AN IMPACT OF INFORMATION SECURITY BREACH ON HOTEL GUESTS' PERCEPTION OF SERVICE QUALITY, SATISFACTION, WORD-OF-MOUTH AND REVISIT INTENTIONS

FOR MASTER OF SCIENCE DEGREE

by

Ekaterina Berezina

A thesis submitted to the Faculty of the University of Delaware in partial fulfillment of the requirements for the degree of Master of Science degree in Hospitality Information Management major

Spring 2010

AN IMPACT OF INFORMATION SECURITY BREACH ON HOTEL GUESTS' PERCEPTION OF SERVICE QUALITY, SATISFACTION, WORD-OF-MOUTH AND REVISIT INTENTIONS

by

Ekaterina Berezina

Approved: _____
Cihan Cobanoglu, Ph.D.
Associate Professor, Department of Hotel, Restaurant and Institutional Management

Approved: _____
Robert R. Nelson, Ph.D.
Chair of the Department of Hotel, Restaurant and Institutional Management

Approved: _____
Conrado M. Gempesaw II, Ph.D.
Dean of the Alfred Lerner College of Business and Economics

Approved: _____
Debra Hess Norris, M.S.
Vice Provost for Graduate and Professional Education

I certify that I have read this thesis and that in my opinion it meets the academic and professional standard required by the University as a thesis for the degree of Master of Science.

Signed: _____

Cihan Cobanoglu, Ph.D.
Professor in charge of thesis

I certify that I have read this thesis and that in my opinion it meets the academic and professional standard required by the University as a thesis for the degree of Master of Science.

Signed: _____

Brian L. Miller, PhD.
Member of thesis committee

I certify that I have read this thesis and that in my opinion it meets the academic and professional standard required by the University as a thesis for the degree of Master of Science.

Signed: _____

Francis A. Kwansa, Ph.D.
Member of thesis committee

ACKNOLEDGEMENTS

Finishing my largest project for the Master's degree at the University of Delaware, I would like to thank all those people who supported me on this challenging way, contributed to my success and helped me to come to this point.

I owe my deepest gratitude to Dr. Cihan Cobanoglu, my major advisor and chair of my thesis committee. He has made his support available in a number of ways. I would like to thank Dr. Cobanoglu for his help with developing my research skills and teaching me how to write academic papers. He made himself available to me and spent a lot of time sorting out my ideas, helping me to design the study and answering my questions. I value the guidance, support and courage that I received from Dr. Cobanoglu on the way to my goal. I cannot thank him enough for his friendship, care and advice throughout all my time in HRIM. Dear Dr. Cobanoglu, I greatly appreciate your contribution to my academic and personal growth!

I would like to show my gratitude to Dr. Brian Miller, a member of my thesis committee, for his positive attitude and personal attention. Dear Dr. Miller, thank you very much for your time and contribution to my thesis. I am very grateful for your ideas and advice how to make my work better. It is my great pleasure to thank Dr. Francis Kwansa, a member of my thesis committee, for his academic advice. I am very grateful for his constructive criticism, for his attempts and success in "making me think".

My sincere appreciation goes to Mr. Dorian Cougias for sharing my research interests and funding for this project. I would not perform this well without his support. I am also very grateful to the AH&LA Technology & E-Business Committee for helping with this research and also for funding my previous study.

It is an honor for me to have been working with Dr. Robert Nelson, the chair of the department. I would like to thank Dr. Nelson for his kindness, support and understanding. I have learned a lot while working together with Dr. Nelson. I would like to thank Ms. Donna Laws, assistant to the chair of the department, for involving me in HRIM life and working with me on numerous interesting projects. I greatly appreciate her English lessons, help, understanding and flexibility.

There are a lot of other wonderful people who helped me during my education at the University of Delaware. My sincere appreciation goes to all HRIM faculty, staff and my HIM classmates for their care and contribution to my learning experience. I also would like to thank my colleagues from other universities: Dr. Mehmet Erdem, Dr. Natasa Christodoulidou and Dr. Clark Hu.

This achievement would not be possible without my friends. I owe them great appreciation. They include but are not limited to Daria Mikheeva, Inara Rezyapova, Natalya Kolyesnikova, Anton Zuykov. Thank you all for your understanding, care, support and help.

And last, but not least, I am very grateful to my family that brought me to the stage where I am right now. I would like to say my special words of appreciation to my mother, Liudmila Kozlechkova, for her unconditional love, understanding, patience and

endless support; to my father, Andrey Berezin, for his care and contribution to my personal growth and education; to my step-father, Yury Kozlechkov, for his kindness, understanding and support to me and my mother over the years.

I would not achieve my goal without all these people. Thank you all again!

DEDICATION

This thesis is dedicated to my mother, Liudmila Kozlechkova.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

LIST OF DEFINITIONS

Information security	Information and information system protection from unauthorized access, use, disclosure
Information security breach	A failure to protect information and information system from unauthorized access, use, disclosure
Payment card industry data security standards (PCI DSS)	A set of requirements for all credit card processing companies aimed to enhance information security and minimize the risk of information security breach
Service quality	A level of service delivery based on the customer perception (Zeithaml, Bitner, & Gremler, 2006)
Satisfaction	A postpurchase evaluation of product quality given prepurchase expectations (Kotler, Bowen, & Makens, 2003)
Word of Mouth	Likelihood of recommending a hotel to relatives and friends by hotel guests
Revisit intentions	Likelihood of coming back to a hotel expressed by hotel guests
Experimental research design	A research design that involves the manipulation of

one or more independent variables by the investigator and random assignment of subjects to experimental groups or treatments (“Design and Analysis of Experimental and Quasi-Experimental Investigations,” 2003)

ABSTRACT

Importance of information technology for hotel operations cannot be denied. However, the advantages, that different applications employed in the lodging industry provide, come together with potential threats. One of them is information vulnerability. Statistics say that about 55% of the credit card breaches happen in the hospitality industry (Cougias, 2008 in Haley & Connolly, 2008). The primarily purpose of this study is to investigate an impact of information security breach on hotel guests' perceived service quality, satisfaction, likelihood of recommending a hotel to others and revisit intentions.

574 US travelers participated in the experimental study. The respondents were exposed to three different scenarios: negative, where an information security breach happened in the hotel where a person stayed last and guest information was compromised; neutral, that introduces the case of information security breach where guest information stayed safe; and a positive one that tells participants about comprehensive security audit in a hotel where they stayed last which means that information is properly handled and secured. The results of the study revealed a significant impact of the treatments on three out of four variables: satisfaction, likelihood of recommending a hotel to others and revisit intentions.

Chapter 1

INTRODUCTION

1.1 Introduction

Information technology advances play an important role in social progress and economic growth (Brown & Ulijn, 2004). They also lead to many innovations and new enterprises. Computers and computer networks have drastically increased the amount and speed of information processing. Development of the internet has changed the nature of communication in businesses. It also established a platform for electronic commerce altering merchandising, advertising and product distributing practices.

Advances in information technology have changed the way of doing business in many industries including lodging. Hospitality technology applications employed in hotels are credited with providing a basis for competitive advantage, productivity improvement, enhanced financial performance, and guest service expansion (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007; Kim, Lee, & Law, 2008; Siguaw, Enz, & Namasivayam, 2000). Technology adoption has significantly increased hotels' offerings to their guests (e.g. in-room technology amenities, on-line reservations and payments). It has also made an impact on the hotel front- and back-office operations

including different spheres such as reservations, check-in/out, guest accounting, housekeeping, payroll, recruiting and others.

However, beginning from the early stage of technology adoption by the hospitality industry in the 1970s (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007; Sammons, 2000) security problems started to emerge (Varga, 1975). The problems include the loss of information stored or transmitted electronically and/or ability to perform important functions. The causes of such problems include hardware or software malfunctions or intentional unauthorized actions by a third party. Information security breach is the term used to describe failure to protect information and information system from unauthorized access, use or disclosure. The nature of hotel operations require them to obtain a lot of guest personal information for reservation purposes and for supporting customer loyalty programs. It is important to note, that information is one of the most valuable resources and assets that a company can possess. Breach of hotel guest personal information can result in identity theft. Identity theft is the misuse of somebody's personal information by a third party in order to obtain a personal gain or commit a crime ("2009 Identity Theft Statistics," 2009; Federal Trade Commission, 2010). According to the Federal Trade Commission (2010) in 2009 identity theft complaints accounted for 21% of all consumer complaints in the United States. In the category of identity theft, credit card fraud was the most frequently reported (17%). Based on this, credit card information security breach was chosen as a primary focus of this thesis to investigate the potential impact of information security breach on hotel guests.

Payment card transactions have become an essential part of hotel operations (Cobanoglu, 2007; Hobson and Ko, 1995; Levin & Hudak, 2009; Tenczar, 2008; Volpe, 2009). With the increasing number of credit card transactions, cardholders' information security has become an important issue. It is difficult to imagine in today's environment a hotel competing in the market without accepting credit cards. However, the convenience of cashless payments causes issues of private information vulnerability and security breaches for hotels. To help all companies to address these problems, the Payment Card Industry Data Security Standards (PCI DSS) were developed by the major credit card issuing companies: Visa, MasterCard, American Express, Discover, and the JCB. The current PCI DSS version 1.2 requires all companies accepting payment cards (merchants) to be PCI-compliant. Even though PCI compliance does not provide complete protection from data security breaches, failure to comply leaves more chances for hackers to commit fraud and steal sensitive information (Collins and Cobanoglu, 2008). The hotel industry is very attractive for hackers' attacks because of traditionally low computer and network security practices employed by hotels (Cobanoglu & DeMicco, 2007). In the United States "upwards of 55% of credit card fraud comes from the hospitality industry (Cougias as cited in Haley & Connolly, 2008, p.1), and the smallest merchants (known as "Level 4" merchants) account for over 85% of the compromises, with a noticeable increase in risks coming from franchisees" (Haley & Connolly, 2008, p.1). This provides strong reasons for hospitality companies to comply and be vigilant about the latest changes in PCI DSS requirements and to invest in compliance. Among the potential consequences

for hoteliers for non-compliance can be financial cost, brand reputation damage, and/or consumer behavior alterations.

1.2 Problem Statement

A closer look at the consequences of the information security breach mentioned in the literature reveals that the financial consequence is clear, however, the impact of the breach on hotels' reputation and consumer behavior has received little attention. Therefore, the latter was chosen as the primary focus of this research study.

Even though information security is not the primary service provided by hotels, it is expected that the information collected from travelers will be properly handled and secured. The hospitality literature suggests, that "one should view information security as an invaluable and expected guest service" (Connolly & Haley, 2008). The question that comes from that suggestion is: how will hotel guests perceive the quality of this service and overall service quality of a hotel where they stayed in case of information security breach?

Service quality is a level of service delivery based on customer perception (Zeithaml et al., 2006). It is not a stand-alone notion; service quality is part of a broader concept of customer satisfaction and loyalty (Zeithaml et al., 2006). Satisfaction refers to the post-purchase evaluation of product quality given pre-purchase expectations (Kotler, Bowen, & Makens, 2003). Customer is satisfied when post-purchase evaluation reveals service quality higher than guests' expected service quality. This situation is the goal for all companies. However, in case when service failure happens, service performance

cannot meet customers' expectations, which causes customer dissatisfaction. Following this logic, the study investigates if the failure to protect hotel guests' information (as a part of hotel's service) will result in guest dissatisfaction; and whether favorable information about guest information security practices will increase guest satisfaction. Above that, literature suggests that guests' satisfaction increases likelihood of recommending a hotel to others (word-of-mouth) and likelihood of coming back to the property (loyalty/revisit intentions) (Boulding, Karla, Staelin, & Zeithaml, 1993; Skogland & Siguaw, 2004; Yee, Yeung, & Cheng, 2009). The study ties all these elements in one model and investigates the impact of information security breach on all of them.

1.3 Research Questions

Based on the findings from the literature described above the following research questions were formulated for the study:

1. Is there an impact of information security breach on hotel guests' perception of service quality?
2. Is there an impact of information security breach on hotel guests' satisfaction?
3. Is there an impact of information security breach on hotel guests' likelihood of recommending a hotel to others (word-of-mouth)?
4. Is there an impact of information security breach on hotel guests' likelihood of coming back (revisit intentions)?

The identified research questions aim to close the gap in the academic literature and to provide researchers and industry with the answers about the impact of information security breach on hotel guests and their behavior.

To answer the research questions the study proceeds with the review of relevant literature, presents rationale for the study and states the hypotheses. The following chapters describe methodology, proposed plan for data analysis, data collection and findings. The results of the study are presented and discussed in the conclusions section along with limitations and recommendations for future research.

Chapter 2

REVIEW OF LITERATURE

2.1 Credit Cards and Identity Theft

Being initially introduced as a credit instrument, credit cards became an "extremely popular payment instrument" in the United States (Chakravorti, 2003). According to the Federal Reserve's Survey of consumer finances, 73% of families in the United States had credit cards in 2007 (Bucks, Kennickell, Mach, & Moore, 2009). The number of payment cards with credit functions issued in the country showed a constant growth from about 1.25 billion in 2004 to almost 1.33 billion in 2007 (Committee on Payment and Settlement Systems, 2009). However, this number decreased to 1.28 billion in 2008. At the same time the number of credit card transactions grew from about 19.13 billion in 2004 to about 23.90 billion in 2008. These figures represent total number of credit card transactions of Visa, MasterCard, Discover, American Express, Diners Club and retailer cards. The value of transactions was also growing from $1,606.9 billion in 2004 to $2,148.5 billion in 2008.

Credit card participants include consumers and their financial institutions (issuers), merchants and their financial institutions (acquirers), and credit card network/operators (Chakravorti, 2003; Chakravorti & To, 2007; Hunt, 2003).

Participation in this network provides particular advantages and disadvantages for both consumers and merchants.

Using credit cards, customers receive a "secure, reliable, and convenient means of payment" (Chakravorti, 2003, p. 52). Credit cards allow consumers to pay off their bills in full and on time. With the development of credit card system and the Internet, credit cards have become one of the essential means of an online payment system that provides efficiency, flexibility, and convenience to consumers (He & Mykytyn, 2007). Disadvantages of using credit cards for consumers include being not able to pay back the bills when they are due and incurring associated fees. From merchants' perspective credit card acceptance allows merchants to increase their sales and profits (Ernst and Young, 1996 as cited in Chakravorti, 2003) as well as to sell their goods and services to "illiquid customers or those paying with future income" (Chakravorti, 2003, p. 53). However, credit cards present the most expensive financial instruments comparing to cash, checks and debit cards (Chakravorti, 2003, Hunt, 2003).

Another disadvantage for both customers and merchants associated with credit card payments is credit card fraud: stealing money electronically and personal information vulnerability ("2009 Identity Theft Statistics ," 2009); Grabosky, Smith, & Dempsey, 2001; Smith & Grabosky, 1998). Identity theft can be identified as misuse of somebody's personal information by a third party in order to obtain a personal gain or commit a crime ("2009 Identity Theft Statistics," 2009; ("Federal Trade Commission," 2010). The Consumer Sentinel Network (CSN), a secure online database of millions of consumer complaints that is available only to law enforcement, recorded 1.3 million

complaints in 2009 including 54% fraud complaints; 21% identity theft complaints; and 25% other types of complaints ("Federal Trade Commission," 2010). In the category of identity theft, credit card fraud was the most frequently reported (17%).

2.2 Information Security and the Hospitality Industry

Information technology (IT) has become an integral part of the hospitality industry (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007). Hospitality technology applications are credited with providing a basis for competitive advantage, productivity improvement, enhanced financial performance, and guest service expansion (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007; Kim et al., 2008; Siguaw et al., 2000).

The guest cycle for hospitality organizations in the 1950s was completely manually operated. Computer penetration in the industry started in the 1960s and at that time only covered back office applications (Kasavana, 1978). In the 1970s information systems started to appear in different areas of hotel operations including reservations, check-in/check-out, guest accounting, and night audit. At that time, reservation modules were being developed to interact with the total hotel system. The use of technology provided for faster and more accurate check-in and speeded up the check-out process for guests who paid with credit cards. Accounting modules brought more accuracy in the postings of charges to guest folios. Deployment of information systems in hotels was justified by the increased amount of information that could be processed as well as enhanced employee productivity, guest satisfaction, and profits (Sheldon, 1983). The trends of the hospitality technology development in early 1980s were seen in improved

system interfacing capabilities within hotels, between hotels in a chain, travel agents and airline networks. Sheldon suggested as early as 1983 that interfacing the latter systems with electronic funds transfer would allow instant billing to credit cards.

However, starting from the early stage of technology adoption by the hospitality industry in 1970s (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007; (Sammons, 2000) the security problems started to emerge (Varga, 1975). Those problems were identified not only as hardware or software malfunctions but as a loss of important features to perform critical operations. The examples included "loss of city ledger file, loss of daily guest records, destruction of the advanced reservation files, as well as reliability of accounting and financial data" (Varga, 1975, p. 56). Criminal acts, malfunctions and natural disasters were cited as reasons for computer resource losses. Varga (1975) highlighted the necessity for hotel managers to be aware of the computer security problems and ways to protect the information. The first stage in the proposed security strategy, risk analysis, included the following measures: analysis of physical facilities of the environment where the technology operates; hardware security; software security; employees who have access to the systems; audit control. In the next stage it was recommended that cost trade-off analysis be performed. This included the comparison of the security measures implementation costs and potential outcomes and benefits. The final stage in this security strategy implementation included the development of programming, documentation, and utilization standards. The importance of the issues was highlighted by pointing out the trend of computers becoming a "part of

the business nerve center of hotel operation" (Varga, 1975, p.60) and consequently the necessity to protect them.

Security of the hotel information resources has become a point of interest for both researchers and industry professionals (Collins & Cobanoglu, 2008; LaBelle & Chatterjee, 2004; Ogle, Wagner, & Talbert, 2008). Cobanoglu and DeMicco (2007) studied the existing threats to hotels' computer network security and the security practices of hotels in the United States. The authors state the importance of the computer networks to support internal hotel operations such as front office functions, restaurant management, human resource management, payroll and accounting and external communication with corporate offices or chain hotels. These networks provide the hotels with Internet presence that help guests search for the information prior to their visit and to get connected to their relatives, friends, and offices when they are in-house. Taking into consideration the number of functions that networks enable, the case for the importance of maintaining network security was made. During the study, the following security attack types were reported by respondents: virus attacks, service denial, sabotage of data networks, system penetration by an outsider and spoofing. The top three security tools used by hotels were anti-virus software, physical security, and firewalls (software and hardware). All the hotels that got breached stated that they learned from their mistakes. However, 50% of hotels that experienced security attacks did not report it to any outside organization. The explanation given by these respondents included "negative publicity" and "competitors would use to their advantage" (Cobanoglu & DeMicco, 2007, p. 55). These findings are consistent with the findings of Canavan (2001) who

reported that most of the security problems stay inside the organization where they happen. Two reasons were given to explain this phenomenon: to protect public trust to the company and to prevent hackers from copying the attack scenario.

Different types of networks (wired and wireless) as well as networks components (hubs, switches and routers) were examined during a study of hotel network security in the U.S. (Ogle et al., 2008). The results showed that "hotels in the U.S. are generally ill-prepared to protect their guests from network security issues" (p. 10). The researchers proposed the use of encryption and detailed terms of service for the guests willing to connect to the Internet. These measures are supposed to minimize the risk of information security breach, data loss and as well as hotels liability in case if any of the above occurs.

Kasavana and Cahill (2007) stated that there is no absolutely secure system. An absolutely secure system would be one that is isolated from the entire world; however, this kind of system would be useless and unable to support any hotel operations. Hospitality information systems interact with each other, receive and transmit information, process the information and present output. The authors highlight that proprietary customer information and operational statistics that are stored and processed by hotel information systems are among the most important assets that a hospitality company can obtain. With regard to this, in the attempt to make the information systems as secure as possible it is important to find a balance between the operational performance and security precautions. Because of the significant number of network

security breaches in the last decade, Payment Card Industry Data Security Standards (PCI DSS) was created. The next section will explain the PCI DSS.

2.3 Payment Card Industry Data Security Standards (PCI DSS)

Payment Card Industry Data Security Standards (PCI DSS) is a set of rules that introduces compliance requirements for all companies that accept credit cards (Connolly & Haley, 2008). Today, to process credit card transactions a company must be in compliance with PCI standards. With the growing volume of payment card transactions, addressing security issues is gaining greater importance.

The process of establishing data security and PCI compliance involves credit card issuing companies, PCI Security Standards Council, banks, vendors and companies processing credit cards transactions (merchants) (Haley and Connolly, 2008). Figure 1 explains relationships and hierarchy between the elements in this chain.

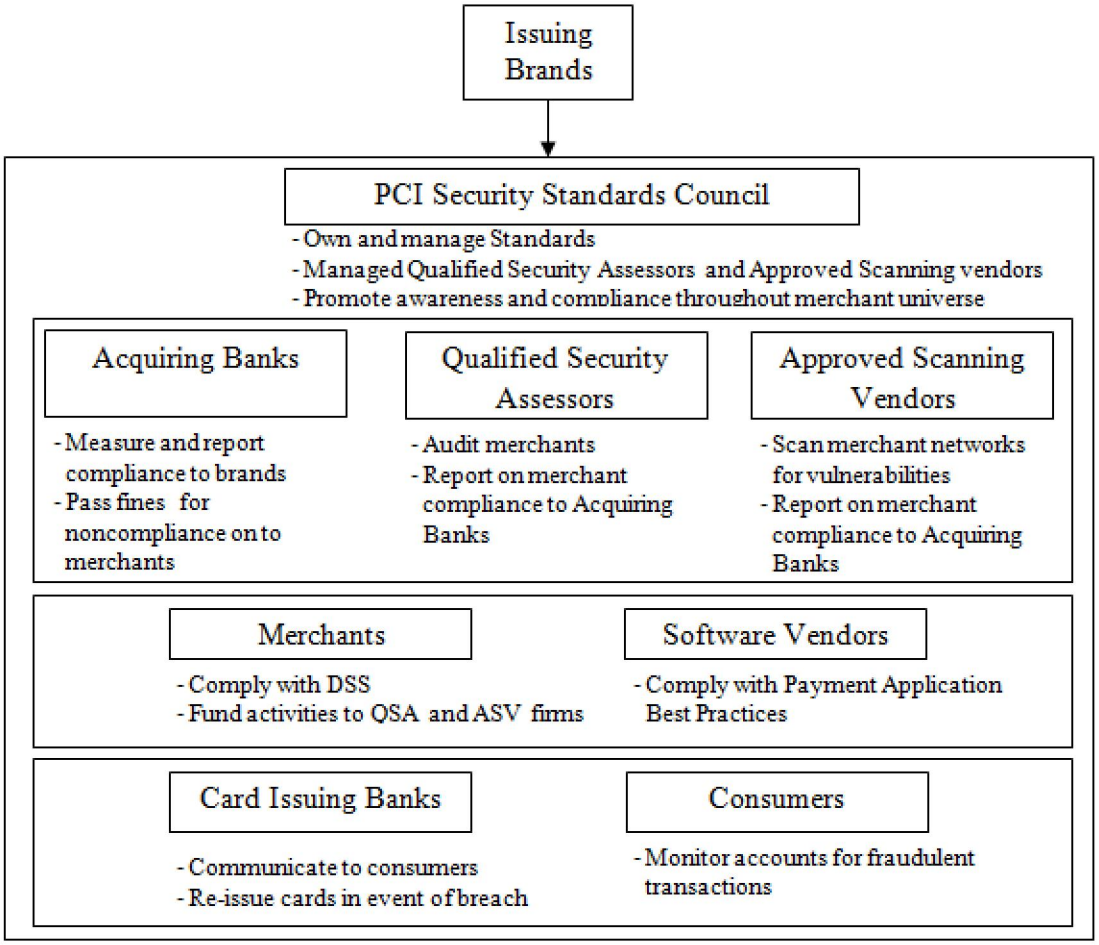

Figure 1. The Payment Card Industry (PCI) Value Chain
Resource: Haley & Connolly, 2008, p. 15

All the companies that accept credit card payments from their customers are divided into several groups (merchant levels) according to the number of credit card transactions per year. Merchant criteria and respective PCI validation requirements are shown in the Table 1 for Visa merchants. Each credit card company has their own categories, however, they seem to be similar to each other.

Table 1. Merchant levels and compliance validation requirements

Level/ Tier	Merchant Criteria	Validation Requirement
1	Merchants processing over 6 million Visa transaction annually (all channels) or Global merchants identified as Level 1 by any Visa region	- Annual Report on Compliance ("ROC") by Qualified Security Assessor ("QSA") - Quarterly network scan by Approved Scan Vendor ("ASV") - Attestation of Compliance Form
2	Merchants processing 1 million to 6 million Visa transactions annually (all channels)	- Annual Self-Assessment Questionnaire ("SAQ") - Quarterly network scan by ASV - Attestation of Compliance Form
3	Merchants processing 20,000 to 1 million Visa e-commerce transactions annually	- Annual SAQ - Quarterly network scan by ASV - Attestation of Compliance Form
4	Merchants processing less than 20,000 Visa e-commerce transactions annually and all other merchants processing up to 1 million Visa transactions annually	- Annual SAQ recommended - Quarterly network scan by ASV if applicable - Compliance validation requirements set by acquirer

Resource: Compliance validation details, 2009

The idea of security standards itself is not new: Hobson and Ko (1995) developed ten recommendations "to reduce hotels' chances of becoming a 'point of compromise' (p.53). Among these include:

1. Avoid collecting imprints of credit cards,
2. Protect guests' credit card information,
3. Tighten security regarding the storage and recording of hotel guests' credit card and other information,
4. Reduce hotel personnel's access to guests' payment card information,
5. Destroy documents containing credit card information (e.g. computer

printouts),

6. Restrict access to photocopying machines, especially during the night,
7. Install closed-circuit cameras in areas where guest information is kept,
8. Educate staff members,
9. Review security procedures,
10. Cooperate with credit card companies, police and agencies to prevent counterfeiting.

Later, credit card companies Visa, MasterCard, American Express, Discover, and the JCB put their efforts together to establish a unified system of requirements to protect cardholders' information (Haley & Connolly, 2008). The first set of requirements for PCI DSS 1.0 appeared in December, 2004. Two revisions have since followed: PCI DSS 1.1 was released in September 2006, PCI DSS 1.2 was released in October 2008 ("Version 1.2", 2008). All of these newer versions were designed to provide detailed information regarding safeguards and to enhance the understanding of PCI-compliance (Cobanoglu, 2008a). The requirements PCI DSS 1.2 are presented in the Table 2.

Table 2. PCI Data Security Standard Requirements

Goals	PCI DSS Requirements – Validated by Self or Outside Assessment
Build and maintain a secure network	1. Install and maintain a firewall configuration to protect cardholder data. 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect cardholder data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a vulnerability management program	5. Use and regularly update anti-virus software 6. Develop and maintain secure systems and applications
Implement strong access control measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly monitor and test networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an information security policy	12. Maintain a policy that addresses information security

Resource: Getting Started with PCI, 2008

These are PCI DSS major requirements. However, each of them is broken down into more specific sub-requirements totaling all together about 250 items. For example, for requirement 1, Install and maintain a firewall configuration to protect cardholder data, there are the following sub-requirements: establish firewall and router configuration standards, build a firewall configuration that restricts connections between untrusted networks and any system components in the cardholder data environment, prohibit direct system access between the Internet and any system component, install personal firewall software on any mobile and/or employee owned computers with direct connectivity to the Internet, which are used to access the organization's network.

To become PCI-compliant, a company is required to follow a particular procedure and meet the requirements indicated above ("Compliance validation details", 2009). Even though PCI-compliance is not mandated by a consistent set of laws in the entire United States, there are guidelines and key dates that need to be met by all firms involved in credit card transactions (Key Data, 2009). For example, the end of September 2009 was a deadline for full PCI-compliance validation for level 1 merchants, the end of the year 2009 was a deadline for level 2 merchants. Also by the end of September 2009 Visa required level 1 and 2 merchants not to retain sensitive card information (Lorden, 2009). However, PCI DSS requirements have already become law in some states. Minnesota became the first state to make core PCI requirements law in 2007 (Vijayan, 2007; Young, 2009). In 2010 the state of Massachusetts passed the law (201 CMR 17.00) about the standards of protecting personal information and all qualifying objects were required to become compliant with this law on or before March 1, 2010. The law describes duty to protect and standards for protecting personal information and also specifies computer system security requirements. The requirements for computer system protection reflect the requirements stated in first nine PCI standards. They include: develop secure IDs and passwords, restrict access to records containing personal information, encrypt all transmitted files containing personal information, ensure up-to-date antivirus, firewall and malware protection, etc.

PCI DSS and the hospitality industry

PCI compliance has become an important part of the hospitality industry operations (Cobanoglu, 2007; Tenczar, 2008; Volpe, 2009; Levin & Hudak, 2009). The fact that about 55% of the credit card breaches happen in the hospitality industry makes PCI DSS more important for hospitality industry (Cougias as cited in Haley & Connolly, 2008). According to Haley and Connolly (2008), there are some unique points that should be considered carefully for PCI compliance in the hospitality industry. Some are discussed below:

1. High speed Internet access (HSIA)

This service is widely provided to hotels' guests and can cause vulnerability to guests' information and hotel networks. Poorly implemented HSIA that is connected to a property management system (PMS) can expose the entire system and cardholder information to hackers.

2. Numerous systems employed in hotels

Hotels implement numerous "inside" and "outside" systems that are necessary for efficient operations (Haley and Connolly, 2008, p. 23). These systems may include, but are not limited to PMS, point of sale systems (POS), sales and catering, golf, spa, electronic locking systems, accounting, central reservation systems (CRS), and website booking engine. Figure 2 demonstrates the systems architecture of a typical hotel.

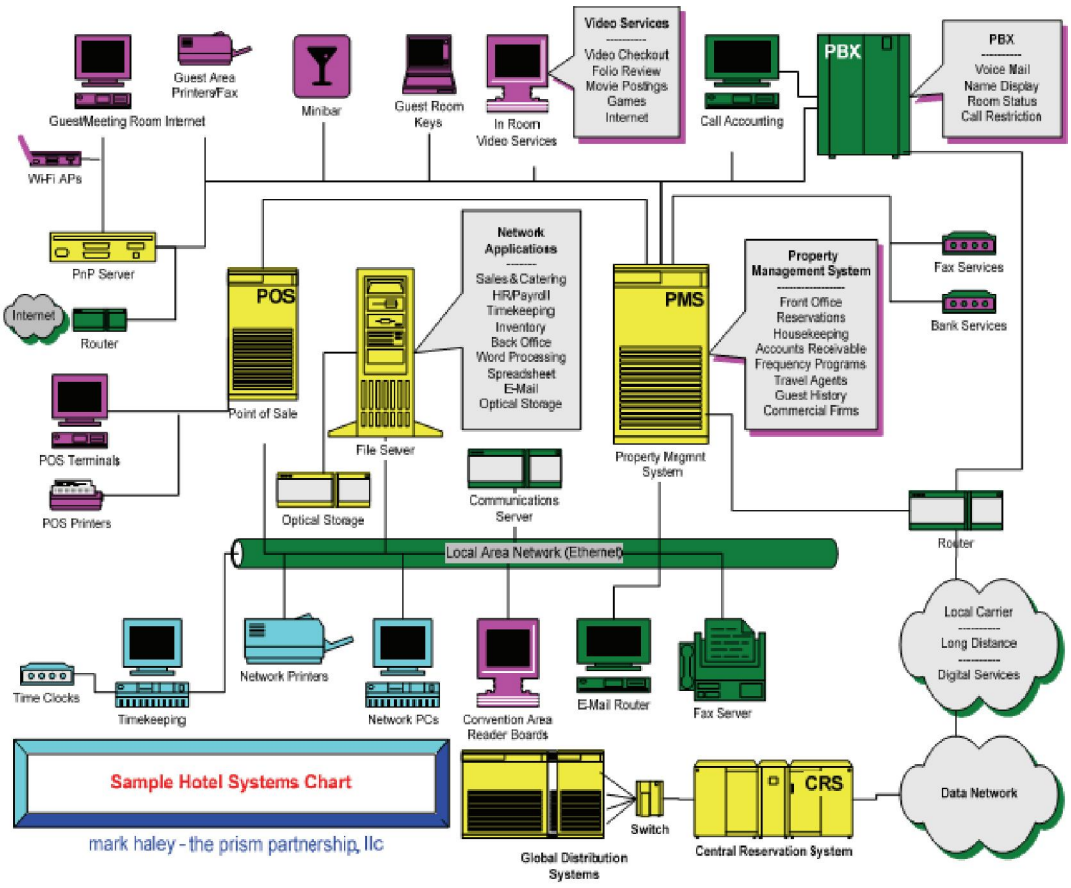

Figure 2. The systems architecture of a typical hotel
Resource: Haley and Connolly, 2008, p. 23

On average, the number of different systems deployed in a full service hotel may be as many as 60, and this number may be as high as 35 in a limited service hotel (Collins & Cobanoglu, 2008).

Due to the complexity of all the systems implemented in hotels, it is important to know which systems collect payment card information in order to protect and secure guest credit card information. Those systems that deal with credit card information form the scope for PCI DSS compliance. In addition, hoteliers should know

the data flow, which is defined as the path of payment information from merchant to the acquirer. Hoteliers should also check with vendors if the applications they provide are PCI Council certified and PCI-compliant. Hotels can reduce vulnerability and become less attractive to hackers if they follow PCI DSS requirements (Haley and Connolly, 2008).

3. Receiving cardholder data from external systems

Hotels often receive reservations from external systems such as global distribution systems (GDS), which is a collective inventory system for hotel, car, and airline reservations (Collins & Cobanoglu, 2008). This refers to the booking process when the reservation along with guest payment information comes from GDS through central reservation system (CRS) to a hotel. Hoteliers are responsible for protecting guest payment information as soon as it hits the hotel's network systems.

4. Culture of shared log-ins and easy vendor access

This problem includes setting up common log-ins and giving remote access to vendors. Cobanoglu & DeMicco (2007) suggested that there is a significant percentage of hotels that use common log-ins where more than one person can access hotel's system by using the same sets of username and password. Under PCI DSS, each system user must have a unique username and password.

There are several reasons pointed out in the literature to be PCI compliant, among them are reputation, financial cost, legal costs (Haley and Connolly, 2008) and guest distrust (Cobanoglu, 2008a). Protecting guest data is of extreme importance to hotels (Cobanoglu, 2008a) especially given the fact that more than half of the hotels are

not PCI compliant (Cobanoglu, 2008b). All these provide strong reasons for hospitality companies to comply and monitor the latest changes of PCI DSS requirements and to invest in compliance. The next section looks at the cost of computer security breaches in more detail.

2.4 Cost of Computer Security Breaches

The hospitality industry provides "rich targets" (Levin & Hudak, 2009) for identity thieves. A lot of information security breaches have occurred in the hospitality industry, examples include:

- Atlantis Resort, January 2006, a database with customer information including payment card, bank account, and social security data was compromised, approximately 55,000 customers affected (Haley & Connolly, 2008).

- University Place Conference Center and Hotel in Indianapolis, Indiana, January 2006, a security breach involving 7,600 guest names, addresses and credit card numbers ("Credit check", 2007),

- Hotels.com, June 2006, 243,000 customers' personal information may have been compromised when a laptop was stolen from an auditing company ("Credit check", 2007),

- Seven hotels in southwest Chicago, November 2006, guest credit card numbers were sold months after guests had checked out of the hotels ("Credit check", 2007),

- Okemo Mountain Resort, March 2008, credit and debit card information of approximately 46,000 of customers affected, (Haley & Connolly, 2008),
- Wyndham Hotels and Resorts, December 2008, as many as 41 hotels and 21,000 guests could be affected, guest names, credit card numbers and their expiration dates, as well as data from the cards' magnetic stripe were accessed by hackers (McMillan, 2009),
- Radisson Hotels & Resorts, November 2008 – May 2009, computer systems of chain hotel in the United States and Canada were breached; information such as the name printed on a guest's card, card number, and card expiration date was compromised (Radisson Hotels & Resorts, 2009).

Cost of PCI compliance

According to the Gartner Group's research conducted in 2008, PCI DSS 1.1 compliance requires investment of about $2.7 million dollars in remediation costs and another direct cost of $237,000 for outside assessors and related expenses for Level 1 merchant (Crawford, 2009). For Level 2 merchants, the investment was $1.1 million for remediation and $135,000 for assessment expenses. Table 3 provides approximate investments necessary for merchants of different levels to become PCI compliant.

Table 3. Approximate investments in PCI compliance

	Level 1	Level 2	Level 3
Assessment	$237,000	$135,000	$30,000
Remediation	$2,700,000	$1,100,000	$155,000
Total	$2,937,000	$1,235,000	$185,000

Resource: Crawford, 2009

Even though every merchant who accepts credit cards must be compliant with PCI DSS (Haley & Connolly, 2008), not all the companies meet these requirements (please see Table 4).

Table 4. U.S. PCI DSS Compliance Status as of 12/31/2009

CISP Category (Visa transactions per year)	Estimated Population Size	Estimated % of Visa Transactions	PCI DSS Compliance Validated	Validated Not Storing Prohibited Data
Level 1 Merchant (>6M)	360	50%	96%	100%
Level 2 Merchant (1 - 6M)	895	13%	94%	100%
Level 3 Merchant (e-commerce only 20,000 – 1M)	2,524	<5%	Moderate	N/A
Level 4 Merchant (<1M)	~5,000,000	32%	Moderate	TBD

Resource: Visa Inc., 2009

A comparison of the data reported at the end of 2009 and 2008 shows a growth of PCI DSS validated compliance from 91% to 96% for Level 1 merchants and

from 87% to 94% for Level 2 merchants. Moderate level of compliance for Level 3 and 4 merchants does not correspond to any particular figure; however, the data reported at the end of 2008 show that, for example, only 57% of the Level 3 merchants were PCI compliant.

Non-compliance with PCI DSS will pose other costs for companies (Halsey, 2009). According to the Identity Theft Resource Center, the number of data breaches actually rose nearly 50% in 2008, compromising the personal records of at least 35.7 million Americans. More than 55% of credit card fraud comes from the hospitality industry (Cougias as cited in Haley & Connolly, 2008). These statistics demonstrate high vulnerability of the hospitality industry and the necessity for careful attention to PCI standards. Failure to meet these requirements will cost between $90 and $300 per record breached, on average (Crawford, 2009). If a breach occurs a company will be responsible for:

- $3 to $10 per card for replacement costs,
- $5,000 to $50,000 (or more) in compliance fines,
- Additional fines based on the actual fraudulent use of the cards, which will vary depending on the number of cards exposed (Halsey, 2009).

Credit cards' issuing companies will apply fines to merchants that fail to comply with PCI DSS (Haley & Connolly, 2008). Visa's fine structure ranges from $5,000 to $25,000 per month. American Express' fine structure starts at $50,000 and goes up. So, cumulative cost for being non-compliant can be really high.

As a potential way of preventing data security problems American Hotel and Lodging Association (AH&LA) suggests establishing a culture of guest information privacy and information security throughout the organization; establishing and maintaining sound documentation and policies; eliminating as much payment card data as possible from paper records and computer systems and utilizing existing resources that may be available at little or no incremental cost, including: payment card acquiring bank; franchisor, management company, or parent company, if any; software vendors; free or low-cost resources found on-line; the American Hotel & Lodging Association or its partner state association in every particular state.

Information technology has emerged as an important component of hotel management (Collins & Cobanoglu, 2008). In addition, technology is one of the major sources of information for guests to find, select and book hotels (Berezina & Cobanoglu, 2009). Also, technology is one of the most important factors in guest satisfaction (Cobanoglu, 2001; Berezina & Cobanoglu, 2009). Given the fact that hotel properties have a responsibility of protecting their guests, “one should view information security as an invaluable and expected guest service” (Connolly & Haley, 2008). Even though this service is not primary to hotels, it is expected that the information collected from travelers will be properly handled and secured. For these reasons, it is important to understand the role of hotel information security in overall service quality. The next section will discuss service quality in a hotel.

2.5 Service Quality

Service quality can be defined as a level of service delivery based on customer perception (Zeithaml et al., 2006). Service quality has an important place in services marketing research (Buttle, 1996; Cronin Jr. & Taylor, 1992; Parasuraman, Zeithaml, & Berry, 1985; Qu & Sit, 2007; Yee et al., 2009). Research in the service quality area started to grow in 1970s (Akbaba, 2006). The major reason for this was the increasing role of the service sector in the overall economy. In the first decade of the 21st century services accounted for about 80% of gross domestic product (GDP) in the United States (Central Intelligence Agency, 2010; Zeithaml et al., 2006). This provided the motivation to study and understand service quality. However, in comparison with goods quality, service quality is difficult to measure objectively (Akbaba, 2006). This difficulty is explained by the main characteristics and nature of services. Specific characteristics of services compared to goods include: intangibility, heterogeneity, simultaneous production and consumption, perishability (Kotler et al., 2003; Reid & Bojanic, 2009; Zeithaml et al., 2006). These features explain variability in service delivery that causes difficulty in maintaining high service quality. Hospitality industry, being a part of services segment, faces the same challenge (Reid & Bojanic, 2009).

In an effort to measure service quality, a special instrument called SERVQUAL was introduced in 1985 (Parasuraman et al., 1985). SERVQUAL scale is based on the comparison of customer expectations of the service and their perceptions of the performance of the service. Originally, the scale included ten dimensions, which are as follows: reliability; responsibility; competence; access; courtesy; communication;

credibility; security; understanding/knowing; and tangibles. In the subsequent work by the same authors, these overlapping dimensions were condensed from ten to five: tangibles; reliability; responsiveness; assurance; and empathy (Zeithaml, Berry, & Parasuraman, 1988). In the new model communication, credibility, security, competence, and courtesy fell into the assurance category (Saleh & Ryan, 1991). The description of the SERVQUAL dimensions is presented in the Table 5.

Table 5. SERVQUAL dimensions

Dimension	Description
Reliability	Ability to perform the promised service dependable and accurately
Responsiveness	Willingness to help customers and provide prompt service
Assurance	Employees' knowledge and courtesy and their ability to inspire trust and confidence
Empathy	Caring, individualized attention given to customers
Tangibles	Appearance of physical facilities

Resource: Zeithaml et al., 2006

SERVQUAL has been used to measure service quality in different service areas, including car industry (Bouman & Van der Wiele, 1992), hospitality and tourism industry (Ekinci, Prokopaki, & Cobanoglu, 2003; Saleh & Ryan, 1991; Qu & Sit, 2007; Yee et al., 2009); and information systems (Jiang, Klein, & Crampton, 2000). In support for the tenets of the service quality measurement instrument, several authors have

developed an analogous measurement scale for information technology services quality (Jiang et al., 2000). The purpose of the development of SERVQUAL for IT services is to assist managers and researchers in the evaluation of service quality.

However, the use of SERVQUAL has also been criticized in the literature (Jain & Gupta, 2004). This criticism has included the length of the instrument and the respondents becoming unfocused because of the double scale. As an alternative to SERVQUAL the model of service performance (SERVPERF) was introduced (Cronin Jr. & Taylor, 1992). This scale uses the same statements developed for SERVQUAL and is loaded to the five dimensions, but only for perceived service, without regard to customer expectations. In comparison to SERVQUAL, SERVPERF does not assess the gaps in scores because the expectations part is omitted from the model. The main justification for the SERVPERF implementation is that customers automatically take their expectations as reference point in their minds when asked to evaluate service quality and perform the rating based on this (Carrillat, Jaramillo, & Mulki, 2007). Consequently, there is no need to ask for expectations separately. There is evidence that the scale has received wide support in measuring service quality in many fields (Jain & Gupta, 2004; and Qu & Sit, 2007). Researchers have highlighted that using the single scale of SERVPERF provides higher efficiency and explains greater variance in the overall service quality. (Boulding et al., 1993) found that service quality is directly influenced by consumers' perceptions and therefore provides support for the usage of the SERVPERF scale.

To address the questions raised about the validity of SERVQUAL and SERVPERF instruments, Carrillat, Jaramillo and Mulki (2007) performed a meta-

analysis of 17 different studies investigating the relationship between SERVQUAL and SERVPERF. The results of the analysis revealed that both instruments are equally valid predictors of overall service quality. At the same time, researchers found that the predictive validity of the SERVQUAL is improved if the instrument is adjusted to a specific field where it is used. However, the predictive validity of SERVPERF is not improved by context adjustments.

The importance of measuring and understanding service quality is important because it is seen as a prerequisite for success in a competitive business environment (Akbaba, 2006). Literature also highlights its role in customer satisfaction and behavioral intentions (Reid & Bojanic, 2009; Zeithaml et al., 2006). These notions will be explained in the next section.

2.6 Consumer Satisfaction & Behavioral Intentions

Perceived service quality is seen as a prerequisite and a part of broader concept of customer satisfaction (Zeithaml et al., 2006). Satisfaction refers to as a post-purchase evaluation of product quality given pre-purchase expectations (Kotler et al., 2003). The interrelation of service quality, customer satisfaction, and customer loyalty is shown on the Figure 3.

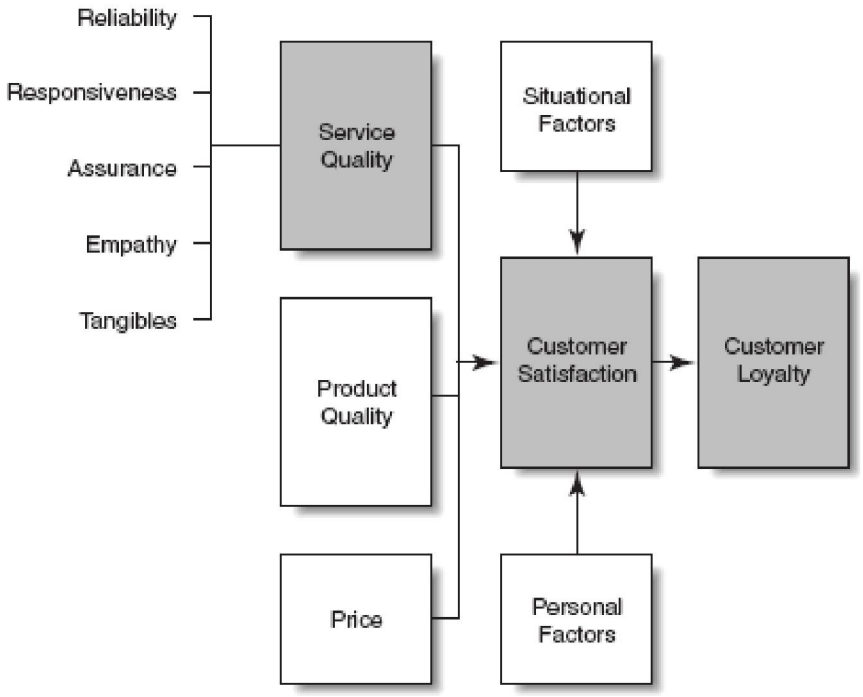

Figure 3. Customer perception of quality and customer satisfaction
Resource: Zeithaml et al., 2006, p. 107

As was shown above in Figure 3, service quality is part of a larger concept of customer satisfaction and loyalty (Zeithaml et al., 2006). Different studies have investigated the relationship between service quality, satisfaction, and customer loyalty (Skogland & Siguaw, 2004; Yee et al., 2009). There is a debate in the literature about the relationships between service quality, satisfaction and loyalty (Zabkar, Brencic, & Dmitrovic, 2009). Even when high service quality is provided and a customer is satisfied, it does not necessarily mean that this customer will come back (Kotler et al., 2003; Reid & Bojanic, 2009; Zeithaml et al., 2006). There can be different reasons why a customer would not come back to a property where he or she received high quality service and was

satisfied. One reason could be that a customer does not want to travel to the same area, but prefers to explore something new; a second could be explained by the willingness to try something new even if the customer returns to the area (he or she can intentionally look for a different hotel); and finally, a customer can be influenced by a better deal offered in another hotel. On the other hand, some research studies suggest that service quality leads to customer satisfaction, attraction of new customers, positive word-of-mouth, repeat visits, enhanced corporate image, increased business performance and so forth (Akbaba, 2006; Reid & Bojanic, 2009; Zabkar et al., 2009; Zeithaml et al., 2006).

Yee et al. (2009) found that service quality has a significant and direct impact on customer satisfaction and that the relationship between customer satisfaction and loyalty is also highly significant. These findings are in line with the results of Skogland & Siguaw (2004) who reported that satisfied stayers (satisfied returning customers) have the greatest loyalty.

The results of the study conducted by Boulding et al. (1993) showed that the higher customers' perceptions of service quality, “the more likely the customers are to engage in behaviors beneficial to the strategic health of the firm (e.g., generate positive word of mouth, recommend the service, etc.)” (p. 24). Based on these findings this study will investigate the impact of information security breach on service quality in connection with satisfaction, word-of-mouth and revisit intentions.

2.7 Rationale for the Study

Network security breaches in hotels result in both financial and non-financial costs as explained above. Tangible and direct costs of security breaches are easy to distinguish. There have been several attempts by researchers to identify these costs. Campbell, Gordon, Loeb, & Zhou (2003) investigated the economic cost of the public announcement of security breaches and found only limited impact on the overall market reaction. However, upon further analysis, they found a more significant negative reaction for security breaches involving confidential data than when the breaches involved non-confidential data. Garg, Curtis, & Halper (2003) studied the financial impact of the information security breach and approximated between 0.5 – 1 % of annual sales loss as a result of negative reaction of the security breach in the value of stocks. However, intangible costs of network security breaches have not been well reported in the literature.

Once there is a security breach in a hotel, it is required by the PCI Council and law that the hotel reports the incident to authorities, which will result in the incident being covered in the media. The impact of these announcements on customers' perception of service quality, satisfaction, word of mouth and revisit intentions is not clear. This study will attempt to examine the impact of network security breaches on hotel guests' satisfaction, revisit intentions, and word-of-mouth recommendations.

The theoretical framework suggests that service quality is a direct predictor of guest satisfaction, which is a direct relationship to guest revisit intentions. For this reason, this study will employ the SERVPERF instrument (that reflects perceived service quality) to measure the perceived service quality of hotel guests before and after

receiving news of a security breach. The variables involved in the study are presented in the following model (Figure 4).

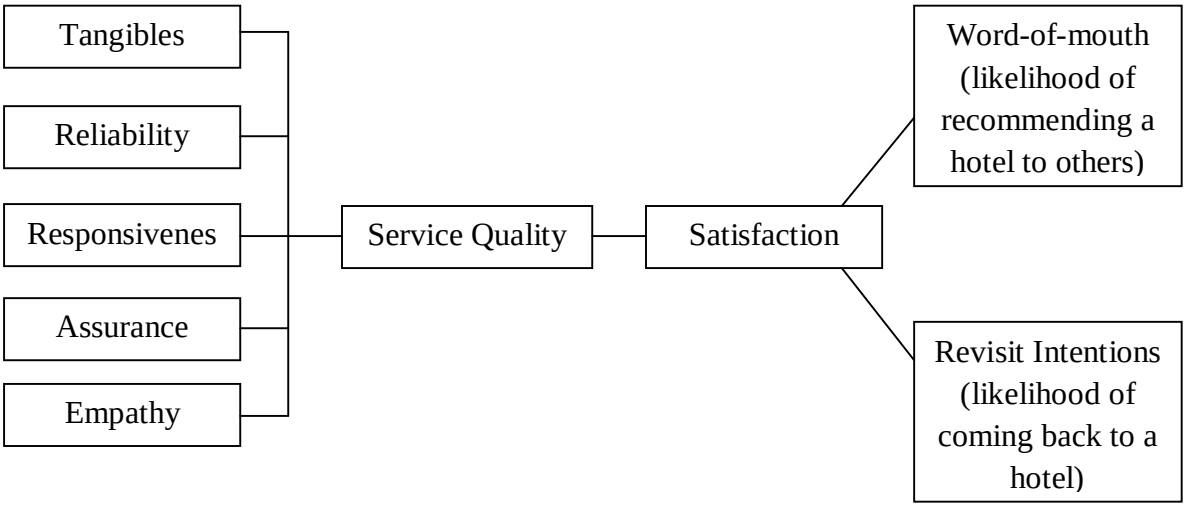

Figure 4. Variables included in the study

These variables underlie the four research questions stated for the study. The next chapter addresses the research design and methodology that have been chosen to answer the research questions in this study.

Chapter 3

METHODOLOGY

3.1 Research Design

A pre-test / post-test experimental research design with the treatment given in the form of scenarios was chosen for the study. Experimental research design is utilized to inform about cause and effect relationship. It involves "the manipulation of one or more independent variables by the investigator and random assignment of subjects to experimental groups or treatments" ("Design and Analysis of Experimental and Quasi-Experimental Investigations," 2003). The specific features of experimental research design that follow from the definition are: random assignment of subjects to groups and active independent variable (Gliner, Morgan, & Leech, 2009). Random assignment of subjects to groups means that each participant is supposed to have equal chances to be in any of the groups (this criterion distinguishes experimental design from quasi-experimental). Active independent variable represents an intervention at least one level of which is given to participants within a specific period during the study. A new curriculum, workshop, training or other kind of treatment usually represent an active variable. Very importantly this treatment should be given to participants as a part of the study, and not as part of a previous experience at some point of time in their lives.

There are two basic designs for control experiments: minimum and maximum diversity designs (Gomm, 2009). The first one investigates effects of different conditions on similar subject, while the second one looks at impacts of similar conditions on different subjects. As was mentioned earlier, this study investigates if failure to protect hotel guests' information (as a part of hotel's service) will result in guest dissatisfaction and have an impact on guest behavioral intentions. There can be at least two outcomes of information security breach for hotel guests: when a breach occurs, information of a guest can be compromised or can stay safe. These two outcomes will serve as two first active variables (or treatments) for the study. And on the other hand, the study aims to know if information about security best practices will increase guest satisfaction and shift behavioral intentions. This will form the third active variable or treatment. Due to the fact that the research investigates an impact of different treatments on the similar subjects (hotel guests), minimum diversity experimental research design was chosen for the study. There are particular steps that are necessary to follow to conduct a study in accordance with this design. The flow of minimum diversity experimental research design is shown in Figure 5.

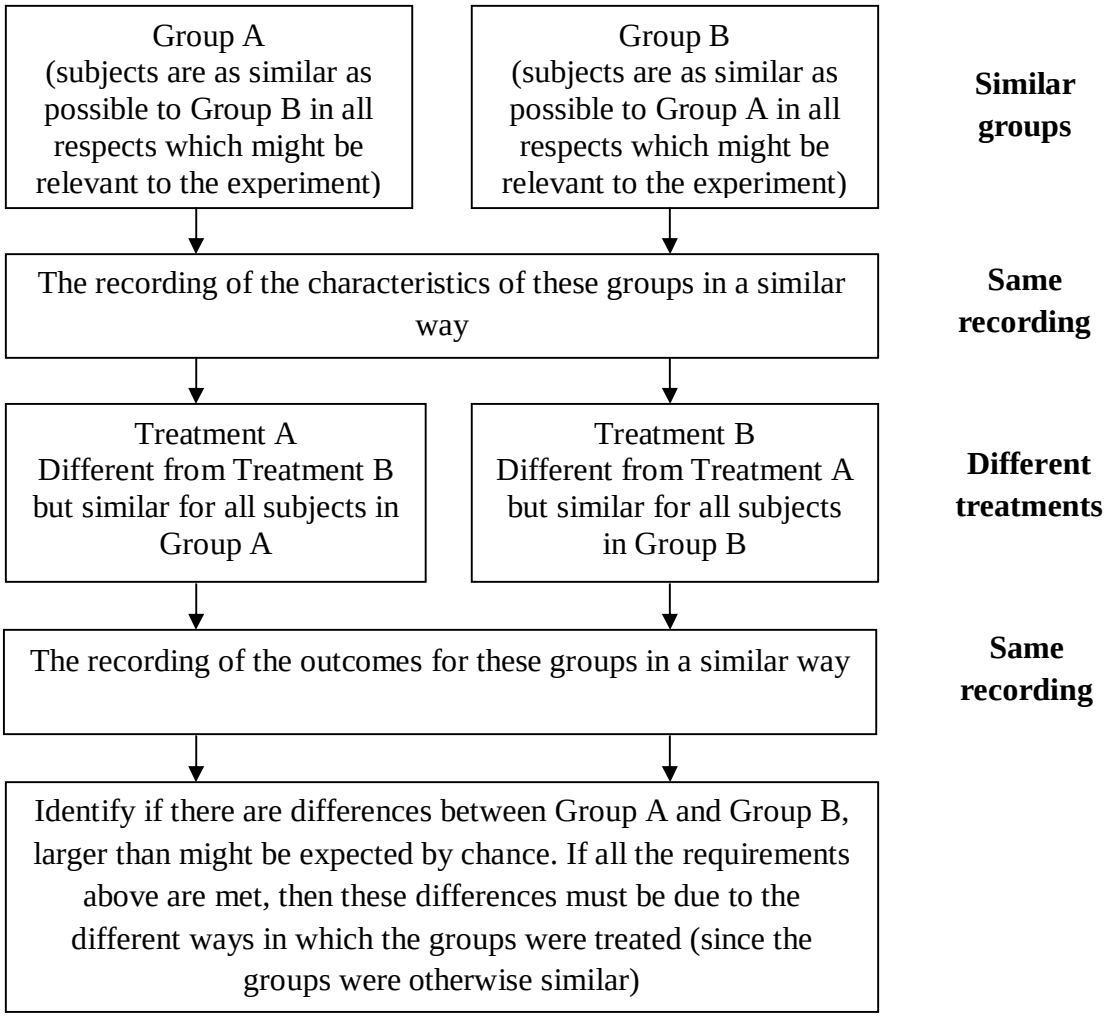

Figure 5. The flow of minimum diversity experimental research design
Resource: Gomm, 2009, p. 125

In order to conduct the study based on this design, three different treatments reflecting different scenarios about information security in hotels were developed. These scenarios are presented below.

Scenario 1 is a negative scenario that introduces respondents to a situation where their credit card information was stolen during a security breach in the hotel they

stayed last. The text of the scenario in the form it was presented to respondents is shown below:

Please, imagine that you have received an email from the hotel where you recently stayed. Please, read the message carefully and then answer the following questions.

"Dear Guest,

Hotel X values your business and respects the privacy of your information, which is why we wish to inform you that there was a computer security breach last week in our hotel and we have found out that the credit card you used when you checked out is one of the credit cards from which information was stolen during the breach. We would like to let you know that we are doing our best to solve this problem. You will receive a new card from your credit card company. Additionally, you will receive a credit history protection plan. All the expenses will be paid by us. We are very sorry for the inconvenience.

For further assistance regarding this incident please visit our website www.HotelX.com or call 1-800-555-5555.

We appreciate your business and understanding.

Sincerely,

John Doe,

Chief Executive Officer,

Hotel X"

Scenario 2 is neutral in its nature and introduces study participants to a situation where a security breach happened in a hotel they stayed last, but their information was not compromised. The text of the scenario in the form it was presented to respondents is shown below:

Please, imagine that you have received an email from the hotel where you recently stayed. Please, read the message carefully and then answer the following questions.

"Dear Guest,

Hotel X values your business and respects the privacy of your information, which is why we wish to inform you that there was a computer security breach last week in our hotel and we have found out that the credit card you used when you checked out is ***NOT*** one of the credit cards from which information was stolen during the breach. We would like to let you know that we are doing our best to solve this problem. Again, thank you for being a guest of our hotel.

If you have any questions regarding this incident please visit our website www.HotelX.xom or call 1-800-555-5555.

As always we appreciate your business.

Sincerely,

John Doe,

Chief Executive Officer,

Hotel X"

Scenario 3 was developed as a positive one. It says that a hotel where a respondent stayed last passed a comprehensive security audit that ensures that guest information is safe and well protected. The text of the treatment in the form it was presented to respondents is shown below:

Please, imagine yourself seeing the following article in the morning newspaper after your last hotel stay. Please, read the passage carefully and then answer the following questions.

"Hotel X, one of the leaders in the international lodging market, has passed comprehensive security assurance evaluation audit. The certification ensures that the private information guests share with the Hotel, such as their personal and credit card information, is in good hands. "We are committed to doing all we can to ensure our guests' security and privacy and to protect them from fraud", says CIO of the Hotel John Doe, "we engaged in a sophisticated technology assessment process, successfully passed it and now we are happy to share this news with our guests".

These treatments developed for the study were incorporated into the questionnaire and presented to respondents randomly. It means that respondents were not assigned to any of the treatment prior the study, but had equal chances of receiving any of the treatments. These scenarios along with the review of relevant literature, theoretical framework and research questions helped to formulate the research hypotheses. All hypotheses developed for the study are presented and explained in the next section.

3.2 Hypotheses Statement

Total of 12 hypotheses, four for each of the treatment, were stated for the study. Hypotheses were designed to test the same variables influenced by different treatments. Those variables were identified in research questions. They include: hotel guest perceived service quality, satisfaction, word-of-mouth and likelihood of coming back to a hotel. Every hypothesis was numbered in the following format: H (states for hypothesis), followed by numbers 1, 2 or 3 (corresponds to the treatment number to which this hypothesis refers) and letters a, b, c or d (represents the variable the hypothesis is testing). For example, this means that, H1a and H1b tests different variables (a and b) influenced by treatment 1, and H1a and H2a test the same variable (variable a) influenced by different treatments (treatment 1 and 2). The logic of hypotheses statement is presented in Figure 6 using the research model and treatments introduced earlier.

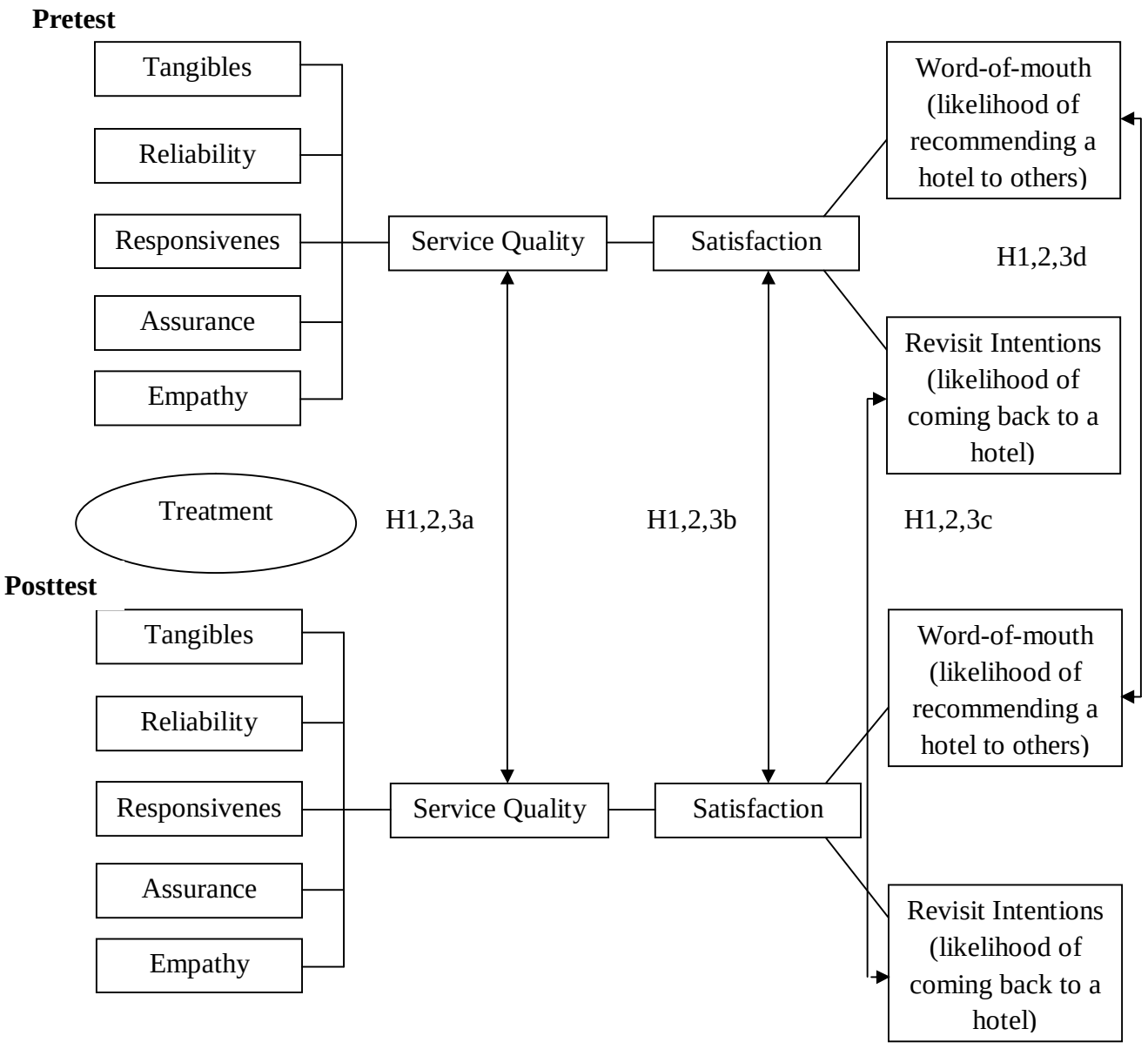

Figure 6. Model for hypotheses statement

Hypotheses for Treatment 1.

H1a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the information security breach - stolen scenario (treatment 1) and after it.

H1b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the information security breach - stolen scenario (treatment 1) and after it.

H1c: There is a significant difference between the customers' revisit intentions to the brand before reading the information security breach - stolen scenario (treatment 1) and after it.

H1d: There is a significant difference between the customers' likelihood of recommending the brand before reading the information security breach - stolen scenario (treatment 1) and after it.

As it was explained in the previous section, treatment 1 is a negative scenario where a security breach happened and guest information was stolen. Viewing the guest information protection as a part of hotel service, failure to perform this service is expected to decrease the perception of service quality by hotel guests. Since the literature describes service quality as a prerequisite for guest satisfaction (Reid & Bojanic, 2009; Zeithaml et al., 2006), the researcher hypothesizes that guests' perception of service quality and satisfaction will be negatively affected by treatment 1. The same is expected for likelihood of recommending a hotel (word-of-mouth) and coming back to a property (revisit intentions), because these both concepts are connected to satisfaction in the

literature. As literature suggests that there are interrelations between all variables included in this study, the researchers expect overall negative impact of treatment 1 (security breach – stolen scenario) on guests' perception of service quality, satisfaction, revisit intentions and word-of-mouth.

Hypotheses for Treatment 2.

H2a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the information security breach – not stolen scenario (treatment 2) and after it.

H2b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the information security breach – not stolen scenario (treatment 2) and after it.

H2c: There is a significant difference between the customers' revisit intentions to the brand before reading the information security breach – not stolen scenario (treatment 2) and after it.

H2d: There is a significant difference between the customers' likelihood of recommending the brand before reading the information security breach – not stolen scenario (treatment 2) and after it.

Scenario 2 was introduced as a neutral treatment in this study. The situation where a security breach happened but did not affect a guest can be seen by respondents differently. One point of view can be negative (similar to treatment 1) when a respondent can assume that if a breach happened it means that a hotel does not do its best to protect

guest information; and even if, in this case, this particular guest was not affected he or she can assume that a similar situation may happen again because the hotel's security practices are not good. Guests also might think that if a hotel does not totally control information flow and network activities, their information can be misused without the hotel knowing about it. Based on this, the researcher assumed that treatment 2 will impact the variables negatively just as treatment 1 does. However, some of the respondents may view treatment 2 positively. After a breach occurs and some other guest information is compromised, a hotel can become more careful and strict about information security. From this perspective a guest can assume that after this event a hotel can bring their service to a higher level and improve information security. Consequently, next time when this guest travels he or she can prefer a hotel that experienced a breach before assuming that after this experience the hotel learned how to protect guest information and establish high security standards. Even though the researcher hypothesizes that negative element is stronger in this scenario, the results of the hypothesis testing will show hotel guests' attitudes towards it.

Hypotheses for Treatment 3.

H3a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the positive information security scenario (treatment 3) and after it.

H3b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the positive information security scenario (treatment 3) and after it.

H3c: There is a significant difference between the customers' revisit intentions to the brand before reading the positive information security scenario (treatment 3) and after it.

H3d: There is a significant difference between the customers' likelihood of recommending the brand before reading the positive information security scenario (treatment 3) and after it.

Treatment 3 in this study refers to a positive treatment which tells respondents about high information security in a hotel where they last stayed. Keeping in mind the interrelations between service quality, satisfaction, revisit intentions and word-of-mouth, one can assume that high level of service quality will positively impact satisfaction, revisit intentions and word-of-mouth. The logic behind this is that respondents can see a competitive advantage for this hotel in enhanced information security. It might be a sign for guests that this hotel does care about its guests and that it will secure guest information properly. This can be seen as a strong reason for revisit intentions and recommending a hotel to relatives and friends. However, it is also important to note, that information security is not a primary service in the lodging industry and most probably is not a key element in hotel selection process for hotel guests. Based on this the researcher would hypothesizes that positive scenario will have either positive or no effect on the variables.

In order to test the hypotheses and answer the research questions, a data collection instrument was developed. The questionnaire used for the study is described in the next section.

3.3 Questionnaire

An on-line research survey was chosen as a main data collection method because of its main advantages: it allows access to demographically and culturally diverse population, enables access to large samples at relatively low cost (Johnson & Christensen, 2008; Reynolds, Woods, & Baker, 2007).

In order to learn more about the impact of information security breaches in hotels and to verify the survey instrument, a focus group interview was conducted. The focus group consisted of American Hotel and Lodging Association (AH&LA) Technology and E-Business Committee, which comprised of ten hotel chief technology executives, two hospitality technology consultants, three hospitality technology academics, five technology vendors, three AHLA executives, and the President of AHLA. Based on the feedback of the focus group members, the survey instrument was revised.

The final questionnaire was developed based on the results of the review of literature and the focus group. The survey targeted the assessment of the service quality of the respondents' last hotel stay within the preceding 12 months using the SERVPERF scale (Cronin Jr & Taylor, 1994). Based on the findings in the literature that SERVQUAL and SERVPERF are equally valid predictors of overall service quality (Carrillat et al.,

2007), SERVPERF scale was chosen because it allows to keep the instrument shorter. If the respondents had not stayed in a hotel within the last 12 months, they were terminated from the survey. The first part of the questionnaire addressed the travel behavior of respondents, including hotel type, purpose of the last hotel stay, method of payment and self-reported method of technology adoption. The second part of the survey asked respondents to rate each of the questions in SERVPERF instrument using 7-point Likert scale (where 1 = Strongly Disagree to 7 = Strongly Agree) regarding their last hotel stay. This group of questions were followed by satisfaction and revisit intentions questions, again all based on their last hotel stay (Zeithaml et al., 2006). Following the logic of the experimental design flow, these two parts allowed to record similar information about different groups. In the third part of the questionnaire all respondents were randomly assigned to read one of three scenarios (treatments). In the fourth part of the questionnaire respondents were asked to answer the same set of service quality, satisfaction, revisit intentions and word-of-mouth questions as in the second part. This allowed the researcher to record the outcome of the treatment for different groups. The fifth and final part of the survey contained demographic type questions.

A questionnaire with a cover letter explaining the purpose of the study was emailed to the sample population of randomly chosen people. Additionally, this letter provided information about the researchers, approximate time to complete a survey and contact phone of the University's Human Subject Review Board (in case of any questions about the study). Participants' responses were kept completely confidential and participation was voluntary. As an incentive to complete the questionnaire, all

respondents were informed about a drawing for an Apple iTouch 32Gb for those who complete the survey fully. The research was started with the pilot study that is described in the following section.

3.4 Pilot Study

A pilot study with a convenience sample of college students was conducted to assess the reliability of the questionnaire developed. During the pilot stage of the data collection 92 responses were received. Among them 70 qualified for the study based on the completion and qualifying questions. These responses were used to check the reliability of the developed instrument. The analysis revealed percentages between 87.8 and 91.6% (Table 6) that demonstrates high reliability.

Table 6. Reliability analysis for pilot study

Service Performance Dimension	Cronbach's Alpha
Tangibles	0.902
Reliability	0.898
Responsiveness	0.878
Assurance	0.916
Empathy	0.902

On the first stage of the data analysis the responses received on the pilot study were compared to the ones received in the main study. Independent sample t-test

that was used to compare the mean scores of the answers provided by the respondents in the pilot and the main study for the service quality questions showed significant difference on only one item out of 22 – "The hotel insisted on error-free records". Based on that, we concluded that the sample will not suffer from the bias if we include pilot stage responses in the study.

3.5 Response Rate & Non-Response Bias Analysis

During the months of January-March, 2010, 20,000 questionnaires were sent electronically to random group of US residents who have an email address through rent-a-list.com's database. In total, 2518 persons clicked on the link for the questionnaire in the invitation email; however, only 1807 completed the survey yielding the gross response rate of 9%. Filtering the results based on the first qualifying question 899 respondents who stayed in a hotel within the last 12 months were identified. The second qualifying question eliminated 325 (36.2%) those respondents who did not use their credit cards to pay for any of the services in their last hotel. Based on the elimination of participants who did not meet these requirements, 574 fully completed responses were qualified for the study and, used for further analysis. The study yielded 2.8% net response rate.

Non-response bias analysis requires comparison of non-respondents with respondents of the study. Rylander, Propst, and McMurtry (1995) suggested that late respondents and non-respondents were alike and wave analysis and respondent/non-respondent comparisons yield the same results. Based on this, late respondents were used

as a proxy for non-respondents and a non-response analysis using wave analysis (early versus later respondents) was conducted to determine, (1) whether non-respondents and respondents differed significantly, (2) whether equivalent data from those who did not respond would have significantly altered the findings. For this purpose all respondents were divided into two groups according to the date they filled out the questionnaire. The responses were collected during the period between January 5, 2010 and March 3, 2010 totaling 58 days. February 2, 2010 was chosen to be the cut-off point for this sample. An independent sample t-test showed that there is no significant difference between the mean scores of early and late respondents with regard to the following: perceived service quality, overall satisfaction, revisit intentions and likelihood of recommending a hotel to others. After concluding that the sample does not suffer from non-response bias, the research proceeded with data analysis. The next section introduces the data analysis strategy.

3.6 Data Analysis Strategy

Statistical Package for Social Sciences (SPSS) version 16.0 and SmartPLS software were utilized to perform data analysis. Data analysis started with looking at the descriptive statistics of the sample. As almost all demographic (gender, marital status, education, etc.) and travel behavior (hotel type, purpose of the trip, room charge) characteristics were recorded as categorical variables, researchers requested frequencies reports for every one of them. Descriptive statistics are important for understanding of the data because they show the distribution for every variable.

Prior to hypotheses testing confirmatory factor analysis was conducted in order to check reliability and validity of SERVPERF scale used to measure service quality in this study. Factor analysis is an appropriate statistical tool to investigate if two or more variables measure aspects of a common underlying dimension (Field, 2009). Confirmatory instead of exploratory factor analysis was utilized in this study because SERVPERF is a well established scale. Confirmatory factor analysis (CFA) was employed to check if the variables load in the same dimensions that were identified in the previous literature and consequently measure the same phenomena that they were designed to measure.

To comply with the requirement of similar groups for minimum diversity experimental design, multivariate analysis of variance for all pre-test dependent variables across different treatments (independent variable). MANOVA is utilized to see the effects of categorical variable (treatment) on multiple dependent interval variables (service quality, satisfaction, revisit intentions and word-of-mouth) together instead of one at one time (Gliner et al., 2009). As expected, the test revealed no significant difference between the groups for pre-test measures.

Paired-samples t-test was chosen as a proper technique for the hypotheses testing. Another MANOVA analysis involving all pre-test and post-test measures was conducted to controls for Type I error that can be accumulated when doing multiple t-tests. After MANOVA analysis confirmed a significance of overall model it was decided to proceed with testing individual hypotheses using t-tests. The hypotheses stated for the study investigate the impact of the treatments on dependent variables: service quality,

satisfaction, revisit intentions and word-of-mouth. This requires a comparison of the variable ratings (mean scores) before the treatment and after the treatment. Paired-samples t-test is an appropriate tool to find out if there is a statistically significant difference for one dependent variable with repeated measures (Field, 2009; Gliner et al., 2009). Afterwards, analysis of variance (ANOVA) and post-hoc analysis were employed to investigate if there is statistically significant difference in the outcomes across three treatments.

Chapter 4

FINDINGS

4.1 Sample Demographic Statistics

Descriptive analysis of the sample is presented in the Table 7. Among all respondents who stayed in a hotel in the United States within the last 12 months, two thirds (66.4%) were females and one third were males (33.6%). Forty-eight point four percent of the respondents were married and 38.3% were single. Most frequently reported age category is between 45 and 54 years old (23.3%), and 22.1% were aged between 18 and 24. Educational characteristics were as follows: 34.1% of the respondents completed some college work, 25.6 % held bachelor's degree and 13.8% received associate degree. One quarter (26.5%) of the respondents reported their annual income to be in the range from $25,001 to $50,000, another quarter (23.5%) reported annual income of $25,000 or less.

Table 7. Sample demographic statistics

Variable	%	Variable	%
Hotel type		**Gender**	
Luxury	5.9	Female	66.4
Upscale	28.0	Male	33.6
Midscale	45.6		
Economy	17.6	**Marital Status**	
Bed & Breakfast	0.5	Single	38.3
Other	2.3	Married	48.4
		Separated	1.9
Purpose		Divorced	8.4
Business	12.9	Widowed	1.9
Leisure	70.0	Prefer not to answer	1.0
Combination	17.1		
		Education	
Room Charge		High School	13.2
Less than $50	8.5	Some college	34.1
$ 51-100	34.8	Associate degree (2 year)	13.8
$ 101-150	30.0	Bachelors Degree (4 year)	25.6
$ 151-200	14.5	Masters Degree	10.1
Over $ 200	12.2	Doctorate Degree	2.3
		Other	.9
Annual income			
$25,000 or less	23.5	**Age**	
$25,001- $50,000	26.5	Younger than 18	.2
$50,001-$75,000	16.4	18-24	22.1
$75,001-$100,000	12.4	25-34	16.7
$100,001 - $150,000	5.7	35-44	18.1
$150,001- $200,000	1.9	45-54	23.3
$200,001-$250,000	.5	55-64	13.1
$250,001 or more	1.0	65 or older	6.4
Prefer not to answer	11.1		

From the perspective of travel characteristics, 45.6% of the respondents stayed in midscale hotels, 28% stayed in upscale hotels and 17.6% in economy properties. Majority of the survey participants (70%) traveled for leisure, 17.1% combined leisure and business purposes in one trip and 12.9% traveled solely for business. The most frequently

reported room rate paid was between $51 and $100 (34.8%) and next largest category reportedly paid in a range of $101 to $150 for their room. Even though the most frequently reported room rate range ($51-$150), which may seem to be low when compared to the most frequently reported hotel types (midscale and upscale), an analysis showed that these two variables are positively correlated with the correlation coefficient of 0.304 ($p<0.01$): when the hotel type increases (from budget to luxury) the hotel room rate also increases. The relatively low room rates reported by respondents can be, most probably, explained by current economic situation in the United States.

The analysis showed that the sample was overrepresented by females and leisure travelers. An independent-sample t-test was conducted to compare the pre-test mean score provided by (1) female and male respondents and (2) business and leisure travelers. A comparison of answers given by males and females showed that there is no gender bias in the sample. Also, no significant difference was found based on the comparison of answers provided by leisure and business travelers. Based on this, the researcher inferred that the sample was a fair representation of the target population of US travelers.

4.2 Reliability Analysis

Prior to hypotheses testing, a confirmatory factor analysis (CFA) for the full data set was conducted using SmartPLS software for 22 SERVPERF statements. Five dimensions of the SERVPERF instrument was validated in the CFA. In addition, Cronbach's alpha reliability scores for the five SERVPERF dimensions were calculated and the scores are presented in Table 8.

Table 8. Reliability analysis for full dataset

Service Performance Dimension	Cronbach's Alpha
Tangibles	0.915
Reliability	0.945
Responsiveness	0.937
Assurance	0.955
Empathy	0.952

High reliability scores were expected given the fact that service quality dimensions of SERVQUAL and SERVPERF are well established and widely used in the literature (Berry, Parasuraman, & Zeithaml, 1988; Brown, Churchill, & Peter, 1993; Lau, Akbar, & Fie, 2005; Yee et al., 2009; Zeithaml et al., 1988; Zeithaml et al., 2006). High reliability scores for SERVPERF dimensions for both the pilot study and full data set show across different samples the instrument is very reliable. Based on this, aforementioned service quality dimensions were used during the data analysis to test the hypotheses.

4.3 Hypotheses testing

Before testing the individual hypotheses, Multiple Analysis of Variance (MANOVA) was conducted to see whether the means of the dependent variables were different across factors. MANOVA F statistic (3.831) yielded a significant overall value

for the multivariate test. For this reason, the research proceeded with the individual paired-t tests to test every hypothesis.

MANOVA analysis of pre-test scores for all dependent variables across treatments showed that there is no significant difference. It means that three groups formed by the different treatments that respondents received during the study were similar. Based on this, study proceeded with further analysis of these three groups. As was mentioned earlier, respondents were assigned to one of the groups randomly by the system hosting an online questionnaire. Among 574 respondents qualified for the study, 191 received treatment 1, 196 received treatment 2 and 187 received treatment 3. A paired-sample t-test was utilized to test the hypotheses. The results are presented and described below for each of three scenarios.

Hypotheses testing for treatment 1.

Table 9 below represents the results of paired sample t-test for treatment 1 when the respondents were exposed to a security breach situation and the information from their credit cards was stolen.

Table 9. Paired sample t-test results for treatment 1 (security breach, credit card stolen)

N	Variables	Pre Test		Post test		Dif.	t	df	Sig.
		Mean*	SD	Mean*	SD				
1	Tangibles	5.52	1.19	5.65	1.20	0.13	-0.13	190	0.002**
2	Reliability	5.69	1.21	5.56	1.30	-0.13	2.4	190	0.018***
3	Responsiveness	5.76	1.23	5.73	1.32	-0.03	0.48	190	0.630
4	Assurance	5.91	1.19	5.52	1.34	-0.39	6.34	190	0.000**
5	Empathy	5.77	1.20	5.75	1.29	-0.02	0.38	190	0.707
6	Overall Service Quality	5.73	1.12	5.65	1.20	-0.08	2.15	190	0.033***
7	Overall Satisfaction	6.00	1.29	5.51	1.56	-0.49	5.82	190	0.000**
8	Likelihood to come back	5.90	1.56	4.97	1.99	-0.92	7.23	190	0.000**
9	Likelihood of recommending this hotel	5.94	1.47	4.87	2.08	-1.07	8.08	190	0.000**

n=191 *: 1=Strongly Disagree 7=Strongly Agree **= Significant at p≤0.01 level ***p≤0.05

H1a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the information security breach - stolen scenario (treatment 1) and after it.

A comparison of means for service quality dimensions showed a significant difference for only three dimensions, where surprisingly tangibles became significantly higher after the treatment than before the treatment (p≤0.01). As expected, reliability and assurance were rated significantly lower after the treatment 1 (p≤0.05 and p≤0.01 respectively). No significant difference was found for responsiveness and empathy. Overall, the mean of service quality dropped from 5.73 to 5.65 and this decrease was found to be significant (p≤0.05).

H1b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the information security breach - stolen scenario (treatment 1) and after it.

The mean for overall satisfaction before treatment 1 was 5.75 while it was 5.51 after the treatment. According to the results of this hypothesis testing, treatment 1 had a significant negative effect on customers' overall satisfaction with their last hotel stay ($p \leq 0.01$).

H1c: There is a significant difference between the customers' revisit intentions to the brand before reading the information security breach - stolen scenario (treatment 1) and after it.

A paired sample t-test showed a significantly lower likelihood of coming back to a hotel after exposure to treatment 1 ($p \leq 0.01$). The mean score decreased from 5.90 before reading the treatment 1 to 4.97 after the treatment.

H1d: There is a significant difference between the customers' likelihood of recommending the brand before reading the information security breach - stolen scenario (treatment 1) and after it.

While the mean score of the customers' likelihood of recommending the brand before reading the treatment 1 was 5.94, after reading the treatment it became 4.87. Likelihood of recommending a hotel was rated significantly lower in the post-test in treatment 1 ($p \leq 0.01$).

In summary, t-test showed significant decrease in the mean scores of all dependent variables ($p \leq 0.05$) after reading treatment 1. The results suggest that negative

news about information security breach result in lower perception of service quality and guest satisfaction. Moreover, after treatment 1 guests are less likely to recommend a hotel to relatives and friends and less likely to come back to a property that experiences an information security breach.

Hypotheses testing for treatment 2.

Table 10 below represents the results of paired sample t-test for treatment 2 when the respondents were exposed to a security breach situation and the information from their credit cards was NOT stolen.

Table 10. Paired sample t-test results for treatment 2 (negative, credit card not stolen)

N	Variables	Pre Test		Post test		Dif.	t	df	Sig.
		Mean*	SD	Mean*	SD				
1	Tangibles	5.52	1.25	5.57	1.32	0.05	-0.85	195	0.396
2	Reliability	5.57	1.38	5.42	1.52	-0.15	1.93	195	0.055
3	Responsiveness	5.62	1.43	5.58	1.45	-0.04	0.52	195	0.604
4	Assurance	5.75	1.39	5.44	1.47	-0.31	3.73	195	0.000**
5	Empathy	5.65	1.35	5.53	1.44	-0.12	1.74	195	0.084
6	Overall Service Quality	5.62	1.30	5.51	1.39	-0.11	1.66	195	0.099
7	Overall Satisfaction	5.69	1.48	5.41	1.67	-0.28	4.09	195	0.000**
8	Likelihood to come back	5.57	1.75	5.06	1.98	-0.51	5.51	195	0.000**
9	Likelihood of recommending this hotel	5.62	1.70	5.08	1.980	-0.54	6.16	195	0.000**

n=196 *: 1=Strongly Disagree 7=Strongly Agree **= Significant at p≤0.01 level

H2a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the information security breach – not stolen scenario (treatment 2) and after it.

Hypothesis testing showed a negative significant difference in the perceptions of assurance after reading the treatment 2 ($p \leq 0.01$). However, the changes for the other four dimensions (tangibles, reliability, responsiveness and empathy) and overall service quality were not found to be significantly different.

H2b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the information security breach – not stolen scenario (treatment 2) and after it.

A significant difference was found between the customers' overall satisfaction of their last hotel stay before reading the treatment 2 and after it. The treatment impacted the overall satisfaction negatively ($p \leq 0.01$): the mean score decreased from 5.69 to 5.41.

H2c: There is a significant difference between the customers' revisit intentions to the brand before reading the information security breach – not stolen scenario (treatment 2) and after it.

The respondents exposed to the treatment 2 were found to be significantly less likely to come back to a property where they last stayed after reading the treatment 2 ($p \leq 0.01$). The mean score in the pre-test was 5.57, while in the post-test it was 5.06.

H2d: There is a significant difference between the customers' likelihood of recommending the brand before reading the information security breach – not stolen scenario (treatment 2) and after it.

A significant decrease in customers' likelihood of recommending the hotel brand was found after reading the treatment 2 from the mean score of 5.62 to 5.08 ($p \leq 0.01$).

In summary, the results of hypotheses testing for treatment 2 showed a significant decrease in mean scores of satisfaction, likelihood of recommending a hotel and likelihood of coming back. However, the overall satisfaction was not affected by the treatment. As was mentioned before, treatment 2 is a neutral scenario but the researcher expected that, just as treatment 1, this scenario would also have a negative impact. This suggestion was confirmed for three out of four variables except perceived service quality. Potential explanation can be as follows: if guest's information was not stolen, a hotel still performed a service of protecting this particular guest properly. However, the hypotheses testing showed that even if guest's information was not compromised during the breach, news about the breach still decrease the satisfaction with the last hotel stay and shift behavioral intentions (likelihood of coming back to a hotel and likelihood of recommending it to others) negatively.

Hypotheses testing for treatment 3.

Table 11 below represents the results of paired sample t-test for treatment 3 when the respondents were exposed to a positive scenario, where the hotel passed a

comprehensive security audit thus ensuring compliance with data security practices in the property.

Table 11. Paired sample t-test results for treatment 3 (positive)

N	Variables	Pre Test		Post test		Dif.	t	df	Sig.
		Mean*	SD	Mean*	SD				
1	Tangibles	5.51	1.17	5.64	1.09	0.13	-2.41	186	0.017***
2	Reliability	5.56	1.32	5.67	1.27	0.11	-2.07	186	0.040***
3	Responsiveness	5.59	1.32	5.67	1.30	0.08	-1.53	186	0.129
4	Assurance	5.78	1.26	5.79	1.24	0.01	-0.21	186	0.831
5	Empathy	5.64	1.30	5.68	1.27	0.04	-0.74	186	0.463
6	Overall Service Quality	5.61	1.20	5.69	1.18	0.08	-1.62	186	0.106
7	Overall Satisfaction	5.74	1.35	5.90	1.30	0.16	-2.97	186	0.003**
8	Likelihood to come back	5.73	1.67	5.83	1.55	0.10	-2.19	186	0.030***
9	Likelihood of recommending this hotel	5.72	1.72	5.84	1.61	0.12	-2.25	186	0.026***

n=187 *: 1=Strongly Disagree 7=Strongly Agree **= Significant at p≤0.01 level ***p≤0.05

H3a: There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the positive information security scenario (treatment3) and after it.

The rating of two of service quality dimensions, namely tangibles and reliability, increased significantly after receiving treatment 3 (p≤0.05). However, the differences for all other dimensions and overall service quality were not found to be significantly different.

H3b: There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the positive information security scenario (treatment3) and after it.

Customers overall satisfaction significantly increased after reading the treatment 3: the mean score rose from 5.74 to 5.90 ($p \leq 0.01$).

H3c: There is a significant difference between the customers' revisit intentions to the brand before reading the positive information security scenario (treatment3) and after it.

A significant positive difference was found between the customers' revisit intentions before and after reading the treatment 3 ($p \leq 0.05$). The mean score calculated for the pre test was 5.73 and 5.83 in the post test.

H3d: There is a significant difference between the customers' likelihood of recommending the brand before reading the positive information security scenario (treatment3) and after it.

The mean score of the customers' likelihood of recommending the brand rose from 5.72 in the pre test to 5.84 in the post test. As the result of the treatment, customers were found to be significantly more likely to recommend the hotel brand after reading the treatment 3 than before it ($p \leq 0.05$).

As was stated before, the researcher expected no effect or positive effect of the treatment on the outcome variables. The results of hypotheses testing showed that positive scenario did not affect service quality. Information security is not the primary service of hotels, so, it is understandable that the positive treatment did not increase

guests' perceptions of service quality. Interestingly, the results of the analysis revealed an increase in satisfaction, likelihood of recommending a hotel and likelihood of coming back. It means that after hearing good news respondents feel better about the hotel where they last stayed (their satisfaction increased). It also shifts their behavioral intentions, making guests more likely to recommend this hotel and come back to it in the future.

The summary of the hypotheses testing for all treatments is presented in Table 12.

Table 12. Summary of hypotheses testing

Hypotheses	Treatment 1	Treatment 2	Treatment 3
a. There is a significant difference between the customers' perception of service quality of their last hotel stay before reading the treatment and after it	Supported (Pre > Post)	Not supported	Not supported
b. There is a significant difference between the customers' overall satisfaction of their last hotel stay before reading the treatment and after it	Supported (Pre> Post)	Supported (Pre> Post)	Supported (Pre<Post)
c. There is a significant difference between the customers' revisit intentions to the brand before reading the treatment and after it	Supported (Pre> Post)	Supported (Pre> Post)	Supported (Pre<Post)
d. There is a significant difference between the customers' likelihood of recommending the brand before reading the treatment and after it	Supported (Pre> Post)	Supported (Pre> Post)	Supported (Pre<Post)

As it was identified during the analysis, the hypotheses were fully supported only for satisfaction, revisit intentions and likelihood of recommending a hotel to others. Looking at the mean scores of the post-test for those variables, one can observe that the

scores for the positive treatment (treatment 3) are consistently higher than for the negative treatments (treatments 1 and 2) (Table 13).

Table 13. Post-test mean scores for different treatments

N	Variables	Treatment 1		Treatment 2		Treatment 3	
		Mean*	SD	Mean*	SD	Mean*	SD
1	Overall Satisfaction	5.51	1.56	5.41	1.67	5.90	1.30
2	Likelihood to come back	4.97	1.99	5.06	1.98	5.83	1.55
3	Likelihood of recommending this hotel	4.87	2.08	5.08	1.980	5.84	1.61

n_1=191, n_2=196 , n_3=187 *: 1=Strongly Disagree 7=Strongly Agree

To determine if this observation is statistically significant a comparison of these scores was conducted using general linear model, multivariate function (MANOVA) in SPSS. The analysis showed a significant difference ($F=6.363$, $p\leq0.01$). Based on that, a series of ANOVA tests (general linear model, univariate function in SPSS) was conducted to find out where exactly those differences are.

Statistically significant differences across treatments were found for all variables: satisfaction ($F=5.621$, $p\leq0.01$), revisit intentions ($F=12.164$, $p\leq0.01$) and likelihood of recommending their hotel to others ($F=13.449$, $p\leq0.01$). Upon further analysis the difference is statistically significant only for the following pairs: treatment 1 – treatment 3 and treatment 2 – treatment 3. There was no statistically significant difference found between the mean scores for treatment 1 and treatment 2 (negative and

neutral scenarios). The results of the Post-Hoc (Tukey) tests for the pairs of treatments are presented in Table 14 and Table 15.

Table 14. Post-Hoc test results for the post-test for treatments 1 and 3

N	Variables	Treatment 1		Treatment 3		Dif.	Sig.
		Mean*	SD	Mean*	SD		
1	Overall Satisfaction	5.51	1.56	5.90	1.30	0.39	0.034
2	Likelihood to come back	4.97	1.99	5.83	1.55	0.86	0.000
3	Likelihood of recommending this hotel	4.87	2.08	5.84	1.61	0.97	0.000

n_1=191, n_3=187 *: 1=Strongly Disagree 7=Strongly Agree

Table 15. Post-Hoc test results for the post-test for treatments 2 and 3

N	Variables	Treatment 2		Treatment 3		Dif.	Sig.
		Mean*	SD	Mean*	SD		
1	Overall Satisfaction	5.41	1.67	5.90	1.30	0.49	0.004
2	Likelihood to come back	5.06	1.98	5.83	1.55	0.77	0.000
3	Likelihood of recommending this hotel	5.08	1.980	5.84	1.61	0.76	0.000

n_2=196 , n_3=187 *: 1=Strongly Disagree 7=Strongly Agree

In summary, all but two hypotheses stated for the current study were supported. Significant differences were found in the post-test mean scores between the positive (treatment 3) and each of the negative scenarios (treatment 1 and treatment 2). An analysis of the findings is presented in the conclusions and discussions section below.

Chapter 5

CONCLUSIONS

5.1 Conclusions and Discussion

An impact of information security on hotel guests' perception of service quality, overall satisfaction, revisit intentions and likelihood of recommending a hotel to others was studied by exposing the study participants to three different scenarios: negative (treatment 1), when the guest's credit card information was stolen during the security breach at a hotel where the participant last stayed; neutral (treatment 2), when there was a security breach at a hotel where the participant last stayed but the guest's credit card information was not stolen; and positive (treatment 3), when a hotel where the participant last stayed has passed a comprehensive security audit confirming high information security in the property and this information was passed onto the guest. All except two hypotheses developed for the study were supported revealing a significant impact of treatments on customers' perceptions of service quality (only for treatment 1) and behavioral intentions (for all treatments).

Treatment 1 (breach – credit card stolen) was found to have a significant impact on the following dimensions of service quality: tangibles, reliability and assurance. However, it is surprising to see an increase in the perception of tangibles

quality caused by treatment 1. As it s stated in the literature that tangibles refer to the equipment used in a hotel, furniture and materials associated with the service (Zeithaml et al., 2006). Given the fact that information security falls into the intangible dimension of service quality and that the tangible infrastructure required to ensure the information security is usually invisible to hotel guests, researchers would not anticipate any impact of the treatments used in this study on the tangible dimension. As expected, treatment 1 caused a decrease in customers' perceptions of the quality of reliability and assurance. These dimensions include problem solving, keeping error-free records and promises (reliability) as well as instilling confidence in customers about employees' knowledge, safety of transactions with the company, and its trustworthiness (assurance) (Zeithaml et al., 2006). In other words, it can be concluded that identity theft undermines a hotel credibility with respect to perceived service quality and customers' trust. Furthermore, overall satisfaction, revisit intentions, and the likelihood of recommending a hotel to others were also negatively affected by the information about a security breach. According to the results found in this study, those travelers who received negative news about the theft of their credit card information during the breach in a hotel indicated significantly lower satisfaction with the hotel where they stayed last and also were less likely to come back to that property and recommend it to their family and friends. These findings are in line with propositions of Cobanoglu (2008a) and Haley and Connolly (2008) about the negative impact of PCI non-compliance and information security breach on hotel's reputation. If, in case of security breach, guests are significantly less satisfied and less likely to return, this will result in a decrease in hotel's sales, business volume,

and profitability. The fact that information security breach diminishes guests' likelihood to recommend a hotel to others might cause a snowball effect where the aforementioned negative outcomes have a longer lasting impact.

Treatment 2 (breach – credit card not stolen), being introduced as a neutral scenario, also was found to have a significant negative impact on customers' perception of the assurance dimension of service quality without negatively affecting the other dimensions and overall service quality. This finding seems to be logical and corresponds with the effect of the treatment 1 on the perceived service quality (where assurance was also negatively affected). Given the fact, that it was found that treatment 2 was smaller in terms of the negative damage to the respondents perceptions, one can foresee it to have less impact on overall service quality. This proposition was eventually confirmed by the analysis: only one out of five service quality dimensions was found to be significantly lower in participants responses and the respondents' perception of the overall service quality was not negatively affected. From this we can conclude that information about security breach that did not directly affect a particular individual does not significantly shift her evaluation of the service quality received during the last hotel stay. However, overall satisfaction and future behavioral intensions were negatively affected. Those respondents who received the second treatment scenario indicated to have a lower likelihood of coming back to the property as well as of recommending it to others, after hearing the news about security breach at the hotel of their last stay. It means that, news about information security breach affect guests' satisfaction, revisit intention and likelihood of coming back with regard to the fact if their information was compromised

during the breach or not. In summation of the results of the current study, both negative scenarios of information security breaches resulted in an overall negative impact of respondents' service perceptions of customers' satisfaction and behavioral intensions, thus confirming the study's hypotheses. This leads to the conclusion that in spite of the degree to which each guest was affected; news about security breach diminish the hotel's reputation and have a negative impact on guests' retention and consequently on business volume. Given the fact that being PCI compliant for a merchant will likely to reduce the risk of being breached (Haley & Connolly, 2008), hotels should seek full compliance with PCI requirements. Today, two states in the U.S. passed laws that require merchants to be compliant with set of information security regulations that are in line with PCI Compliance requirements. It is conceivable that other states will likely to follow suit with the passage of state regulations with the expectation that these efforts will increase the security of consumer private information.

It is interesting that in the current study, treatment 3 (positive) was found to have a positive impact on service quality, overall guest satisfaction, likelihood of coming back to the property, and recommending the hotel to others. Respondents' evaluations of two of the service quality dimensions, namely, tangibles and reliability, increased significantly after the exposure to treatment 3. Again, the change in the tangibles dimension was surprising for this researcher, while increase in reliability scores seem to be very logical. However, no significant difference was found in the respondents' perceptions of overall service quality. At the same time, positive news about enhanced information security protection in a hotel resulted in significant improvement in the

overall satisfaction, revisit intentions, and positive word-of-mouth. One can speculate that this was due to the fact that guests appreciate hotel's attention and protection of their privacy and will trust that property more. These findings suggest that hoteliers should continue to increase and sustain their efforts in securing guest information and credit card transactions and moreover, to promote their achievements in this area. The results of the current study suggests that the public relations efforts of hotels in communicating their good practices of information security may be result it positive perceptions of their services by their guests. Additionally, these positive achievements of information security may be appropriate to exploit in the advertising to their market segments.

Overall, two scenarios that illustrated information security breach provided an evidence of the impact of breaches on hotel guests' overall satisfaction, revisit intentions, and likelihood of recommending a hotel to others. The results of this study support the propositions that hotel reputation decreases when there are information security breaches and also provides strong evidence for hoteliers to maintain PCI compliance. As it is stated in the literature, within the hospitality industry hotels are believed to be only about 50% compliant with PCI security standards (Cobanoglu, 2008b). Negative effect of information security breach on company's reputation as found in the current study justifies the investments expended to adhere to PCI compliance standards. In addition to the monetary and legal costs, non-compliance with PCI may cause a decrease in customers' perception of service quality, overall satisfaction, and negatively shift future behavior, which all will result in a significant negative impact on the bottom-line of the company. Moreover, advertising the information security

precautions and compliance may help hotels to build a stronger reputation in the marketplace.

Answering the research questions stated for the study, we can conclude that information about data security in hotels does not consistently affect guests' perceptions of service quality. This variable was impacted by the negative treatment (treatment 1), however, no impact was found after neutral (treatment 2) and positive (treatment 3) scenarios. The study confirms that there is an impact of information security breach on hotel guest satisfaction, revisit intention and word-of-mouth. The impact was found to be negative for both security breach scenarios (treatment 1 and treatment 2) regardless of whether guest information was stolen during the breach. On the other hand, positive news about enhanced security protection in a hotel produced higher satisfaction scores, increased likelihood of coming back and recommending a hotel to others.

In summary, the current study contributes to the body of knowledge by investigating the impact of credit card information security breach on hotel guest satisfaction and future behavior. Limitations and potential directions for future research emerging from this study are discussed in the next session.

5.2 Limitations and Future Research

One of the limitations of the study is application of the online instrument utilized for data collection. Only people with valid email addresses could be recruited for the study. This affects generalizability of the findings, limiting collection of data only to active Internet users. However, given the 74.1% Internet penetration in the United States

("Internet Usage Stats," 2009) web-based instrument should not be such a limiting factor of the study.

It should also be pointed out that females and leisure travelers are heavily represented in the sample. One would prefer a sample that is more evenly distributed. However, preliminary testing showed that there were no significant difference between the pre-test scores of service quality, overall satisfaction, revisit intentions and likelihood of recommending a hotel given by males and females and business and leisure travelers. Based on that, it was concluded that the sample does not suffer from a bias based on gender or reason for travel. However, this testing did not cover post-test behavior. These potential biases and issues should lead to future research that will explore if there is a statistically significant difference in attitudes towards information security breach and consequent consumer behavior between male and female travelers, business and leisure travelers, and frequent and non-frequent travelers. More advanced statistical tools such as structural equation modeling (SEM) can be used to develop and compare models for different types of travelers.

Another research topic that extends the work of the current study is to explore the longevity of the effects of the treatments presented to the respondents. Based on the findings from the current research that found that information security breaches has a negative impact on the hotel guests' perception of service quality, overall satisfaction, revisit intentions, and likelihood of recommending a hotel to others, one can explore if there is an opportunity for hotels to recover from the service failure and how long will it take to change customers' negative attitudes and bring them back to the hotel.

Another need for research attention identified by the researchers is for designing a future study that develops an assessment instrument specifically designed to measure technology quality and satisfaction in the lodging industry. While for the current study it was useful to utilize the PERFQUAL instrument to test if the information security breach/no-breach scenarios shift customers' perceptions and intentions overall, a specific measurement scale should be proposed for the capture of information technology quality and may provide a more precise picture for hoteliers and researchers working in the field of hotel information technology. With the increasing role of technology in the hospitality industry (Collins & Cobanoglu, 2008; Kasavana & Cahill, 2007) and its impact on the perceptions of consumers on the quality of hotel service (Connolly & Haley, 2008), it is important to measure and document guests' perception of IT service quality and satisfaction. A proposed scale can include an assessment of quality of different technologies that guests face before, during, and after a hotel stay. It should reflect consumers' quality rating of web sites, booking engines, in-room technologies, security (e.g. electronic locking systems), and so forth. Alternatively, IT elements can be incorporated into PERFQUAL instrument, which is a well established model, because different functions that IT serves in a hotel can be described through the same dimensions. Deeper analysis of this idea can reveal a necessity of new dimensions, which will describe more aspects of service quality that emerged over time.

REFERENCES

About the PCI Data Security Standard (PCI DSS). (2009). Retrieved on 06/02/2009 from https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

2009 Identity Theft Statistics . (2009). Retrieved February 27, 2010, from http://www.spendonlife.com/guide/2009-identity-theft-statistics.

Akbaba, A. (2006). Measuring service quality in the hotel industry: A study in a business hotel in Turkey. *International Journal of Hospitality Management*, *25*(2), 170–192.

Berezina, E., & Cobanoglu, C. (2009, September 19). Does IT matter? The Impact of technology amenities on hotel guest satisfaction. Presented at the Annual Convention of Hospitality Financial and Technology Professionals, Las Vegas, NV.

Berry, L. L., Parasuraman, A., & Zeithaml, V. A. (1988). The service-quality puzzle. *Business Horizons*, *31*(5), 35–43.

Boulding, W., Karla, A., Staelin, R., & Zeithaml, V. A. (1993). A dynamic process model of service quality: from expectations to behavioral intentions. *Journal of Marketing Research*, *30*(1), 7-27.

Bouman, M., & Van der Wiele, T. (1992). Measuring service quality in the car service industry: building and testing an instrument. *International Journal of Service Industry Management, 3*, 4–4.

Brown, T. E., & Ulijn, J. M. (2004). *Innovation, entrepreneurship and culture: the interaction between technology, progress and economic growth*. Edward Elgar Publishing.

Brown, T. J., Churchill, G. A., & Peter, J. P. (1993). Improving the measurement of service quality. *Journal of Retailing, 69*, 127–127.

Bucks, B. K., Kennickell, A., Mach, T., & Moore, K. (2009). Changes in U.S. Family Finances from 204 to 2007: evidence from the Survey of Consumer Finances. *Federal Reserve Bulletin, February*. Retrieved February 27, 2010, from http://www.federalreserve.gov/pubs/bulletin/2009/pdf/scf09.pdf.

Buttle, F. (1996). SERVQUAL: review, critique, research agenda. *European Journal of Marketing, 30*(1), 8–32.

Campbell, K., Gordon, L. A., Loeb, M. P., & Zhou, L. (2003). The economic cost of publicly announced information security breaches: empirical evidence from the stock market. *Journal of Computer Security, 11*(3), 431–448.

Canavan, J. E. (2001). *Fundamentals of network security*. Artech House Publishers.

Carrillat, F. A., Jaramillo, F., & Mulki, J. P. (2007). The validity of the SERVQUAL and SERVPERF scales: A meta-analytic view of 17 years of research across five continents. *International Journal of Service Industry Management, 18*(5), 472–490.

Central Intelligence Agency. (2010). *The world factbook. North America. United States.* Retrieved April 16, 2010, from http://webcache.googleusercontent.com/search?q=cache:1XDMEvdhY7sJ:https://www.cia.gov/library/publications/the-world-factbook/geos/us.html+share+of+services+in+us+gdp&cd=1&hl=en&ct=clnk&gl=us&client=firefox-a.

Chakravorti, S. (2003). Theory of credit card networks: A survey of the literature. *Review of Network Economics, 2*(2).

Chakravorti, S., & To, T. (2007). A theory of credit cards. *international Journal of industrial organization*, *25*(3), 583–595.

Cobanoglu, C. (2001). Unpublished Thesis. Analysis of business travelers' hotel selection and satisfaction. Oklahoma State University.

Cobanoglu, C. (2007). PCI What? *HT Magazine*. Retrieved December 20, 2009, from http://www.htmagazine.com/ME2/Sites/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=6A4F7994987648E18CCF10AAD9AFD947&SiteID=AAED287C668148CCB10E4FBA73326A07.

Cobanoglu, C. (2008a). Understanding PCI Version 1.2. *HT Magazine*. Retrieved December 19, 2009, from http://www.htmagazine.com/ME2/dirmod.asp?sid=783D4AA2541D483C98659D20A3539C6E&nm=Additional&type=MultiPublishing&mod=PublishingTitles&

mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=CC1FC41FF38F428E94608244CE634976.

Cobanoglu, C. (2008b). PCI Security Woes. *HT Magazine.* Retrieved December 19, 2009, from http://www.htmagazine.com/ME2/dirmod.asp?sid=783D4AA2541D483C98659D20A3539C6E&nm=Additional&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=7DF7AC1459464A4BBC32B818E75A57F6.

Cobanoglu, C., & DeMicco, F. J. (2007). To be secure or not to be: Isn't this the question? A critical look at hotel's network security. *International Journal of Hospitality & Tourism Administration, 8*(1), 43–59.

Collins, G. R., & Cobanoglu, C. (2008). *Hospitality information technology: Learning how to use it* (6th ed.). Dubuque, IA: Kendall/Hunt Publishing Company.

Committee on Payment and Settlement Systems. (2009). *Statistics on payment and settlement systems in selected countries. Figures for 2008*. Bank for International Settlements. Retrieved February 27, 2010, from http://www.bis.org/publ/cpss88.pdf.

Compliance validation details for merchants. (2009). Retrieved on 06/02/2009 from http://usa.visa.com/merchants/risk_management/cisp_merchants.html

Connolly, D. J., & Haley, M. (2008). PCI DSS compliance: Just whose responsibility is it? Retrieved March 12, 2010, from http://www.htmagazine.com/ME2/dirmod.asp?sid=&nm=&type=MultiPublishing

&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=D70138F32BB54C2ABED5EFDB27ACB157.

Crawford, C.S. (2009, June 1). Beyond PCI… The advent of cardholder data 'tokenization'. *The 2009 Eastern Region Hospitality Law Conference*, Baltimore, MD

Credit check: is your hotel PCI compliant? (2007). *Hotels*, January, 46 - 48

Cronin Jr, J. J., & Taylor, S. A. (1994). SERVPERF versus SERVQUAL: reconciling performance-based and perceptions-minus-expectations measurement of service quality. *The Journal of Marketing*, 125–131.

Cronin Jr., J. J., & Taylor, S. A. (1992). Measuring service quality: a reexamination and extension. *The Journal of Marketing*, *56*(3), 55–68.

Design and Analysis of Experimental and Quasi-Experimental Investigations from Blackwell Handbook of Research Methods in Clinical Psychology. (2003). Retrieved December 20, 2009, from http://proxy.nss.udel.edu:6959/entry/bkhrmcp/chapter_6_design_and_analysis_of_experimental_and_quasi_experimental_investigations.

Ekinci, Y., Prokopaki, P., & Cobanoglu, C. (2003). Service quality in Cretan accommodations: marketing strategies for the UK holiday market. *International Journal of Hospitality Management*, *22*(1), 47–66.

Federal Trade Commission. (2010). *Consumer sentinel network data book for January - December 2009*. Retrieved February 27, 2010, from http://www.ftc.gov/sentinel/reports/sentinel-annual-reports/sentinel-cy2009.pdf.

Field, A. (2009). *Discovering statistics using SPSS*. Sage Publications Ltd.

Garg, A., Curtis, J., & Halper, H. (2003). The financial impact of IT security breaches: What do investors think? *Information Security Journal: A Global Perspective, 12*(1), 22–33.

Gliner, J. A., Morgan, G. A., & Leech, M. (2009). *Research methods in applied settings: An integrated approach to design and analysis* (2nd ed.). Taylor & Francis Group.

Gomm, R. (2009). *Key concepts in social research methods*. UK: Palgrave Macmillan.

Grabosky, P. N., Smith, R. G., & Dempsey, G. (2001). *Electronic theft: unlawful acquisition in cyberspace*. Cambridge Univ Pr.

Haley , M., & Connolly, D. J. (2008). *The PCI compliance process for hotels*. American Hotel & Lodging Association.

Halsey, R. (2009). The real cost of data breach. Retrieved from http://www.pcicomplianceguide.org/merchants-20090416-cost-data-breach.php

He, F., & Mykytyn, P. P. (2007). Decision factors for the adoption of an online payment system by customers. *International Journal of E-Business Research, 3*(4), 1–32.

Hobson, J.S.P, & Ko, M. (1995). Counterfeit credit cards – how to protect hotel guests. *Cornell Hotel and restaurant Administration Quarterly,* August, p. 48 – 53

Hunt, R. (2003). An introduction to the economics of payment card networks. *Review of Network Economics, 2*(2), 80–96.

Internet Usage Stats - Population Statistics. (2009). . Retrieved March 17, 2010, from http://www.internetworldstats.com/america.htm.

Jain, S. K., & Gupta, G. (2004). Measuring service quality: SERVQUAL vs. SERVPERF scales. *Vikalpa, 29*(2), 25.

Jiang, J. J., Klein, G., & Crampton, S. M. (2000). A note on SERVQUAL reliability and validity in information system service quality measurement. *Decision Sciences, 31*(3), 725–740.

Johnson, B., & Christensen, L. (2008). *Educational research: quantitative, qualitative, and mixed approaches.* Los Angeles, CA: Sage Publications.

Kasavana, M. L. (1978). *Hotel Information Systems.* CBI Publishing Company.

Kasavana, M. L., & Cahill, J. J. (2007). *Managing technology in the hospitality industry* (5th ed.). Lansing, MI: American Hotel & Lodging Educational Institute.

Key Data Security Compliance Dates. (2009). Retrieved on 06/03/2009 from http://usa.visa.com/merchants/risk_management/cisp_key_dates.html

Kim, T. G., Lee, J. H., & Law, R. (2008). An empirical examination of the acceptance behavior of hotel front office systems: An extended technology acceptance model. *Tourism Management, 29*(3), 500–513.

Kotler, P., Bowen, J., & Makens, J. C. (2003). *Marketing for hospitality and tourism* (3rd ed.). Upper Saddle River, NJ: Pearson Education, Inc.

LaBelle, P., & Chatterjee, A. (2004). Securing your IT assets - the time is now. *Hospitality Upgrade, Summer2004*, 22-24.

Lau, P. M., Akbar, A. K., & Fie, D. Y. (2005). Service quality: a study of the luxury hotels in Malaysia. *Journal of American Academy of Business, 7*(2), 46–55.

Levin, A.K., & Hudak, R.G. (2009). Identity theft targets hospitality: protect guests. *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=E4482C1CF4A343A293D352C8A83C1724

Lorden, A.A. (2009). PCI going global. Hospitality Technology. Retrieved from http://www.htmagazine.com/ME2/Sites/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&SiteId=AAED287C668148CCB10E4FBA73326A07&tier=4&id=5737D36517AD4FAE8BD698BDB8362D61

McMillan, R. (2009). Hackers steal thousands of Wyndham credit card numbers. Retrieved from http://www.computerworld.com/action/article.do?command=viewArticleBasic&articleId=9128222

Ogle, J., Wagner, E., & Talbert, M. (2008). Hotel network security: A study of computer networks in U.S. hotels. *Cornel Hospitality Report*, *8*(15), 1-20.

Parasuraman, A., Zeithaml, V. A., & Berry, L. L. (1985). A conceptual model of service quality and its implications for future research. *The Journal of Marketing*, *49*(4), 41–50.

Qu, H., & Sit, C. Y. (2007). Hotel Service Quality in Hong Kong: An Importance and Performance Analysis. *International Journal of Hospitality & Tourism Administration*, *8*(3), 49-72.

Radisson Hotels & Resorts. (2009). Open letter to Radisson guests. *Radisson Hotels & Resorts*. Retrieved December 20, 2009, from http://www.radisson.com/openletter/openletter.html.

Reid, R. D., & Bojanic, D. C. (2009). *Hospitality marketing management* (4th ed.). Wiley.

Reynolds, R. A., Woods, R., & Baker, J. D. (2007). *Handbook of research on electronic surveys and measurements*. Idea Group Reference.

Rylander, R. G., Propst, D. B., and McMurtry, T. R. (1995). Nonresponse and recall biases in a survey of traveler spending. *Journal of Travel Research, 33* (4), 39-45.

Saleh, F., & Ryan, C. (1991). Analyzing service quality in the hospitality industry using the SERVQUAL model. *The Service Industries Journal*, *11*(3), 324–345.

Sammons, G. (2000). Technology: How hospitality sales managers use and view it! *Journal of Convention and Exhibition Management*, *2*, 83–96.

Sheldon, P. J. (1983). The impact of technology on the hotel industry. *Tourism Management*, *4*(4), 269–278.

Siguaw, J. A., Enz, C. A., & Namasivayam, K. (2000). Adoption of information technology in US hotels: strategically driven objectives. *Journal of Travel Research*, *39*(2), 192.

Skogland, I., & Siguaw, J. A. (2004). Understanding switchers and stayers in the lodging industry. *Cornell University Center for Hospitality Research Report*.

Smith, R. G., & Grabosky, P. (1998). Plastic Card Fraud. *Australian Banker*, *112*, 92–99.

Tenczar, J. (2008). PCI Sharpens its Teeth: Are You Ready? *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/Sites/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=1A8333A1BA3E428B90E9BED3550176B7&SiteID=AAED287C668148CCB10E4FBA73326A07

Varga, J. (1975). Safeguarding your computer resources. *Cornell Hotel and Restaurant Administration Quarterly*, *16*, 56–60.

Version 1.2 of PCI Data Security Standard Released. (2008). *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=7C3D9D1F483447D0B4AA49FFE82660AD

Vijayan, J. (2007). Minnesota becomes first state to make core PCI requirement a law. Retrieved March 23, 2010, from http://www.computerworld.com/s/article/9020923/Minnesota_becomes_first_state_to_make_core_PCI_requirement_a_law.

Visa Inc. (2009) U.S. PCI DSS compliance status. Retrieved March 23, 2010, from http://usa.visa.com/download/merchants/cisp_pcidss_compliancestats.pdf

Volpe, C. (2009). Is PCI enough? *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/Sites/dirmod.asp?sid=&nm=&type=MultiPublishing&mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1

&tier=4&id=F06D09D69E9248578A47EF5A7AE4A8B5&SiteID=AAED287C668148CCB10E4FBA73326A07

Yee, R. W., Yeung, A., & Cheng, T. (2009). An empirical study of employee loyalty, service quality and firm performance in the service industry. *International Journal of Production Economics*. Retrieved December 19, 2009, from http://proxy.nss.udel.edu:2109/scholar?hl=en&q=Yee+An+empirical+study+of+employee+loyalty%2C+service+quality&btnG=Search&as_sdt=2000&as_ylo=&as_vis=0.

Young, F. (2009). Is PCI compliance a law? Should it be? Retrieved March 23, 2010, from http://www.pcicomplianceguide.org/security-tips-20090227-pci-compliance-law.php.

Zabkar, V., Brencic, M. M., & Dmitrovic, T. (2009). Modelling perceived quality, visitor satisfaction and behavioral intentions at the destination level. *Tourism Management*.

Zeithaml, V. A., Berry, L. L., & Parasuraman, A. (1988). Communication and control processes in the delivery of service quality. *The Journal of Marketing*, *52*(2), 35-48.

Zeithaml, V. A., Bitner, M. J., & Gremler, D. D. (2006). *Services marketing: Integrating customer focus across the firm*. New York, NY: McGraw Hill/Irwin.