IDEA GROUP PUBLISHING
701 E. Chocolate Avenue, Suite 200, Hershey PA 17033-1240, USA
Tel: 717/533-8845; Fax 717/533-8661; URL-http://www.idea-group.com
ITB12745

This paper appears in the book, *Emerging Trends and Challenges in Information Technology Management, Volume 1 and Volume 2* edited by Mehdi Khosrow-Pour © 2006, Idea Group Inc.

RFID: Risks to the Supply Chain

Sanjay Goel, University of Albany, State University of New York, 1400 Washington Avenue, Albany, NY 12222, SGoel@uamail.albany.edu

Jakov Crnkovic, University of Albany, State University of New York, 1400 Washington Avenue, Albany, NY 12222, yasha@uamail.albany.edu

ABSTRACT

Many businesses are incorporating RFID technology into the supply chain to improve efficiency and reduce errors, such as, late deliveries, excess inventory, and shortage of inventory. Application of this technology is very broad and is limited only by technological challenges in their design the cost of procuring them. In addition, there are several consumer concerns posed by RFID deployment, such as, privacy, security, and environmental damage. Thus far, issues with the introduction of RFID technology have been examined in isolation; a clear comprehensive view of the impact of the technology has not yet emerged. When considering RFIDs, companies typically perform a cost-benefit analysis that incorporates the deployment cost and the productivity gains. Consumer concerns in deployment of this technology also need to be incorporated in the business analysis. This paper presents a scheme for comprehensively examining the risks of deploying RFID technology using a matrix-based approach.

INTRODUCTION

Companies are increasingly adopting RFID technology for tracking goods and products, primarily through the supply chain (Sarma et al., 2003). RFID technology can be used to tag goods with special wireless sensors that respond to radio frequency probes allowing them to be detected without line-of-sight access. Coupled server data able to identify where and when the item was manufactured, how long and where it has been in the store (in the back room and/or on the shelf), its price history, its placement on the shelf (e.g. what was next to it), there is room for an in-depth analysis at several levels. Since RFID does not require direct contact or line-of-sight scanning, it provides a significant productivity advantage over traditional barcodes by allowing rapid inventory of products and providing real-time visibility to the supply chain.

Technologically, a RFID system consists of three components: 1) an antenna, 2) a transceiver, and 3) a transponder (or tag). The transponder provides the data. Together, the antenna and transceiver collect and aggregate information. There are two types of RFID tags: 1) active, and 2) passive. Passive RFID tags do not have a power source and reflect the RF-energy of the receiver's antenna. In contrast, active tags have their own power source that allows them emit RF-energy. In passive tags, the radio signal from the antenna activates the transponder, which then reflects the energy and transmits a radio signal back to the antenna. Passive tags have a lower overall cost and an indefinite lifespan because it is not dependent on battery life. Active tags can support higher data rates, increased processing speeds, and longer signal range from the tag reader to the tag.

The potential of RFID portrayed in the literature is decidedly mixed. Quotes demonstrating apprehensiveness are easy to find, such as that by Shutzberg (2004): "We believe many early adopters have underestimated the cost of implementing RFID. Moreover, faster-than-usual technology obsolescence should make RFID costlier, as additional investments will be required to leverage evolving capabilities". However, more optimistic views are also prevalent, such as that by Schwartz (2004): "RFID is going to change the way companies do business … it will give unprecedented visibility into the supply chain and will someday give companies the ability to make decisions while goods are in transit – decisions that could swing millions of dollars to the plus column". Implementation of any new technology comes with obstacles that need to be managed. Many important business challenges like establishing RFID Standards, ROI, and managing the explosion of data have been discussed in the literature (Holstein et al., 2005).

While this technology has been touted to improve efficiency in the supply chain by streamlining operations and allowing inventory levels reduction, there are significant risks to using this technology that need to be considered while evaluating its incorporation into the supply chain. Threats include spoofing, physical destruction, eavesdropping, counterfeiting, and denial-of-service (Henrici & Müller, 2004). While the risks of this technology have been discussed extensively in the literature, work on aggregating these risks to estimate organizational exposure has not been done. In this paper, we will analyze these risks and present a risk analysis framework (Goel & Chen, 2005) to model the risks of using RFIDs in the supply chain. The framework computes the exposure of the organization due to threats exploiting vulnerabilities in the supply chain. The rest of the paper is organized as follows: Section 2 presents the methodology for analyzing the RFID risks, Section 3 presents the results of the analysis, and Section 4 presents the conclusions of this work.

RISK ANALYSIS

Risk analysis is the process of systematically examining the potential losses that an organization can incur due to internal or external threats. Risk is often portrayed in terms of assets, threats, vulnerabilities, and controls where threats exploit vulnerabilities to damage assets and controls mitigate the impact of threats on the assets. The framework uses a series of matrices where assets, threats, vulnerabilities, and controls are collected, along with the probabilities correlating these parameters. Assets are items of economic value owned by an individual or an organization and can be of two types: 1) tangible assets (have a physical existence, i.e., cash, equipment, and people), and 2) non-tangible assets (cannot be physically touched, i.e., a brand, trust, and employee morale). Vulnerabilities are weaknesses in an organization (e.g., security holes in software, security procedures, administrative controls, physical layout, internal process controls, etc.) that allow unauthorized access to information or disruption of operations. Threats are sources of harm, which can exploit vulnerabilities to cause damage to organizational assets. Controls are mechanisms that can be deployed to either eliminate or mitigate the impact of threats.

The procedure that was used for risk analysis employs three matrices: 1) an asset-vulnerability matrix (data on the impact of a vulnerability on an asset), 2) a vulnerability-threat matrix (data on the potential of a threat exploiting a vulnerability), and 3) a threat-control matrix (data on the impact of a control on mitigating a threat). The data in the asset-vulnerability matrix is aggregated and cascaded into the vulnerability-threat matrix, which is then aggregated to obtain a relative ranking of different threats. Controls can be also incorporated in the analysis by cascading the aggregate information from the vulnerability-threat matrix to the threat-control matrix and then aggregating the data to obtain the relative importance of different controls. The focus of this work is collecting data on assets, threats, vulnerabilities, and controls; gathering the coefficients of sensitivity among different assets, vulnerabilities, threats, and controls; and analyzing the data to determine risk

posture and the impact of controls on mitigation of threats. More details on the procedure can be obtained from Goel and Chen (2005).

RFID risks stem from several sources, which include: security, privacy, as well as failure of tags and readers. The fundamental problem in this work is the lack of data for effective quantitative valuation of the risk impacts of this technology. For some risks, such as the failure rates of devices (e.g. transponders and receivers), data is available from the literature. However, it is more difficult to obtain accurate values from non-tangible losses such as privacy, security, and consumer acceptance. This research will employ qualitative evaluation in the risk analysis. While RFID technology is evolving and the price of tags is gradually reducing, privacy and security requirements may require technology changes that will increase additional burden. Based on trends in the industry, RFID technology will soon be so pervasive that consumer advocates will force privacy legislation on the use of such identifiers. This would likely result in significant financial impact due to compliance requirements mandating periodic audits. In addition, the RFID systems installed today may become obsolete as the technology changes and new formats and tools emerge. This work will allow organizations to determine their organizational exposure and explore the feasibility of implementing RFID technology into their supply chains. By perturbing the variables in the risk matrices, sensitivities that reflect the impact of market changes on decision-making can be computed.

OBSERVATIONS FROM THE PILOT STUDY

The observations presented here are based on a pilot study that investigates the key threats, vulnerabilities, and controls necessary for an organization, which intends to implement RFID technology into the supply chain. The final data set will be collected from different European company executives engaged in the Executive MBA joint program run by the Graduate School of Business Administration (GSBA) from Zurich, Switzerland and University at Albany. The complete data set will be reported in the journal version of the paper. The results presented here demonstrate the process followed to collect the data and to interpret the data. A series of matrices were used to collect the risk data, as discussed earlier. In the first step, the assets, threats, vulnerabilities, and controls were enumerated and added to the matrices. In the second step, the valuations were given in the matrices based on a scale of 0 (no impact), 1 (low impact), 3 (medium impact), and 9 (high impact). In the first matrix, the assets were collected and ranked, as indicated in Table 1. According to this table, reliability, productivity, communication, supply chain, and employee morale were determined to be the most important assets of the organization.

Table 2 shows the asset-vulnerability matrix that relates the assets to the vulnerabilities of the organization. The relative ranking of different assets was transferred to the asset-vulnerability matrix from the asset table (Table 1). The relative impact of each of the vulnerabilities in exposing an asset was gathered from the users and the data was aggregated to compute the relative impact of different vulnerabilities. The most important vulnerabilities were determined to be management deficiencies followed by the supply chain and market competition. A surprising observation from this was that liability appeared to be a weaker vulnerability than most of the other vulnerabilities, especially since companies are becoming increasingly concerned about liabilities.

Table 1. Assets of the organization

Assets	Examples	Valuation
Privacy	Eavesdropping	1.00
Reliability	Failures can cause excess inventory or loss of revenue	9.00
Reputation	Image that the company has outside	3.00
Product Quality	Appearance, Robustness	3.00
Productivity	Additional expenditure of adding RFID to products	9.00
Health & Safety	Excessive emf / harmful substance for injestion	1.00
Communication	Interference	9.00
Supply Chain	Disruptions through bad RFIDs, counterfiet RFIDs	9.00
Consumer Data	Consumer Data has value (Litigation)	3.00
Corporate Data	Competitive Advantage	3.00
Revenue	Driver for the business	3.00
Employee Morale	Non tangible asset that can get impacted	9.00

Table 2. Asset-vulnerability matrix

Assets	Privacy	Reliability	Reputation	Product Quality	Productivity	Health & Safety	Communication	Supply Chain	Consumer Data	Corporate Data	Revenue	Employee Morale	Aggregates (Impact)
Asset Values/ Vulnerabilities	1	9	3	3	9	1	9	9	3	3	3	9	Σ (*asset value* x *vulnerability*)
Competition (Market)	3	3	9	9	9	3	3	9	3	3	3	3	330
Supply Chain	3	9	3	3	9	3	3	9	3	3	3	1	330
Employees	0	3	3	3	3	1	1	3	1	1	3	9	205
Consumers	9	3	1	3	0	3	3	0	1	1	1	3	114
Tag Readers	0	9	3	9	9	0	1	9	0	0	0	3	315
RFID	9	3	3	3	9	3	1	9	1	9	3	3	294
Information System	3	9	3	1	1	0	9	9	3	9	3	1	321
Liability	1	1	1	3	0	0	0	3	3	3	3	3	103
Management	3	9	3	9	9	1	3	9	3	9	9	9	454
Union	9	3	3	1	3	1	3	3	3	3	3	3	184

Table 3. Vulnerability-threat matrix

Vulnerabilities	Competition (Market)	Supply Chain	Employees	Consumers	Tag Readers	RFID	Information System	Liability	Management	Union	Aggregates (Threat Impact)
Impact Values/ Threats	330	330	205	114	315	294	321	103	454	184	Σ (impact value x threat value)
Data Overflow	3	3	3	0	0	0	9	3	3	0	7155
Defective RFIDs	9	9	3	1	1	1	9	3	3	0	11838
Eavesdropping	3	3	3	3	1	1	3	1	1	1	5250
Counterfeiting	3	3	3	3	3	3	3	3	9	1	10306
Sabotage	9	9	1	1	1	1	9	3	3	3	11980
Defective RFID Readers	3	9	3	3	9	9	3	3	3	1	13216
Human Errors	3	3	0	9	3	3	9	1	1	1	8463
Illegal Monitoring (Manufacturers)	3	1	0	3	3	3	1	3	3	1	5665
Illegal Monitoring (Government)	3	1	1	9	3	3	1	1	3	3	6716
Illegal Monitoring (Stores)	3	1	9	3	3	3	1	1	3	9	8776
Theft	3	1	3	3	1	1	3	1	9	1	8222
Hacking	3	9	3	1	1	1	9	1	9	0	12376
Denial-of-Service	3	3	3	1	3	3	3	1	3	9	8620
Lawsuits	1	1	3	0	0	0	3	0	1	1	2876
Disruption of Work	1	3	3	1	1	3	3	3	3	3	6432
Incompatibility of RFID with Inf. Systems	3	9	1	0	0	3	9	1	3	1	9585
Obsolescence of Technology & Software	3	9	1	1	1	3	9	1	3	3	10382
Marginalization of Small Companies	3	1	0	0	0	0	1	0	3	3	3555

Table 4. Threat-control matrix

Threats	Data Overflow	Defective RFIDs	Eavesdropping	Counterfeiting	Sabotage	Defective RFID Readers	Human Errors	Illegal Monitoring (Manufacturers)	Illegal Monitoring (Government)	Illegal Monitoring (Stores)	Theft	Hacking	Denial-of-Service	Lawsuits	Disruption of Work	Incompatibility of RFID with Inf. Systems	Obsolescence of Technology & Software	Marginalization of Small Companies	Aggregates (Control Impact)
Impact Values/ Controls	7155	11838	5250	10306	11980	13216	8463	5665	6716	8776	8222	12376	8620	2876	6432	9585	10382	3555	Σ (threat importance x impact of controls)
RFID Dismantler	9	9	0	0	3	9	3	3	3	3	3	0	1	3	9	9	9	3	704851
Encryption	3	3	1	3	3	9	9	3	3	3	1	3	3	1	3	9	1	1	581253
Data Aggregation System	9	9	1	0	0	0	3	1	1	1	0	0	0	0	3	3	3	0	301930
Research	3	3	3	1	1	3	3	1	1	3	3	3	3	1	1	9	3	0	413134
Legislation	3	3	3	9	9	3	1	9	9	9	9	9	1	9	0	0	0	0	731713
Firewalls	1	3	3	3	3	9	3	3	3	3	0	9	1	0	9	9	9	0	690676
IDS	9	3	3	1	9	3	1	3	3	1	1	3	3	0	3	9	9	0	598024
Redundant Servers	9	9	3	3	3	3	3	1	1	1	1	3	9	1	3	3	3	1	638997
Middleware	9	9	3	1	9	3	1	1	1	1	3	9	3	0	9	9	9	3	784247

The vulnerability-threat matrix (Table 3) contains the aggregated data from the asset-vulnerability matrix and data on the chance threats would exploit any vulnerability. The largest threat was determined to be defective RFID readers, followed by hacking, defective RFID tags, sabotage, and obsolescence of technology. Surprisingly, privacy-related issues and lawsuits did not surface to the top even though these factors are receiving the greatest attention in the press.

The threat-control matrix (Table 4) shows that the most important control was middleware (software that manages data collection and security of the data). This was followed by the following categories: new legislation, RFID dismantler, and redundant server in order of importance. Research came relatively low even though the authors feel that significant research is required in order to ensure reliability of RFIDs as well as security and privacy of data collected through these sensors.

CONCLUSION

The paper emphasizes the importance of aggregating the different risks of incorporating RFID technology in the supply chain. It presents data collected in a pilot test survey and shows the interpretation of a single data sample to give readers an understanding of the process of examining risks related to use of RFID technology. This approach is adaptable wherein new assets, threats, vulnerabilities, and controls can be added to update the risk posture. In addition, the results from this approach can be used for cost benefit analysis to determine the benefit of incorporating RFIDs in the supply chain. The journal version of paper will present the final set of matrices from the data collected in the test sample. A rationalization and some directions for the future needs in the RFID field will also be provided.

REFERENCES

1. Goel, S. & Chen, V. (2005). Information Security Risk Analysis - A Matrix-Based Approach. *Proceedings of the Information Resource Management Association (IRMA) 16th International Conference*, San Diego, CA, May 2005.
2. Henrici, D., and Müller, P. (2004). Tackling Security and Privacy Issues in Radio Frequency Identification Devices. A. Ferscha and F. Mattern (Eds.): *PERVASIVE 2004, LNCS 3001*, 219-224, 2004. Springer-Verlag Berlin Heidelberg.
3. Holstein, W.K., Crnkovic, J., and Ribeiro, M. (2005) Management Issues in RFID Projects. *Proceedings of the Information Resource Management Association (IRMA) 16th International Conference*, San Diego, CA, May 2005.
4. Sarma, S.E., Weis, S.A., and Engels, D.W. (2003). RFID Systems and Security and Privacy Implications. B.S. Kaliski Jr. et al. (Eds.), *CHES 2002, LNCS 2523*, 454–469, Springer-Verlag Berlin Heidelberg.
5. Schwartz, E., (November 29, 2004). RFID: Look Before You Leap. *Information Week.*
6. Shutzberg, L. (November 1, 2004). Early Adopters Should Be Wary of RFID Costs. *Information Week*.