Journal of Hospitality Financial Management
The Professional Refereed Journal of the Association of Hospitality Financial Management Educators

Volume 18 | Issue 2 Article 5

Fall 10-14-2010

A Financial Analysis of Payment Card Industry Compliance Journey of A Hotel: A Case Study

Katerina Berezina
Oklahoma State University, katerina.berezina@okstate.edu

Cihan Cobanoglu
University of South Florida Sarasota-Manatee, CIHAN@CIHAN.ORG

A Financial Analysis of Payment Card Industry Compliance Journey of A Hotel: A Case Study

Cover Page Footnote
N/A

A Financial Analysis of Payment Card Industry Compliance Journey of a Hotel: A Case Study

Abstract

Payment card transactions have become an essential part of hotels operations. The purpose of this study is to explore the procedure, approximate the cost, and describe the real-life hotel experience of becoming PCI-compliant in order to provide guidelines and approximate expenses for recently opened hotels and for existing ones that are not PCI-compliant. A case study method approach was used. One hotel located in the Northeast part of the U.S. agreed to participate in this study. This is a limited-service, 120-room hotel; a major brand franchisee that is operated by a management company. The data was collected through a structured interview with the general manager of the hotel by the researchers. Findings indicated the cost for being PCI Compliant is not easy to calculate as many of the costs were integrated in typical costs of the hotel such as franchise fee and IT budget. Findings also suggested that the key elements every hotel is required to invest in to become PCI compliant; among them secure PMS/POS systems with firewalls and anti-virus software, and protected Internet networks. There are also some particular procedures (e.g. changing passwords, limiting access to the cardholders' information, etc.) that a hotel needs to follow: necessary training for employees and potentially monitoring and controlling systems.

Keywords: Payment Card Industry Data Security Standards, Costs, Hotels

A Financial Analysis of Payment Card Industry Compliance Journey of a Hotel: A Case Study

Introduction

Nowadays hotels have to operate in a very competitive fast–changing environment with constantly increasing roles of technology (Verma, Victorino, Karniouchina and Feickert, 2007). Payment card transactions have become an essential part of hotels operations (Cobanoglu, 2008b). In our contemporary age, it is hard to imagine a hotel that can successfully operate and compete on the market without accepting credit cards (Haley and Connolly, 2008). However, the convenience of cashless payments introduces the potential for issues such as private information vulnerability and security breaches because of data stored in credit cards. To help all companies address these problems, Payment Card Industry Data Security Standards (PCI DSS), was developed by major credit card issuing companies: Visa, MasterCard, American Express, Discover, and the JCB. The current PCI DSS version 1.2 requires that all companies accepting payment cards to be PCI-compliant (Cobanoglu, 2008a). However, since PCI compliance is not established by law, many companies still fail to comply. Even though PCI compliance does not provide 100% guarantee from data breaches, failure to comply provides more opportunity for hackers to commit fraud and steal sensitive information. The hotel industry is a very attractive market for hackers to attack because it involves large amounts of money, relaxed guests, or busy businessmen who often do not pay enough attention to their credit cards security. In the United States more than 55% of credit card fraud comes from the hospitality industry (Haley and Connolly, 2008). This provides strong evidence that hospitality companies need to comply and keep an eye on the latest changes of PCI DSS requirements and invest in compliance; otherwise the cost of PCI non-compliance could turn out to be even higher.

The purpose of this study is to explore the procedure, approximate the cost, and describe the real-life hotel experience of becoming PCI-compliant in order to provide guidelines and approximate expenses for recently opened hotels and for existing ones that are not PCI-compliant.

Review of Literature

Understanding PCI DSS

PCI DSS stands for Payment Card Industry Data Security Standards (www.pcicomplianceguide.org). This is a set of rules that introduces the requirements for all companies that accept credit cards (Connolly & Haley, 2008). Today, in order for a company to conduct credit card transactions, they should be in compliance with PCI standards. With the growing volume of payment card transactions, security issues have become more and more important. The idea itself is not new: Hobson and Ko (1995) developed ten recommendations "to reduce hotels' chances of becoming a 'point of compromise'" (p.53), among them:

1. Avoid 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 other agencies to prevent counterfeiting.

Later, the 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 (Payment card industry, 2009). The first set of requirements introduced as PCI DSS 1.0 appeared in December2004. Two more versions have followed since the initial one: PCI DSS 1.1 was released in September 2006, PCI DSS 1.2 was released in October 2008 ("Version 1.2", 2008). Each version was designed to detail the safeguards and enhance the understanding of PCI-compliance (Cobanoglu, 2008a).

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

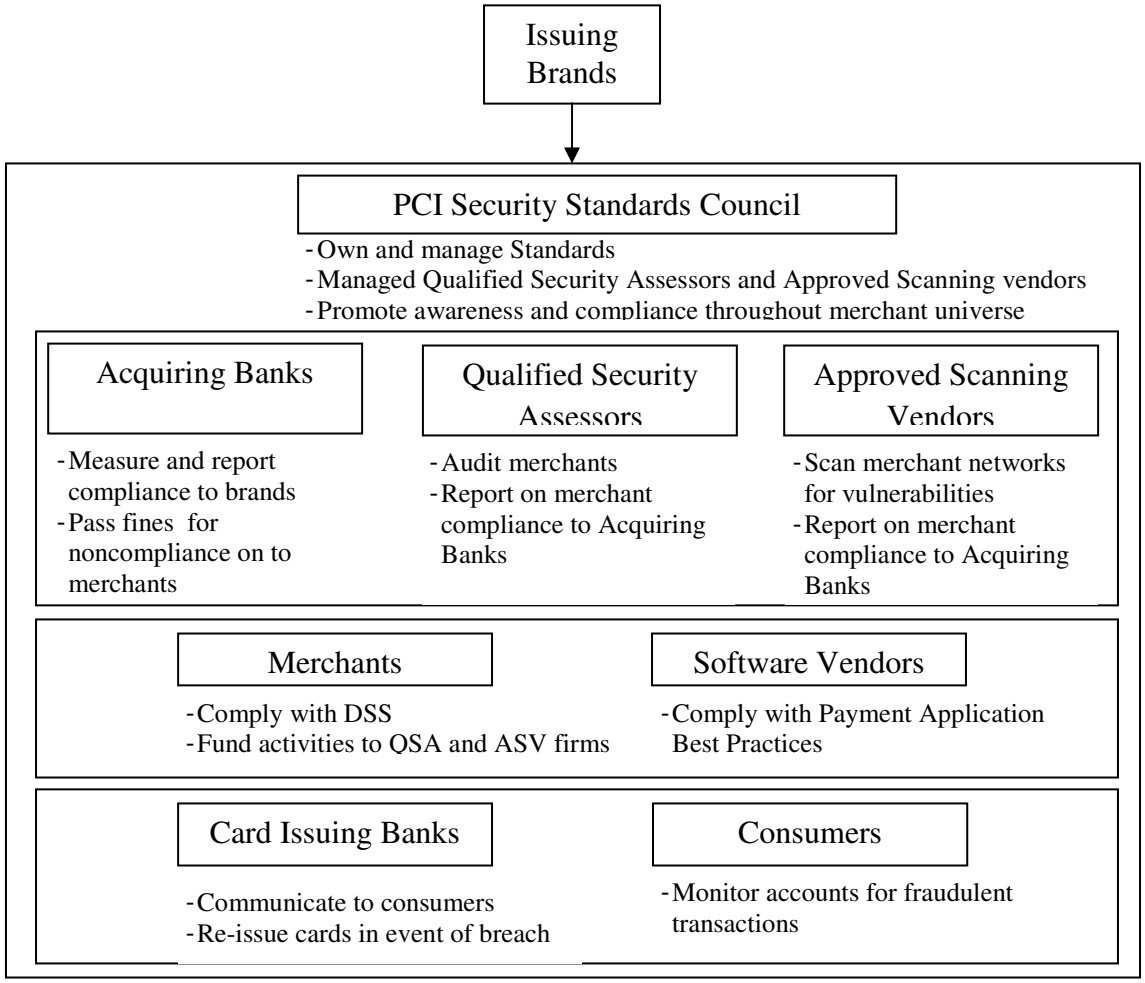

Figure 1. The payment Card Industry (PCI) Value Chain
Resource: Haley and Connolly, 2008, p. 15

The current version of PCI DSS is targeting several goals, such as building and maintaining a secure network, protecting cardholder data, maintaining a vulnerability management program, implementing strong access control measures, regularly monitoring and testing networks, and maintaining an information security policy ("About the PCI", 2009). The requirements of PCI DSS 1.2 are presented in the Table 1.

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

Table 1. PCI Data Security Standard Requirements
Resource: Getting Started with PCI, 2008

To become PCI-compliant a company is required to follow a particular procedure and must meet the requirements indicated above ("Compliance validation details", 2009). All companies that accept credit card payments from their customers are divided into several groups (merchant levels) according to the number of their credit card transactions per year. Merchant criteria and respective PCI validation requirements are shown in the Table 2.

Level/ Tier	Merchant Criteria	Validation Requirement
1	Merchants processing over 6 million Visa transactions 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

Table 2. Merchant levels and compliance validation requirements
Resource: Compliance validation details, 2009

Even though PCI-compliance is not mandatory by law now, there are some guidelines and key dates that are required to be met (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 this year Visa will require level 1 and 2 merchants not to retain sensitive card information (Lorden, 2009).

PCI DSS and the hospitality industry

PCI compliance has become a very important part of the hospitality industry's operations (Cobanoglu, 2007; Levin & Hudak, 2009; Tenczar, 2008; Volpe, 2009;). Hotels implement numerous "inside" and "outside" systems that are necessary for efficient operations (Haley & Connolly, 2008, p. 23). These systems may include, but are not limited

to Property Management System (PMS), Point of Sale (POS), Sales & catering, golf, spa, electronic locks, accounting, central reservation system (CRS), website booking engine, etc.

Due to a complexity of all the systems implemented in the hotels, it is very important to know which of these are using payment card information in order to protect it and ensure guest security. Hoteliers should also check with vendors if the applications they provide are certified and PCI-compliant. Being very attractive for hackers, hotels can reduce vulnerability if they follow PCI DSS requirements.

- The hospitality industry actually provides rich targets (Levin & Hudak, 2009) for identity thieves. A lot of information breaches have occurred in the hospitality industry, for example, in Radisson Hotel (Radisson Hotels & Resorts, 2009) and Wyndham Hotels and Resorts (McMillan, 2009).

Cost of PCI compliance

According to the Gartner Group's research conducted in 2008, PCI DSS 1.1 compliance requires an investment of about $2.7 million in remediation costs and another direct cost of $237,000 for outside assessors and related expenses from Level 1 merchants (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.

	Level 1	**Level 2**	**Level 3**
Assessment	$237,000	$135,000	$30,000
Remediation	$2,700,000.00	$1,100,000	$155,000
Total	$2,937,000	$1,235,000	$185,000

Table 3. Approximate investments in PCI compliance
Resource: Crawford, 2009

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

CISP Validation Category (Visa transactions / year)	Population	Estimated % of Visa Transactions	PCI DSS Compliance Validated***	Initial Validation Submitted / Remediating	Initial Validation In Progress	Pending Commitment
Level 1 Merchants (> 6M)	362	50%	91%	9%	0%	0%
Level 2 Merchants[2] (1 – 6M)	702	13%	87%	11%	2%	0%
Level 3 Merchants (e-commerce only 20,000 – 1M)	2627	< 5%	57%	19%	23%	1%

1 - Validation statistics are based on merchant compliance reporting provided by acquirers.

2 – Excludes 272 Level 2 merchants identified in 2007 that were required to validate compliance by 12/31/08.

It is worth noting that 99% of Level 1 and 2 merchants confirmed that they do not store prohibited data. Acquirers of Level 1 and 2 merchants that continue to store prohibited data are subject to monthly fines.

Table 4. PCI DSS Compliance Validation as of 12/31/2008

Resource: Visa Inc. Cardholder Information Security Program (CISP)

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 (Haley & Conolly, 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 on average between $90 and $300 per record breached (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 fines structure ranges from $5,000 to $25,000 per month. American Express' fine structure starts at $50,000 and goes up. So, cumulative costs for being non-compliant can be really high.

Methodology and Data Collection

A questionnaire instrument was developed based on the actual Payment Card Industry Data Security Standards version 1.2. The instrument contained questions about elements necessary for PCI-compliance and approximate range of investments. These elements were derived from 12 main PCI DSS requirements ("About the PCI", 2009).

Several hotels were contacted to participate in this study. Since the study included the disclosure of financial information, all but one hotel declined to participate in the study. Only one hotel located in the Northeast part of the U.S. agreed to participate in this study. This is a limited-service, 120-room hotel; a major brand franchisee that is operated by a management company. The data was collected through a structured interview with the general manager of the hotel by the researchers. The conversation was audio taped with the permission of the interviewee for future analysis and later transcribed manually. The interview took about 90 minutes in total. The general manager was selected as the interviewee for this study as the ultimate responsible person for ensuring that the hotel is PCI compliant; in the case of a breach, general managers are held liable. However, general manager consulted with other managers to answer some questions. A case study method was used for analyzing data for this research. The case study method is a widely used and is the accepted research method in the field of hospitality information technology (IT) (Cho, 1996; Connolly, 1999).

Findings

The hotel chosen for this case study is fully compliant with PCI requirements. This hotel's management cannot make any decisions about main systems to be implemented in the hotel (e.g. PMS, POS) and also cannot undertake any market research to support these decisions due to strict franchise requirements. Such decisions are made at the corporate level, and all hotels under the brand are required to follow them.

The next section will list the compliance process that the hotel went through for each of the PCI DSS requirements ("About the PCI", 2009).

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Firewall was installed on all the workstations in the hotel. The general manager of the hotel emphasized that firewall is necessary for the hotel's every-day operations and security; it is not just PCI DSS requirement. Moreover, firewall is included in the PMS and POS systems that are required by the franchising company to be installed in all the hotel chains. Consequently, it can be mentioned as a necessary element for PCI compliance, however, its cost cannot be counted toward PCI-compliance expense, because every hotel needs it regardless of whether they are compliant or not. Also, as a part of the first requirement, the hotel obtained a data flow diagram that describes the payment card data flow; for example, from the POS system in the restaurant, to the corporate office, and then to the bank. This diagram is essential for establishing credit card information security at a hotel: it is necessary to know how the information travels through the network in order to protect it. Requirement 1 also prescribes to prohibit direct public access between the Internet and any system component in the cardholder data environment. To comply with this rule, two networks were established in the hotel: one for the hotel's guests and another for the hotel's internal use. This required an additional investment of $5,000 to buy a new

server and it also causes an extra charge of $1,500 per month for the second network bandwidth, which is a T-1 connection (1.5 mega bit per second).

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

The vendor supplied defaults for system passwords and other security parameters were changed immediately upon initial installation by the IT manager. This will prevent hackers from accessing the hotel's systems by guessing well-known default usernames and passwords. The hotel also changed encryption keys from the default at installation, and they are changed anytime an employee with knowledge of the keys leaves the company or changes positions. In addition, the hotel changes default passwords/passphrases on access points. This particular requirement does not need any additional investment from the hotel.

Requirement 3: Protect stored cardholder data.

To comply with this requirement the hotel tries to keep cardholder data storage to a minimum. For example, credit card information is not available in a guest's folio. Under PCI guidelines, the hotel does not have access to full credit card information once it is submitted to the Central Reservation System. When the guest calls the hotel directly to make a reservation, the hotel must ask for the credit card number again. Guests expect that the hotel will keep the credit card in storage so that they are not asked again. It is interesting to note that some guests become irritated by this policy because the hotel is sacrificing the guest's convenience for security.

Requirement 4: Encrypt transmission of cardholder data across open, public networks.

All data transmissions across open, public networks in the hotel are encrypted for security purposes. The open and public networks used in this hotel include the Internet and Wireless technologies. The Internet pages that transmit cardholder data use Secure Socket Layer (SSL) protection which is a cryptographic protocol that provides security for communications over networks. The hotels verify that HTTPS appears as a part of the

browser's Universal Record Locator (URL) for the hotel's reservation website (franchisor's central reservation website) and no cardholder data is required when HTTPS does not appear in the URL.

Requirement 5: Use and regularly update anti-virus software.

Anti-virus software as a firewall is included in PMS/POS packages and is required by the franchisor company to be installed in all chain hotels. Now the hotel can obtain current, actively running, and regularly updated anti-virus software. Its cost is included in the price of the PMS/POS systems. In addition, anti-virus software is installed in all personal computers and laptops in the hotel.

Requirement 6: Develop and maintain secure systems and applications.

While the hotel's PMS was PCI compliant when the hotel started its PCI compliance journey, the POS system was not PCI compliant, because it lacked encryption capability of credit cardholder data. Normally, the POS vendor does not provide a patch to make its system PCI compliant. The franchisor's IT department provides the patch for a onetime investment of $15,000 to upgrade the POS system in order to be PCI compliant. If the hotel had not been a part of this franchisor, it would have needed to purchase a new POS system that would cost significantly much more money. The general manager mentioned the benefit of the franchisor in dealing with PCI compliance issues several times.

Requirement 7: Restrict access to cardholder data by business need-to-know.

In accordance with this principle, only two people in the hotel have access to cardholders' information on a business need-to-know basis. For example, even the general manager of the hotel does not have access to this information because he does not need it to perform his every-day duties. Front desk mangers also cannot see it; they can check only the last four digits of the credit card number that is shown in the guest folios. The cardholder information that is on paper is kept in a secure room where only one person can have access.

Requirement 8: Assign a unique ID to each person with computer access.

Every employee in the hotel has a unique ID and password to access the network. These passwords are required to be of at least eight characters in length and consist of alpha-numeric characters. The passwords must be changed every 60 days; general PCI DSS requirements require that a password must be changed at least every 90 days. It may be concluded that the hotel participating in this study is even more cautious about PCI DSS compliance. All ID and password combinations of the employees who left the company are erased within 15 days of the last day. This standard does not impose any cost, but requires following the procedure very carefully.

Requirement 9: Restrict physical access to cardholder data.

This requirement refers to limiting physical access to all information storage areas. Here we can mention employees' awareness of this rule. The hotel has a policy that prohibits the staff to speak out guest names and room numbers together to ensure safety and security. For these purposes, regular training meetings are required in the hotel. As it was explained by the general manager, there is no necessity to develop any learning material for these trainings because plenty of information is available from the web sites of American Hotel & Lodging Association (AH&LA), National Restaurant Association (NRA), PCI Council, and the credit card companies. So, these trainings do not impose any additional development or personnel costs for the hotel. Normally restaurant managers perform training for restaurant employees and front office managers lead meetings for front office staff. These two areas of the hotel operations are the most important because it is here that employees have direct contact with customers. The training lasts for about two hours and takes place at least once a month. The main purposes of the meetings are to keep employees updated and remind them about the main procedures established in the hotel.

The hotel has a big challenge with this requirement in the Sales and Catering department, as the credit card number of the guest is often written on the Banquet Event Order (BEO), many weeks or months before the event. Since the credit card number of the guest is physically written on the BEO, normally, it should be kept locked where no other

employees have access. However, the hotel management informed researchers that BEOs are often faxed by hotel guests to the hotel's general fax number. During the weekends, these BEOs can sit in the fax machine for days, making the guest's credit card information vulnerable. The hotel signed up with electronic fax service with efax.com to prevent this from happening. However, an inspection of the BEO template revealed that the general fax number of the hotel is listed on the BEO. Obviously, the guests will fax the signed BEO with credit card information to the number listed.

An inspection of the sales manager's desk revealed that there were several BEOs with guest credit card numbers available on her desk, again making them vulnerable. The hotel's sales and catering system does not have a field for credit card numbers, therefore, this forces the sales team to keep the credit card numbers on physical paper. After the event is finished, the sales team is supposed to mark out the credit card numbers on BEOs; however, this is hardly done.

The last three requirements mainly cover testing and monitoring procedures; they take place when PCI-compliance has already been established in the hotel.

Requirement 10: Track and monitor all access to network resources and cardholder data.

As each user has a unique username and password and each system requires a login, access to cardholder data systems is logged. Since the network for guest Internet access and hotel systems are separate, there is no need to log guest access to guest network.

Requirement 11: Regularly test security systems and processes.

The hotel's management company conducts an annual audit that involves the IT and network systems. In addition, the hotel uses an intrusion-detection system. All traffic in the cardholder data environment is monitored.

Requirement 12: Maintain a policy that addresses information security.

The hotel has access to a security policy that is established and disseminated by the franchisor. This policy addresses the 12 requirements of PCI DSS requirements. The franchisor also sends updates to the general manager when there is a change to this document. The hotel visits this policy periodically.

Conclusions and Recommendations

As a result of this case study we found the different areas that the hotel needs to work on and invest in, in order to achieve PCI-compliance. To better understand the cost of PCI-compliance we need to look at some elements in a budget structure for a franchise hotel:

- IT budget – about 0.5% of total revenues,
- Sales and marketing – about 3.5% of total revenues,
- Utilities – about 7% of total revenues,
- Franchisee fees – about 8.5% of total revenues.

PCI-compliance charges would most probably fall into the category of IT budget. However, these expenses include not only PCI costs, but also the cost of running all the PCs in the hotel, paper, supplies, ink, etc. But at the same time, there are some indirect costs that will not fall into the IT budget category, but are still related to PCI DSS compliance. We can find some examples under franchisee fees. Franchisor company fees are based on two variables: number of rooms and number of reservations – they normally end up at about 8.5%. These fees include charges for using the reservation system, the franchisor company rewards system, different franchisor company technologies, the yield management system, etc. For example, costs of using secure PMS, POS, and reservation systems are embedded here. And moreover, as it was mentioned above, prices for anti-virus and firewall are included in the cost of PMS/POS systems, which means that they are also hidden into franchisee fees. In this case the hotel is not paying for PCI directly, but paying for the

privilege of being a franchisee and using all the services associated with it. For these reasons, it is not easy to calculate the definite costs of being PCI Compliant for a hotel.

As a result of this case study we determined the key elements every hotel is required to invest in to become PCI compliant; among them secure PMS/POS systems with firewalls and anti-virus software, and protected Internet networks. There are also some particular procedures (e.g. changing passwords, limiting access to the cardholders' information, etc.) that a hotel needs to follow: necessary training for employees and potentially monitoring and controlling systems.

The Sales and Catering department of the hotel was found to be the most vulnerable department in the hotel for guest credit card information. Credit card numbers of most guests are written on Banquet Even Orders, going from one hand to another. The hotels should invest in a PCI compliant sales and catering system for securing credit card numbers for sales and catering events.

Considering the example of this chain hotel, we can note that the PCI-compliance process is not very complicated and investment-demanding. The main advantage of being a franchise hotel in this sense is that all necessary research will be done at the parent corporate level and a hotel will need just to implement those requirements identified by the corporate office. We also can say that there is no exact cost of making a hotel PCI-compliant. In many cases, PCI DSS requirements describe general rules for a hotel's well-being and common sense practices to stay in business.

One of the limiting factors for this paper was the sample size used for the study. Even though we can assess some results and understand the PCI compliance process for hotels, a larger population would provide more reliable results.

To improve this research in order to strengthen the results, researchers could also conduct the analogous study at the corporate level of chain hotels and involve independent hotels as well. Those would be studies that demonstrate the decision-making and PCI-compliance process in more detail. For example, the authors can suggest that a new hotel

willing to become PCI-compliant, will need to conduct research in this area, and may need to hire a consultant to explore vendors' market, choose PMS/POS system, and buy them. Of course, all of these will lead to additional charges for the hotel.

The results of this study indicate that hotels should focus in four core areas to reduce the risk of an information technology breach. These four areas consist of:

a) The use of firewalls in each networked workstation, regardless of processing or storing cardholder data. A firewall is a part of a computer system or network that is designed to block unauthorized access while permitting authorized communications. It is a device or set of devices that is configured to permit or deny computer applications based upon a set of rules and other criteria.

b) Restrict remote access privileges: Each networked workstation comes with a potential to be accessed remotely. This can be very useful in getting technical support or patches from the corporate office or vendor. However, the workstations should be closed to remote access. Whenever there is a need, the workstation may be allowed to be accessed remotely. Right after receiving the service, support or patch, the remote access feature should be disabled.

c) Change vendor-provided username and passwords: This is a very simple but yet very useful technique. Each computer system such as PMS or POS system comes with a default user name and password which is known publicly. The users of the system should change this to something else (obeying the company policy for username and passwords) at installation. This will ensure that if hackers access the company systems, they would not be able to login into the systems with these well known default user names and passwords.

d) Use of anti-virus software: Each workstation should have anti-virus software. Every day, the virus definition files must be downloaded. This way, the anti-virus software will protect the workstation from the newest viruses.

The four steps explained above will not be a large expense for hotels; however, they will reduce the risk of breaches significantly. Research has shown that credit card breaches in a hotel reduce the overall satisfaction level, likelihood of recommending the hotel to family and friends, and the likelihood of coming back to that hotel (Berezina, 2010). It is also a known fact that a breach will cost a hotel a lot of money in financial penalties and increased commissions. For these reasons, it makes perfect sense for hotels to obtain PCI DSS compliance.

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

Berezina, E. (2010). An impact of information security breach on hotel guests' perception of service quality, satisfaction, word-of-mouth and revisit intentions. Unpublished Thesis. University of Delaware.

Cobanoglu, C. (2007). PCI what? *Hospitality Technology*. Retrieved 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. *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/dirmod.asp?sid=783D4AA2541D483C98659D20A3539C6E&nm=&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=3E1967433073 4FF1BBDA3D67B50C82F1&tier=4&id=7DF7AC1459464A4BBC32B818E75A57F6.

Cho, W. (1996). A case study: Creating and sustaining competitive advantage through an information technology application in the lodging industry. Unpublished doctoral dissertation, Virginia Polytechnic Institute and State University.

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

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. (1999). Understanding Information Technology Investment Decision-Making in the Context of Hotel Global Distribution Systems: A Multiple-Case Study. Unpublished doctoraldissertation, Virginia Polytechnic Institute and State University. URL: http://scholar.lib.vt.edu/theses/available/etd-113099-200845/

Connolly, D.J., & Haley M.G. PCI DSS compliance: just whose responsibility is it? (2008). *Hospitality Technology*. Retrieved from http://www.htmagazine.com/ME2/dirmod.asp?sid=8D86DF469BD74C098382D9532C904D8E&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

Getting Started with PCI Data Security Standard. (2008). PCI Security Standards Council LLC. Retrieved on 06/02/2009 from https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf

Haley , M., & Connolly, D. J. (2008). *The PCI compliance process for hotels*. American Hotel & Lodging Association. Retrieved December 19, 2009, from https://ms2.nss.udel.edu/wm/mail/window.html?sessionid=-6c4b0ca17.

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

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

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

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

Payment card industry – PCI – compliance. (2009). Retrieved on 06/03/2009 from http://www.solidcactus.com/pci.html

PCI compliance process for hotels. (2008). American Hotel & Lodging Association.

PCI DSS Compliance Validation as of 12/31/2008. (2009). Visa Inc. Cardholder Information Security Program (CISP)

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

Tenczar, J. PCI Sharpens its Teeth: Are You Ready? (2008). Hospitality Technology. Retrieved from http://www.htmagazine.com/ME2/Sites/dirmod.asp?sid=&nm=&type=MultiPublishing&

mod=PublishingTitles&mid=3E19674330734FF1BBDA3D67B50C82F1&tier=4&id=1A833
3A1BA3E428B90E9BED3550176B7&SiteID=AAED287C668148CCB10E4FBA73326A07

Verma, R., Victorino, L., Karniouchina, K., & Feickert, J. (2007). Segmenting hotel customers based on the technology readiness index. *Cornell Hospitality Report*, September 2007, 4 – 13

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

Volpe, C. Is PCI enough? (2009). *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

Warner, B. (2008).Best Western and the worst kind of security mix-up. *Times Online*, August 27. Retrieved from http://technology.timesonline.co.uk/tol/news/tech_and_web/the_web/article4621021.ece