Jurnal Teknologi

Full paper

Risk Assessment in Securing Radio Frequency Identification (RFID) Systems: A Case Study on Petra Christian University Library

Lily Puspa Dewi*, Ibnu Gunawan, Chris Winoto

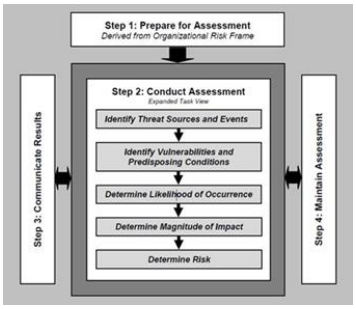
Informatics Department – Faculty of Industrial Technology, Petra Christian University, Siwalankerto 121-131, Surabaya 60292, Indonesia

*Corresponding author: lily.puspa.dewi@gmail.com

Article history

Received :1 January 2014
Received in revised form :
15 February 2014
Accepted :18 March 2014

Graphical abstract



Abstract

Each library collection has an identification number which is unique number for each book. Identification numbers are used in searching process, and library's circulation. Identification number is presented by barcode, and will be coupled with RFID, in order to facilitate collection information searching service, collection circulation service, and as a function of the collection security. The current barcode system problem lacks security features, the process of collection finding is very difficult, and the circulation process takes more time. This problem can result in losses of the library assets, and reduce library user satisfaction. Therefore, Petra Christian University Library plans to implement the RFID system as the solution of collection security. The RFID implementation process requires an analysis to be done to assess the risk factors that affect the library's business processes and provide a response to those risks. This paper discusses the risk assessments for the RFID system to be implemented in the library. Risk assessments are based on the NIST SP800-98 standard Guidelines for Securing Radio Frequency Identification (RFID) System and NIST SP800-30 Guide for Conducting Risk Assessments. Risk factors are categorized into two, namely business process risk and risk intelligence process. The results show most of the risk factors are related to the server system.

Keywords: Risk assessment; RFID; NIST; library

© 2014 Penerbit UTM Press. All rights reserved.

1.0 INTRODUCTION

Organizations in the public and private sectors depend on information technology and information systems to successfully carry out their missions and business functions. Information systems can include very diverse entities ranging from office networks, financial and personnel systems. Information systems are subject to serious threats that can have adverse effects on organizational operations and assets, individuals, and other organizations. It is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk - that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

Risk assessment is one of the fundamental components of an organizational risk management process. The purpose of risk assessments is to inform decision makers and support risk responses by identifying: (i) relevant threats to organizations or threats directed through organizations against other organizations; (ii) vulnerabilities both internal and external to organizations; (iii) impact (i.e., harm) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring) [1].

Risk management is expected to identify and analyze the risks that might occur when the project is implemented, and from these analyzes can help the companies protect and anticipated losses that may adversely affect the company. Therefore, using risk management, the company can identify risks that may occur earlier and be able to anticipate and mitigate the impact of risks.

At this time, many libraries still use barcode system for inventory control. Moreover, the barcode label is used for help librarian in circulation process such as lending collection for library users, checking in collection returned, and monitoring collection for damage and routing them to the appropriate staff for repair or replacement. The barcode label results in speed and accuracy at a central lending and return point. The barcode system cannot be used as security for collection theft. It needs a separate electromagnetic detection system for theft [2].

Currently, Petra Christian University library plans to implement the Radio Frequency Identification (RFID) system. The RFID system has the ability to store information relating to the specific item which they are attached to. It facilitates multiple, automatic object identification, tracking, sorting as well as speedier data collection, which tremendously improves the efficiency of

libraries, thereby freeing librarians to provide other value added services, such as assisting in library information searching, providing a more desirable document format, supplying more accurate, current, and reliable information and documents [3]. Library theft prevention is easy to manage as it is built into the RFID technology. Using a single RFID technology can achieve both inventory management and library security.

Therefore, in this research we propose a risk assessment related to library security using RFID system. The library can identify and analyze the risks that might arise. In addition, the library can anticipate problems and risks that arise, thus they will not affect the library operation. We conduct the risk assessment as illustrated in Step 2 as in Figure 1.

■2.0 LITERATURE REVIEW AND PREVIOUS RELATED WORK

2.1 Radio Frequency Identification (RFID)

Radio Frequency Identification, or RFID, is a generic term for technologies that use radio waves to automatically identify individual items. Several libraries around the world announced their intent to integrate RFID technology into their library systems, pioneering its use for contemporary library functions [4].

A comprehensive RFID system has four components: (i) RFID tags that are electronically programmed with unique information, (ii) Readers or sensors to query the tags, (iii) Antenna, (iv) Server on which the software that interfaces with the integrated library software is loaded [5]. RFID Tag, also known as smart label, consists of an integrated circuit and an antenna combined to form a transponder. Smart labels collect the energy to operate from a Radio Frequency (RF) field emitted by a reader device; therefore they do not need a battery. When energized by a radio signal from a fixed position reader or handheld scanner, the tag returns the stored information in order that the item to which it is attached can be easily located.

RFID Tag comes in all shapes, sizes and read ranges. It is thin, flexible and thus can be laminated between paper and plastic. Patron is totally unaware that the tag is there. An additional advantage of using RFID tags is the built-in EAS (Electronic Article Surveillance), an in-built feature addressing the anti-theft requirements. The various types of RFID tags are used for different materials in the library such as a book, magazine, CD-ROM or Video Cassette tape.

2.2 NIST SP800:30 Rev1 Guide for Conducting Risk Assessments

The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., adverse impact) that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., typically a function of the degree of harm and likelihood of harm occurring) [1].

The risk assessment framework is done as describe in Figure 1. The first step in the risk assessment process is to prepare for the assessment. The key activities are identifying the purpose, and scope of the risk assessment. The second step in the risk assessment process is to conduct the assessment. The objective of this step is to produce a list of information security risks that can be prioritized by risk level and used to inform risk response decisions. The third step in the risk assessment process is to communicate the assessment results and share risk-related information. The objective of this step is to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions. The fourth step in the risk assessment process is to maintain the assessment. The objective of this step is to keep current, the specific knowledge of the risk organizations incur. The results of risk assessments inform risk management decisions and guide risk responses [1].

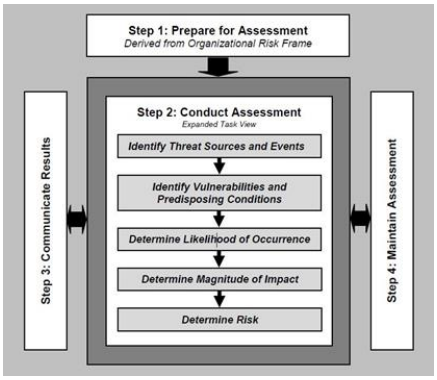


Figure 1 Risk assessment processes

In the NIST SP800-30 rev1, weighing of the risk is done based on the *likelihood of threat event initiation* (how often the threat will occur or appear), *likelihood of threat event resulting in adverse impacts* (impact of losses caused by the threat), and the results of the above assessments adjusted back into the *overall likelihood.* Table 1 shows the assessment scale.

Table 1 Assessment scale – overall likelihood
Source: NIST 800:30 Rev 1 guide for conducting risk assessments

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

The next stage is to determine the adverse impacts from threat events of concern considering: (i) the characteristics of the threat sources that could initiate the events; (ii) the vulnerabilities/predisposing conditions identified; and (iii) the susceptibility reflecting the safeguards/countermeasures planned or implemented to impede such events. The matrix for determining the impact scale is shown in Table 2.

Table 2 Determination of impact scale
Source: NIST 800:30 Rev 1 guide for conducting risk assessments

Qualitative Values	Semi-Quantitative Values		Description
Very High	96-100	10	The threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	80-95	8	The threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation. A severe or catastrophic adverse effect means that, for example, the threat event might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life-threatening injuries.
Moderate	21-79	5	The threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A serious adverse effect means that, for example, the threat event might: (i) cause a significant degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is significantly reduced; (ii) result in significant damage to organizational assets; (iii) result in significant financial loss; or (iv) result in significant harm to individuals that does not involve loss of life or serious life-threatening injuries.
Low	5-20	2	The threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation. A limited adverse effect means that, for example, the threat event might: (i) cause a degradation in mission capability to an extent and duration that the organization is able to perform its primary functions, but the effectiveness of the functions is noticeably reduced; (ii) result in minor damage to organizational assets; (iii) result in minor financial loss; or (iv) result in minor harm to individuals.
Very Low	0-4	0	The threat event could be expected to have a **negligible** adverse effect on organizational operations, organizational assets, individuals other organizations, or the Nation.

Organizations assess the risks from threat events as a combination of likelihood and impact. The level of risk associated with identified threat events represents a determination of the degree to which organizations are threatened by such events. Organizations make explicit the uncertainty in the risk determinations, including, for example, organizational assumptions and subjective judgments/decisions. Organizations can order the list of threat events of concern by the level of risk determined during the risk assessment—with the greatest attention going to high-risk events. Organizations can further prioritize risks at the same level or with similar scores [1].

Table 3 Assessment scale – level of risk
(combination of likelihood and impact)
Source: NIST 800:30 Rev 1 guide for conducting risk assessments

Likelihood (Threat Event Occurs and Results in Adverse Impact)	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

2.3 NIST SP800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems

The major high-level business risks associated with RFID systems so that organizations planning or operating these systems can better identify, characterize, and manage the risk in their environments [6]. The risks are as follows:

- Business Process Risk. A direct attacks on RFID system components and potentially could undermine the business processes the RFID.
- Business Intelligence Risk. An adversary or competitor potentially could gain unauthorized access to RFID-generated information and use it to harm the interests of the organization implementing the RFID system.

According to NIST SP800-98 Standard Guidelines for Securing Radio Frequency Identification (RFID) Systems, we need to hold a analysis to determine that the RFID project align with the goals of the library, and to know the importance of RFID in the Petra Christian University Library [6]. We do this analysis by using the Boston Consulting Group (BCG) Matrix.

2.4 Boston Consulting Group (BCG) Matrix

BCG matrix is a table that has been created by Bruce Henderson for the Boston Consulting Group in 1968 [7]. The Boston Consulting Group (BCG) Matrix is a simple tool to assess a company's position in terms of its product range. The point of this matrix is to help companies/nonprofits understand the current position and potential growth of their different products. It helps a company think about its products and services and make decisions about which it should keep, which it should let go and which it should invest in further. In the BCG matrix is divided into four positions, namely: Dogs, Stars, Question Marks, and Cash Cow, as shown in Figure 2.

Figure 2 BCG matrix
Source: Perspectives on Strategy from the Boston Consulting Group

Cash cows have a high market share but low growth. For nonprofits, in this case is for the library, these are usually the big contracts from foundations and corporate partners. They often make e bulk of donation income (such as books, AV collection) and are unlikely to get any bigger. These are worth maintaining, but are not likely to be the source of long-term growth.

Dogs are low income sources in a highly competitive market. They are usually very inefficient, barely break-even and sometimes make a loss. Because of their low return on investment (ROI), too much money is spent on administration and fundraising, which is a big turn off for donors. They therefore have little scope for growth and are probably not worth continuing. Activities related to dogs could be small community events, selling donated products, door-to-door fundraising and low-value time-intensive grants.

Question marks grow quickly but eat up a lot of cash and don't have a large market share. However, what separates them from dogs is their growth potential. The classic example for charities is a direct mail or marketing program. They cost a lot of money to set-up and run for the first year or two, but if done correctly they can bring in lots of core donations and build up the 'donor pyramid' (i.e. turn long-term supporters into major donors and planned givers/legacies). Questions marks can turn into stars, cash cows or (if managed incorrectly) dogs.

Stars have high market share and high growth. The hope is that they will turn into cash cows. For nonprofits, this is what all your hard fundraising and development work is for: to cultivate

stars though relationship building and converting them into cash cows. So, stars could be major donor prospects, your planned giving/legacy program, small grants/contracts that could turn into bigger ones [7].

3.0 DATA GATHERING

3.1 Identify Threat Source and Events

The data gathering process is conducted by doing an interview with the head of the library and librarians based on the BCG matrix. The purpose of this interview is to determine the RFID presences in the library that will be influential in determining the value of risk were found.

From the interview with the librarians, we obtained information that RFID requires substantial funds at first but the results are not yet visible at this time. But RFID has the potential to improve the library service, thus it would increase user satisfaction. This shows that library is in the *question mark* position and the RFID project already align with the goals and mission of Petra Christian University Library.

3.2 Identify Vulnerabilities and Predisposing Conditions

The next step is conducting interview for Business Process Risk and Intelligence Process Risk. The business process risk interview is done to the head of the library and library staff. This interview aims to gather data for identifying the risks that arise in the Business Process risk. The interview is based on the NIST document SP800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems. Some points of the interview are:

- The RFID durability against physical interference either intentionally or unintentionally (Disruption of physical contact, water).
- The effectiveness and efficiency of the security of the RFID system
- Subsystem failure. The effect other systems, when the RFID system is failed, and how big the impact is.
- Relationships between RFID system and the library mission. It will be fatal effect when RFID is experiencing a failure or disruption when RFID is the important system for library mission.
- The backup system. The readiness of other system for replacing RFID system when it is failed (fallback).
- The duration needed for the replacing RFID system (fallback) and the recovery time needed to fix RFID damaged.
- Security control. The stronger the controls and countermeasures, the lower the risk.
- Business process risk mostly caused by human activity, either intentionally or unintentionally. Unlike most of the other risks, business process risk can occur as a result of both human action and natural causes. Moreover, human causes may be intentional or unintentional. For example, a tag might fail to perform its intended function because someone removed it from its packaging, an employee accidentally damaged it with a box cutter, or a severe storm covered it in ice.
- The potential risk is not only in RFID subsystem, but when it connected to the network, thus the risk spreads to the network as well.

The second interview aimed to collect data necessary to identify the risks that arise in the Risk Intelligence Process. Some interview points are based on the NIST document SP800-98 Guidelines for Securing Radio Frequency Identification (RFID) Systems. The points are:

- Unauthorizaed partieds. A competitor or adversary can gain information from the RFID system in a number of ways, including eavesdropping on RF links between readers and tags, performing independent queries on tags to obtain relevant data, and obtaining unauthorized access to a back-end database storing information about tagged items. Supply chain applications may be particularly vulnerable to this risk because a variety of external entities may have read access to the tags or related databases. The risk of unauthorized access is realized when the entity engaging in the unauthorized behavior does something harmful with that information.
- Security control. The use of controls such as database access controls, password-protection, and cryptography can significantly mitigate business intelligence risk if applied properly.
- Location. When tagged items are located in public areas (library), business intelligence risk is considerably higher than it would be if tags stay within access-controlled facilities. Another consideration is the ability of radio communication to occur beyond the physical perimeter. For example, if an adversary can read tags outside of a facility's fence, then the business intelligence risk is higher than it would be if signals were limited to a few feet and could not easily penetrate walls. The physical location of supporting IT infrastructure can also play a role in risk determination.

3.3 Determine Likelihood and Occurrences

The risk assessment (according to the *likelihood of thread event initiation* and *likelihood of threat events resulting in adverse impacts*) found from interviews Business Process Risk and Intelligence Process as in Table 4. Assessor scale was taken according to NIST SP 800:30 rev 1.

3.4 Determine Magnitude of Impact

The literature describes adverse impacts in terms of the potential harm caused to organizational operations and assets, individuals, and other organizations. Where the threat event occurs and whether the effects of the event are contained or spread, influences the severity of the impact. Assessing impact can involve identifying assets or potential targets of threat sources. The magnitude of impact is shown in Table 5.

Table 4 Risk assessment according to the likelihood of threat events initiation

	Risk List	Initiation	Adverse impact	Overall
Fallback system				
1	The fallback system is not ready to replace RFID systems.	Very Low	High	Low
Effects when RFID is failed				
2	The circulation process will take more times using barcode system	Moderate	High	Moderate
3	Collection safety	Moderate	High	Moderate
4	Problem in collection inventory	Moderate	High	Moderate
5	Collection information retrieval will take more time	Moderate	High	Moderate
Providing plastic cover will minimize the physical risks of the collection				
6	Fatal physical contact (either intentionally or unintentionally)	Moderate	High	Moderate
7	User vandalism causing by absence of CCTV	Moderate	Very High	High
Recovery for damaged RFID				
8	RFID tag is damaged	Moderate	High	Moderate
9	RFID reader is damaged	Low	High	Moderate
Physical server security				
10	Physical contact that make server hang, down, and crash	Low	Very High	Moderate
11	Temperature, dust, humidity that make server hang, down, and crash	Low	Very High	Moderate
12	Security for the server room.	Low	Very High	Moderate
13	The absence of CCTV for server room	Low	Very High	Moderate
Privilege				
14	There are two part timer students who know the server password	Low	Very High	Moderate
15	The possibility of other person who access the server	Very Low	Very High	Low
Sofware server security				
16	Linux based server	Low	Very High	Moderate
Network topology				
17	The absence of network topology documentation might cause difficulty in RFID network maintenance	Very Low	Low	Very Low

Table 5 Determination of impact

	Risk List	Score	Category
Fallback system			
1	The fallback system is not ready to replace RFID systems.	5	Moderate
Effects when RFID is failed			
2	The circulation process will take more times using barcode system	0	Very Low
3	Collection safety	5	Moderate
4	Problem in collection inventory	2	Low
5	Collection information retrieval will take more time	5	Moderate
Providing plastic cover will minimize the physical risks of the collection			
6	Fatal physical contact (either intentionally or unintentionally)	2	Low
7	User vandalism causing by absence of CCTV	5	Moderate
Recovery for damaged RFID			
8	RFID tag is damaged	2	Low
9	RFID reader is damaged	2	Low
Physical server security			
10	Physical contact that make server hang, down, and crash	8	High
11	Temperature, dust, humidity that make server hang, down, and crash	8	High
12	Security for the server room.	8	High
13	The absence of CCTV for server room	8	High
Privilege			
14	There are two part timer students who know the server password	8	High
15	The possibility of other person who access the server	8	High
Sofware server security			
16	Linux based server	8	High
Network topology			
17	The absence of network topology documentation might cause difficulty in RFID network maintenance	2	Low

3.5 Determine Risk

The next stage is to determine the risk to the organization from threat events of concern considering: (i) the impact that would result from the events; and (ii) the likelihood of the events occurring. Input from Tables 4 and 5 are compiled to form Table 6.

Table 6 determination of risk

	Risk List	Overall Likelihood	Impact
Fallback system			
1	The fallback system is not ready to replace RFID systems.	Low	Moderate
Effects when RFID is failed			
2	The circulation process will take more times using barcode system	Moderate	Very Low
3	Collection safety	Moderate	Moderate
4	Problem in collection inventory	Moderate	Low
5	Collection information retrieval will take more time	Moderate	Moderate
Providing plastic cover will minimize the physical risks of the collection			
6	Fatal physical contact (either intentionally or unintentionally)	Moderate	Low
7	User vandalism causing by absence of CCTV	High	Moderate
Recovery for damaged RFID			
8	RFID tag is damaged	Moderate	Low
9	RFID reader is damaged	Moderate	Low
Physical server security			
10	Physical contact that make server hang, down, and crash	Moderate	High
11	Temperature, dust, humidity that make server hang, down, and crash	Moderate	High
12	Security for the server room.	Moderate	High
13	The absence of CCTV for server room	Moderate	High
Privilege			
14	There are two part timer students who know the server password	Moderate	High
15	The possibility of other person who access the server	Low	High
Sofware server security			
16	Linux based server	Moderate	High
	Network topology		
17	The absence of network topology documentation might cause difficulty in RFID network maintenance	Very Low	Low

Level of risks can be divided into 5 levels, namely Very Low, Low, Moderate, High, and Very High [1]. Table 7 shows the mapping between likelihood and impact of the level of risk.

Table 7 Mapping level of risk

Likelihood	Level of Impact				
	Very Low	Low	Moderate	High	Very High
Very High	Very Low	Low	Moderate	High	Very High
High	Very Low	Low	Moderate	High	Very High
Moderate	Very Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Low	Moderate
Very Low	Very Low	Very Low	Very Low	Low	Low

Based on Table 5, the risks can be grouped as below:

Very Low : Risk no. 2, and Risk no. 17
Low : Risk no. 1, Risk no. 3, Risk no. 4, Risk no. 5, Risk no. 6, Risk no.8, Risk no.9 and Risk no. 15.
Moderate : Risk no. 7, Risk no. 10, Risk no. 11, Risk no. 12, Risk no. 13, Risk no. 14, and Risk no.16.
High : -
Very high : -

6.0 CONCLUSION

The RFID system has tremendous influence both in terms of security collection security; find the book that misplaced in the shelf, as well as for the process of circulation. And these factors aim to increase user satisfaction and to realize the mission of the university is a campus-based IT.

Risk level might be determined by qualitative calculations, using standard NIST SP800: 98. It gives the mapping of risk calculation by using qualitative, i.e. with manual tables according to the risk characteristics.

There are two categories of risk assessment as the result of this study. The moderate risks show that the absence of CCTV in library has a possibility for library user do some vandalism; the server location has possibility a physical contact to the server that make server hang, down, and crash; temperature, dust, humidity of server room that make server hang, down, and crash; security for the server room has possibility for anyone can go inside; the absence of CCTV for server room; library's part timer students know the server password and gain access to its root server; Linux based server which has a good stability, durability and open source but require special person as a server administrator. The low risks have four kind of risk. The first is there is no special fallback system to substitute the RFID system. When it happens, library will use the old system to substitute RFID such as circulation process, securing collection and inventory process. The second risk is physical damaged for RFID tag has been prevented by giving plastic and extra label. The third risk is when RFID tag and reader are damaged, there is a backup system using barcode system, tag and reader. The last risk is possibility of other person who access the server is low.

Acknowledgement

We would like to express our deepest appreciation to our research partners that have provided data and information.

References

[1] National Institute of Standards and Technology. 2012. *NIST 800:30 Rev 1 guide for conducting risk assessments*. Retrieved September 3, 2013, from http://csrc.nist.gov/publications/nistpubs/800-30-rev1/sp800_30_r1.pdf.

[2] Houeida Kammourie-Charara. 2005. *Technology and libraries: RFID vs barcode.* Alexandria: Egypt. MELCOM International 27th Conference.

[3] Richard T. Sweeney. 1997. *Creating Library Services with Wow! Staying Slightly Ahead of the Curve.* Library Trends. 46(1): 129–151.

[4] American Library Association. 2013. *RFID and Libraries: ALA Library Fact sheet number 25.* Retrieved September 19, 2013, from http://www.ala.org/tools/libfactsheets/alalibraryfactsheet25.

[5] Syed MD. Shahid. 2005. *Use of RFID Technology in Libraries: a New Approach to Circulation, Tracking, Inventorying, and Security of Library Materials*. Library Philosophy and Practice. 8(1).

[6] National Institute of Standards and Technology. 2012. *NIST 800:98 Guidelines for Securing Radio Frequency Identification (RFID) Systems*. Retrieved September 3, 2013, from http://csrc.nist.gov/publications/nistpubs/800-98/SP800-98_RFID-2007.pdf

[7] Carl W. Stern, George Stalk, Jr. 1998. *Perspectives on Strategy from the Boston Consulting Group*. Toronto: Wiley.