 Rijeka, Croatia
Phone: +385 (51) 770 447
Fax: +385 (51) 686 166
www.intechopen.com

InTech China
Unit 405, Office Block, Hotel Equatorial Shanghai
No.65, Yan An Road (West), Shanghai, 200040, China
中国上海市延安西路65号上海国际贵都大饭店办公楼405单元
Phone: +86-21-62489820
Fax: +86-21-62489821

© 2011 The Author(s). Licensee IntechOpen. This chapter is distributed under the terms of the Creative Commons Attribution-NonCommercial-ShareAlike-3.0 License, which permits use, distribution and reproduction for non-commercial purposes, provided the original is properly cited and derivative works building on this content are distributed under the same license.