Payment Card Industry Data Security Standards (PCI DSS) Compliance in Restaurants

Payment Card Industry Data Security Standards (PIC DSS) Compliance in Restaurants

AUTHORS

Kutay Kalkan
Graduate Student

Francis Kwansa
Associate Professor

and

Cihan Cobanoglu
Associate Professor
University Of Delaware

Payment Card Industry Data Security Standards (PCI DSS) Compliance in Restaurants

Abstract

In order to improve the security of customer data, the credit card companies have come together to create a security standard, called Payment Card Industry Data Security Standard (PCI DSS), which involve mandatory requirements for merchants that accept credit card transactions. All restaurants that accept a credit card must comply with PCI DSS. The purpose of the study was to examine the PCI DSS compliance levels of Quick Service, Casual/Family and Fine Dining restaurants. A random sample of 1000 restaurant managers that are in charge of information technology at their companies and are subscribers of *Hospitality Technology* Magazine were surveyed. One hundred ninety managers responded to the survey. The results indicate that restaurants are far from full compliance with PCI DSS. This may have significant financial and non-financial consequences for restaurant owners and operators.

Keywords: Restaurants, Computer Security, Network, Information Technology, PCI DSS

INTRODUCTION

Consumers are concerned about the security of their personal information when using their credit cards to purchase goods and services. In the U.S., about 75 percent of households have at least one credit card (creditcard.com). Javelin Survey and Research Company released the findings of the 2007 Identity Fraud Survey, which found that 8.4 million people in the U.S. have been the target of identity theft. The monetary loss was $49.3 billion or an average of $5,720 per victim. Additionally, it took an average of 25 hours to resolve the issue for each victim.

In order to improve the security of customer data, the credit card companies have come together to create a security standard, called Payment Card Industry - Data Security Standard (PCI DSS), which involve mandatory requirements for merchants that use credit card transactions. As of June 30, 2007, all businesses that process credit card transactions are required to have achieved PCI compliance ("PCI Compliance Deadline", 2006). However, most U.S. restaurants are still not fully compliant with PCI DSS.

The purpose of the study was to examine the compliance levels of Quick Service (QSR), Casual/Family and Fine Dining restaurants. An on-line research survey method was employed and the results are expected to assist security-sensitive customers in their choice of restaurant type to patronize. The research questions were:

1) What is the level of PCI DSS compliance of restaurants?
2) Are there significant differences in the PCI DSS compliance levels of restaurants based on restaurant type (Quick Service Restaurant, Casual/Family Restaurants, Fine Dining Restaurants)?

Growth of Credit Card Transactions

Over the years representations of value have become more and more abstract, evolving from barter through bank notes, payment orders, checks, credit cards, and now electronic payment systems (Asokan, Janson, Phillippe, Steiner, & Waidner, 1997, p. 28). Research by Rysman (2007) showed that the percentage of transactions conducted with payment cards has increased from 12.4% (1994) to 28.9% (2001). Furthermore, according to the American Bankers Association, use of cash fell from 39% in 1999 to 32% in 2003. Checks now account for just 15% of all store purchases while use of debit cards has risen to 31% of all purchases, up from 21% four years ago.

"The advantages of electronic transactions - swift, reliable, and silent - over clunky checks and bulky cash are apparent to consumers" (Epstein and Brown, 2006). What is more, they are mobile and easy to use. However, just like other electronic technologies, the major drawbacks of using payment cards are privacy and security of the cardholder's personal information.

With the universal access of the Internet, credit card holders' personal information has become especially easier for professionals to obtain. Identity thieves use personal information such as names, social security numbers, and birth dates to commit fraud and other white collar crimes in someone else's name (Albany Law Review, 2004). Hackers "phish" for security breaches of data files to break in and steal personal information of customers that use credit cards for the payment of goods and services. Moreover, digital documents can be copied perfectly, often without a trace to the hacker, which further increases the vulnerability of these data. Once digital signatures are produced anybody who knows the secret cryptographic key can gain access

to buyers' personal information that is associated with each credit card transaction (Asokan et al., 1997, p. 28). Hoffman and Novak (1999) stated that almost 95% of Web users have declined to provide personal information to Web sites at one time or another when asked.

Payment Card Industry Security Standards Council

The threats identified above have left customers with serious concerns about their information security. Consumers today want and need absolute assurance from businesses that their financial and personal information are safe (Kalogeris, 2005). American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International came together to form the PCI Security Standards Council with a mission to enhance payment account data security by fostering broad adoption of the PCI Security Standards. According to the Council, PCI DSS is multifaceted and includes requirements for security management, policies, procedures, network architecture, software design and other critical protective measures.

PCI DSS originally began as five different programs: Visa Card Information Security Program, MasterCard Site Data Protection, American Express Data Security Operating Policy, Discover Information and Compliance, and the JCB Data Security Program. Each credit card company's intentions was similar: to create an additional level of protection for customers by ensuring that merchants meet minimum levels of security when they store, process and transmit cardholder data. The Payment Card Industry Security Standards Council was formed in December 2004, and the credit card companies aligned their individual policies and created the Payment Card Industry Data Security Standards. In September 2006, the PCI standard was updated to version 1.1 to provide clarification and minor revisions to version 1.0.

In October 2007, Visa International announced new Payment Applications Security Mandates "that are designed to help companies comply with PCI." Visa required these mandates to be implemented by 2010 calling for "new merchants that want to be authorized for payment card transactions will have to be using only Payment Application Best Practice - validated applications." These new mandates were designed to help companies achieve Payment Application Best Practice (www.visa.com/PABP) compliance, an implementation of PCI DSS in vendor software.

REVIEW OF LITERATURE

Payment Card Industry Data Security Standards (PCI DSS)

As specified in the PCI DSS guidelines, merchants are categorized according to the volume of transactions processed annually and the potential risk and exposure they introduce into the payment system. Each merchant classification has been charged with different levels of compliance tasks. The following is the list of the merchant levels along with their compliance tasks (“Compliance Validation,” n.d.).

Merchant Level 1

Defined as:

- Any merchant-regardless of acceptance channel-processing over 6,000,000 Visa e-commerce transactions per year (approximately 16,348 per day).
- Any merchant that has suffered a hack or an attack that resulted in an account data compromise.
- Any merchant that Visa, at its sole discretion, determines should meet the Level 1 merchant requirements to minimize the risk to the Visa network.

- Any merchant identified by any other payment card brand as Level 1.

Merchant Level 1 Compliance Tasks

- Annual On-site PCI Data Security Assessment (performed by CISP authorized external vendor)
- Quarterly Network Scan (performed by CISP authorized external vendor)

Merchant Level 2
Defined As:

- Any merchant processing 150,000 to 6,000,000 Visa e-commerce transactions per year (approximately 411 - 16,438 per day).

Merchant Level 2 Compliance Tasks

- Annual Self-Assessment Questionnaire
- Quarterly Network Scan (performed by CISP authorized external vendor)

Merchant Level 3
Defined As:

- Any merchant processing 20,000 to 150,000 Visa e-commerce transactions per Year (approximately 55 - 411 per day).

Merchant Level 3 Compliance Tasks (same as a merchant level2)

- Annual Self-Assessment Questionnaire
- Quarterly Network Scan (performed by CISP authorized external vendor)

Merchant Level 4
Defined As:

- Any merchant processing fewer than 20,000 Visa e-commerce transactions per year (less than 55 per day).

Merchant Level 4 Compliance Tasks

- Annual Self-Assessment Questionnaire (recommended but not mandatory)
- Quarterly Network Scan (recommended but not mandatory)

To comply with PCI DSS, a merchant should meet the following requirements (PCI DSS version 1.1):

1. Build and Maintain a Secure Network
    a. Install and maintain a firewall configuration to protect data
    b. Do not use vendor-supplied defaults for system passwords and other security parameters
2. Protect Cardholder Data
    a. Protect stored data
    b. Encrypt transmission of cardholder data and sensitive information across public networks
3. Maintain a Vulnerability Management Program
    a. Use and regularly update anti-virus software
    b. Develop and maintain secure systems and applications
4. Implement Strong Access Control Measures
    a. Restrict access to data by business need-to-know
    b. Assign a unique ID to each person with computer access
    c. Restrict physical access to cardholder data
5. Regularly Monitor and Test Networks
    a. Track and monitor all access to network resources and cardholder data

b. Regularly test security systems and processes

6. Maintain an Information Security Policy

a. Maintain a policy that addresses information security

However, the cost and complexity of establishing PCI DSS-compliant transaction architecture is challenging. “The time required by retailers to establish total end-to-end compliance on their own, compounded with the time and expense of PCI DSS audits by third-party security certification companies, build a compelling case for working with vendors and service providers who can make the job easier” (PCI Compliance, 2007).

While some companies develop, deploy, assess and test a compliance strategy on their own, others find that there are certain advantages of using a third-party vendor for these activities. For some organizations, an outside vendor can provide external validation of the appropriateness of the processes and policies. This action provides reassurance to customers, partners, shareholders and card issuers. Most importantly, a third-party vendor can also provide an objective analysis of current compliance status and gives recommendations for closing any gaps (Profiting from PCI Compliance, 2007).

When compliance validation is not outsourced, company officials become fully liable for any omissions or errors. Using a third-party vendor helps to spread the risk carried by corporate management. However, companies have the chance to conduct their own penetration testing if they prefer. Nevertheless, external network scans are required for the majority of merchants and service providers, and these scans must be performed by an approved third-party assessor. When companies reach a certain number of payment card transactions, a certified PCI assessor must validate PCI compliance. The PCI Security Standards Council manages a Qualified Security

Assessor (QSA) program in order to ensure that assessors are fully certified to conduct PCI assessments.

Compliance in Restaurants

Restaurants are vulnerable to security attacks simply because about 80 percent of credit-card data breaches are tied to cash-registers and other POS terminals majority of which are found in restaurants (Clark, 2007). Again, it is estimated that losses which are caused by credit card skimming has become a worldwide problem with losses exceeding $1 billion a year.

As a consequence, companies that process card transactions are increasing the pressure on restaurants, threatening to cut off service, along with fines, to those who are not complying with their security rules (Sidel, 2007). The minimum fine for data loss is $500,000 for retailers who are dealing directly with the card companies (Gentry, 2007). On the other hand, fines start at $50,000 for non-compliance without data loss. Furthermore, if cardholder data is stolen in mass quantities, the retailer will be required to pay a reissue fee of as much as $200 per card.

For instance, the credit card processing system of Atlanta Bread Co. restaurant in Kansas City, was compromised by a hacker at a cost of over $25,000 (Stagemeyer, 2007). The restaurant was threatened with fines of up to $1 million and had $16,000 withdrawn from their bank account without notice. This prohibited them from buying inventory for a period of time and then they had to spend $7000 to upgrade their POS system.

Another example is Chipotle Mexican Grill. Prior to August 2004, the company experienced nearly 2,000 incidents of customers' credit card theft resulting in $1.4 million of fraudulent charges for which the restaurant chain became responsible. For this reason, they had to pay $4 million to cover the following: reimbursement of the fraudulent charges, the cost of

replacing cards, monitoring expenses and fines imposed by Visa and MasterCard. Their 2005 annual report showed that the fines from Visa and MasterCard totaled $1.3 million.

In summary, a large number of restaurants do not comply with PCI DSS and about 60% of the security breaches come from restaurant industry, according to Sidel (2007). Similar data from Visa International suggests that 50% of incidents in which credit-card information was accessed illegally occurred in restaurants.

METHODOLOGY

In this study, a descriptive, online survey research design was employed. The sample consisted of 1000 randomly selected restaurant technology managers who are current subscribers of *Hospitality Technology* magazine as of November 2007. One hundred ninety two respondents completed the survey. Two surveys were not usable; therefore the final sample was 190 with a response rate of 19.0 percent. There were 57 respondents representing Quick Service restaurants, 87 representing Casual Dining restaurants, 32 representing Fine Dining restaurants and 14 representing other types of restaurants (i.e. Clubs). All of the sample members had an email address, therefore, only an online version of the survey was conducted.

A non-response analysis using wave analysis (early versus later respondents) was conducted to answer (1) whether non-respondents and respondents differed significantly, (2) whether equivalent data from those who did not respond would have significantly altered findings. 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. Therefore, an independent t-test was conducted to see if early respondents'

responses are different from late respondents'. The analysis indicated that there was no significant difference, concluding that this survey did not suffer from non-response bias.

The two research questions guiding this study again were:

1. What is the level of PCI DSS compliance of restaurants?
2. Are there significant differences in the PCI DSS compliance levels of restaurants based on restaurant type?

Dependent Variables

The PCI DSS contains 12 main standards that restaurants must meet and the online survey was created around these 12 standards to assess the level of restaurant compliance. Therefore the survey consisted of 12 general items which were measured by a five-point Likert-scaled items ranging from 1= "Not Compliant Yet" to 5="Fully Compliant". The survey items are as follows:

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
3. Protect stored cardholder data
4. Encrypt transmission of cardholder data across open, public networks
5. Use and regularly update anti-virus software
6. Develop and maintain secure systems and applications
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

10. Track and monitor all access to network resources and cardholder data
11. Regularly test security systems and processes
12. Maintain a policy that addresses information security for employees and contractors

Independent Variables

- Quick Service Restaurant
- Casual/Family Restaurant
- Fine Dining Restaurant
- Other (i.e. Clubs)

FINDINGS

The total number of units represented (that is the number of units each responding company owns, operates or franchises) is 204,565, of which 161,605 are quick service restaurants, 41,985 are casual/family restaurants, and 975 are fine dining restaurants. In terms of company type, 24% were national restaurant chain, 20% were independent restaurant company without franchised brand, 18% were regional restaurant chain, and 12% were global restaurant chain (See Table 1). This shows a balanced mix of restaurant companies.

PLEASE INSERT TABLE 1 HERE

In terms of respondents' job responsibility, only 32% of the respondents major job function was information technology management. Twenty percent were owner or operator, 15% were in corporate management, 11% were food and beverage managers, and 6% were financial managers (See Table 2). This data shows that majority of respondents were from a variety of managerial

positions in the restaurant companies.

PLEASE INSERT TABLE 2 HERE

In terms of annual revenue, 37.2% of the respondents reported yearly revenue less than $50 million, 9.4% reported $50 million to $99 million, 20.6% reported annual revenue of $100 million to $499 million, 7.8% reported annual revenue of $500 million to $1 billion, and 10% reported more than $1 billion. About 15% of the respondents preferred not to answer this question.

PLEASE INSERT TABLE 3 HERE

In response to the first research question, the survey contained 12 main requirements of PCI DSS and asked the respondents how compliant their companies were with each of the requirements (See Table 4). There were no restaurant companies that were fully compliant with all 12 requirements of the PCI DSS. The breakdown of each requirement is shown in Table 4 regardless of the restaurant type. Only 75.2% of the respondents have firewalls to protect cardholder data. There are still about 30% of restaurant companies using vendor supplied passwords (i.e. system/system or admin/admin). This could lead to serious security breach. Majority of the hackers hack into systems by using these very common vendor supplied username and passwords. Seventy-three percent of the respondents can protect cardholder data fully. It was surprising that there were still 18% of the respondents' companies that do not use anti-virus software. Anti-virus software is accepted as one of the fundamentals of computer

security and its implementation is rather simple and inexpensive. It was equally surprising that about 33% of the respondents do not assign unique IDs to their employees. Failing to assign unique user IDs to users makes it impossible to find the responsible party in case of a security breach or fraud. About 30% of the restaurants do not restrict physical access to cardholder data, which makes it easy for data to be stolen by disgruntled employees. Only 45% of the respondents test security systems and processes fully.

PLEASE INSERT TABLE 4 HERE

PCI DSS Compliance across Different Restaurant Types

In response to the second research question, a crosstab analysis of the compliance levels of PCI requirements with the type of restaurant was conducted. The results showed that fine-dining restaurants were the worst regarding compliance (See Table 5). Only 56.3% of the fine-dining restaurants fully implemented firewall configuration while 79.1% of casual/family restaurants and 75.6% of QSR fully implemented firewall configuration. Similarly, 18.8% of the fine-dining restaurants used vendor-supplied usernames and passwords for their systems while only 4.5% of the casual/family restaurants and 9.1% of QSR used vendor supplied login information. In terms of assigning a unique ID to each employee with computer access, only 59.1% of the QSR and 56.3% of fine dining restaurants were fully compliant. Casual/family restaurants were better with respect to this requirement (72.7% fully compliant).

PLEASE INSERT TABLE 5 HERE (ATTACHED AS A DIFFERENT FILE)

An analysis of variance was conducted on the PCI DSS compliance levels among the different restaurant types. In 5 of the 12 requirements significant differences were found across all restaurant types. These were: “Do not use vendor-supplied defaults for system passwords and other security parameters”, “Use and regularly update anti-virus software”, “Develop and maintain secure systems and applications”, “Restrict access to cardholder data by business need-to-know”, and “Restrict physical access to cardholder data.”

A Tukey post-hoc analysis was conducted to see the differences in restaurant types. With regard to all of the requirements for compliance, fine dining restaurants’ compliance level was significantly lower than QSRs and casual/family type restaurants. There were no significant difference between QSRs and casual/family type restaurants. This may be due to the fact that most of the fine-dining restaurants are independently owned and do not have the resources that QSRs and casual/fine dining restaurants have. Therefore, fine-dining restaurants are most vulnerable to hackers because they offer open doors even though they may not offer the credit card volume that some hackers may desire. However, this finding does not mean that QSRs and casual/family type restaurants are fully compliant with PCI DSS, they still lack full compliance which is a serious security risk.

Conclusions

PCI Compliance is the most important challenge that is facing the restaurant industry (Parker, 2009). This study only confirmed this statement. There are significant numbers of restaurants that are not PCI compliant. According to Leach (2009), there is no partial compliance in PCI, a company is either compliant or not. The results show that not even a single restaurant company is 100% compliant. This finding may have significant implications for the restaurant

industry. In the case of a credit card breach, restaurant companies may face hundreds of thousands of dollars in fines and expenses. In an industry where profit margins are between five to eight percent and failure rate is about 60% within the first five year's of operation (Cobanoglu & Erdem, 2009), non-compliance could bankrupt a restaurant company, especially in the case of small restaurants. In addition to fines, restaurants may face other tangible monetary losses when a breach occurs, including: lost business, increased cost of credit card transactions, replacement cost of credit cards to affected customers, and payment of credit protection service for affected customers (Navetta, 2009).In addition, there are non-financial consequences such as damaged reputation of the company and customer loyalty. PCI compliance does not guarantee that the business will not be breached (Leach, 2009), nonetheless, it reduces the risk significantly. Hackers usually will avoid hacking into a well protected computer network which PCI requirements aim to achieve. Instead, they will target business networks that are not well protected.

According to the data, QSR restaurants with less than 10 units are more compliant compared to the restaurants with higher number of units. One may speculate that small units have a limited scope which may be defined as the areas where confidential customer data are collected and kept. Therefore, controlling small areas may be relatively easier and cheaper to achieve. Similarly, as the size of the company increases, the scope increases too; which makes it more challenging to be PCI compliant. Some may logically think that as the number of units increase, a company should be more compliant because of the reputation and security issues. This study showed that this is not always the case. Based on the findings of this study, the following are recommended for restaurant owners and operators:

- scan their systems to understand where data is transmitted and stored.

- Use anti-virus software and regularly update the virus dictionary files
- Do not use vendor-provided passwords
- restrict access to credit card holder data
- use PCI compliance tools such as tokenization where possible
- use outsourcing companies to handle credit card transactions
- update their non-compliant systems such as Point of Sale systems
- use a consultant to evaluate PCI compliance of their companies

There is no doubt that all of these will cost money and resources to the restaurant company, however they will prevent big problems in the future. Future study may focus on the cost of non-PCI DSS compliance.

References

Albany Law Review. (2004). *Identity Theft Statutes: Which will Protect Americans the most?* (Issue Brief No. 4). New York: Catherine Pastrikos.

Asokan, N., Janson, Philippe A., Steiner, M., Waidner, M. (1997). The State of the Art in Electronic Payment Systems. *IEEE JNL, 30*(9), 28-35.

Clark, T. (2007). *Protecting Payments.* Retrieved November 26, 2007, from: http://www.htmagazine.com/HT/archive/1007/1007_04.html

Cobanoglu, C. & Erdem, M. (2009). 11th Annual Restaurant Technology Study: Driving Efficiency. Supplement to *Hospitality Technology, 13* (2)

Compliance Validation Details for Merchants. Retrieved November 26, 2007, from: http://www.usa.visa.com/merchants/risk_management/cisp_merchants.html?it=cl/merchants/risk_management/cisp.html|Defining%20Your%20Merchant%20Level#anchor_2

Epstein, R. A. and Brown, T. P., (2006). "The War on Plastic". *Regulation*, 29(3), pp12-16, Available at SSRN: http://ssrn.com/abstract=944870

Gentry, C. R. (2007, May). Hardening the targer: achieving PCI compliance is one step to network security. *Chain Store Age, 83(*5), 248.

Hoffman, D. L., Novak, T. P. (1999). Building ConTrust Online. *Communications of the ACM, 42*(4), 80-85.

Kalogeris, R. (2005, Fall). Are you S.A.F.E.? Secure Against Fraud Electronically. *Hospitality Upgrade*, 160.

Leach, T. (2009). Payment Card Industry Data Security Standards: From the Council's Perspective. *The Second Payment Card Industry Compliance in Hospitality Conference*, Houston, TX.

Navetta, D. (2009). Bridging the Communications Divide between IT, Risk, and Legal. *The Second Payment Card Industry Compliance in Hospitality Conference*, Houston, TX.

Parker, J. (2009). Lessons Learned in the Field, How to not Repeat them in the Future, The Operators' IT Viewpoint. *The Second Payment Card Industry Compliance in Hospitality Conference*, Houston, TX.

PCI Compliance Deadline Too Soon for Most (2006), retrieved on October 23, 2007 from http://www.itbusinessedge.com/item/?ci=20698

PCI Compliance: Low Risk, High Reward. (September, 2007). Retrieved November 26, 2007, from Hughes Networks Systems Web site: http://www.hughes.com/HUGHES/Doc/0/BIJENRGP3AT4JFJSEAUGLUJ7C1/PCI%20Compliance.H36659.09-24-07.pdf

Profiting from PCI Compliance. (September, 2007). Retrieved November 26, 2007, from IBM Corporation Web site: www-935.ibm.com/services/us/iss/pdf/**profiting**_from_**pci_compliance**_wp.pdf

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

Rysman, M. (2007). An Emprical Analysis of Payment Card Usage. *The Journal of Industrial Economics*, *55*(1), 4, 13.

Sidel, R. (2007). Card companies crack down on restaurants. *Wall Street Journal - Eastern Edition, 249*(69), B1-B2.

Stagemeyer, S. (2007). Fraud rings up a large ticket. Kansas City Business Journal. Retrieved from Kansas City Business Journal website: http://kansascity.bizjournals.com/kansascity/stories/2007/03/26/story3.html?b=1174881600^1436311

Table 1: Respondents' Company Type

	%
National restaurant chain	24.1
Independent restaurant management company without franchised brand	20.9
Regional restaurant chain	18.2
Global restaurant chain	12.3
Franchisor	10.2
Other	7.5
Independent restaurant management company with franchised brand	6.4
Club (i.e. Golf, Country)	0.5

Table 2: Job Function of Respondents

	%
Information systems/Technology Management	32.3
Owner/Operator	19.6
Corporate Management	15.3
Food/Beverage Management	11.1
Financial Management	6.3
Other (please specify)	5.3
Sales/Marketing Management	4.2
Operations/Property Management	3.7
Purchasing Management	2.1
Total	100

Table 3: Approximate Annual Revenue of Respondent Companies

	Percent
More than $1 billion	10
$500 million - $1 billion	7.8
$100 - $499 million	20.6
$50 - $99 million	9.4
Less than $50 million	37.2
I prefer not to answer	15

Total 100

Table 4: PCI DSS Compliance Levels of Respondent Companies

	Fully compliant (%)	Partially compliant (%)	Not compliant at all (%)	Mean*	St. Dev.
Install and maintain a firewall configuration to protect cardholder data	75.2	18.8	6	1.54	1.10
Do not use vendor-supplied defaults for system passwords and other security parameters	69.7	22.7	7.6	1.62	1.17
Protect stored cardholder data	73.5	21.2	5.3	1.48	1.02
Encrypt transmission of cardholder data across open, public networks	77.9	18.3	3.8	1.41	0.94
Use and regularly update anti-virus software	81.7	16.8	1.5	1.31	0.78
Develop and maintain secure systems and applications	65.6	32.8	1.5	1.53	0.91
Restrict access to cardholder data by business need-to-know	74.8	22.9	2.3	1.42	0.87
Assign a unique ID to each person with computer access	66.4	29.8	3.8	1.63	1.07
Restrict physical access to cardholder data	69.5	28.2	2.3	1.48	0.91
Track and monitor all access to network resources and cardholder data	53.4	40.5	6.1	1.84	1.16
Regularly test security systems and processes	45	45	10	2.11	1.29
Maintain a policy that addresses information security for employees and contractors	51.1	38.9	10	1.97	1.28

*: 1=Fully Compliant; 5=Not compliant at all.

PCI DSS Requirements	QSR Mean¥	SD	Casual/Family Mean¥	SD	Fine Dining Mean¥	SD	Other Mean¥	SD	F§	Sig.
Install and maintain a firewall configuration to protect cardholder data	1.56	1.14	1.43	1.00	2.00	1.41	1.40	0.89	1.17	0.324
Do not use vendor-supplied defaults for system passwords and other security parameters	1.70	1.29	1.42	0.92	2.31	1.58	1.40	0.89	2.78	0.044**
Protect stored cardholder data	1.55	1.15	1.39	0.90	1.75	1.13	1.40	0.89	0.63	0.600
Encrypt transmission of cardholder data across open, public networks	1.45	1.09	1.30	0.80	1.75	1.06	1.40	0.89	1.01	0.392
Use and regularly update anti-virus software	1.32	0.86	1.17	0.41	1.88	1.31	1.40	0.89	3.84	0.011 ***
Develop and maintain secure systems and applications	1.66	1.10	1.35	0.62	1.94	1.18	1.60	0.89	2.34	0.076*
Restrict access to cardholder data by business need-to-know	1.50	1.05	1.26	0.54	1.88	1.26	1.40	0.89	2.44	0.067*
Assign a unique ID to each person with computer access	1.75	1.12	1.52	1.01	1.81	1.22	1.40	0.89	0.67	0.575
Restrict physical access to cardholder data	1.59	1.02	1.29	0.65	2.06	1.29	1.20	0.45	3.80	0.012**
Track and monitor all access to network resources and cardholder data	1.98	1.36	1.67	1.01	2.31	1.20	1.40	0.55	1.85	0.142
Regularly test security systems and processes	2.11	1.37	2.05	1.26	2.44	1.36	1.80	0.84	0.49	0.691
Maintain a policy that addresses information security for employees and contractors	1.93	1.26	1.92	1.29	2.38	1.41	1.60	0.89	0.71	0.550

Table 5: ANOVA Analysis Table for PCI Requirements Across Restaurant Types

¥= 1=Fully compliant; 5=Not compliant at all §= F statistics (ANOVA)

*=Significant at .01 level **= Significant at .05 level ***=Significant at .001 level