

FACTORS INFLUENCING THE ADOPTION OF THE PAYMENT CARD INDUSTRY DATA SECURITY STANDARD

Barry Noonan

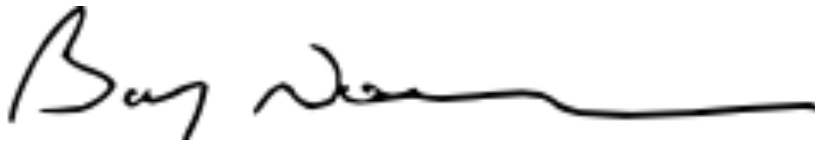
A dissertation submitted to the University of Dublin
in partial fulfilment of the requirements for the degree of
MSc Management of Information Systems

1st September 2015

Declaration

I declare that the work described in this dissertation is, except where otherwise stated, my own work and has not been submitted as an exercise at this or another institution. I further declare that the research has been carried out in compliance with the current ethical and research guidelines of the School of Computer Science and Statistics at Trinity College Dublin.

Signed:

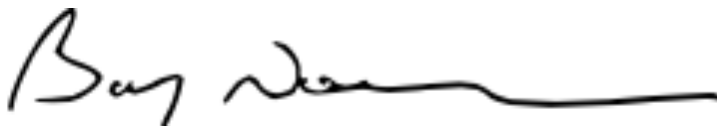
A handwritten signature in black ink, appearing to read "Bay", followed by a long horizontal flourish.

Date: 01/09/2015

Permission to Loan and / or Copy

I agree that the School of Computer Science and Statistics at University of Dublin may lend or copy this dissertation on request.

Signed:

A handwritten signature in black ink, appearing to read "Bay", followed by a long horizontal flourish.

Date: 01/09/2015

Acknowledgement

I would like to specifically acknowledge and thank my supervisor Aideen Keaney for her advice, patience, council, support and encouragement throughout this research. The time she spent with me on this research was invaluable and enjoyable.

I would like to thank all the interview participants. Without their participation, this research would not have been possible.

Finally, I would like to thank my wife for her support and understanding over the past two years.

Abstract

The explosion in internet usage in the past twenty years has resulted in a significant rise in e-commerce. E-commerce is characterised by the buying and selling of goods and services using computer networks. With the significant growth in e-commerce sites like “Amazon.com”, “eBay.com” and “Alibaba.com” (retail sites), Paddypower.com (bookmaking site) or Priceline.com (travel site) there has been a significant increase in payment card transactions. This has resulted in an increase in attempted fraud. The Payment Card Industry “PCI” has attempted to maintain credibility in e-commerce payments by requiring all e-commerce sites, who accept payment cards, to be compliant with the Payment Card Industry Data Security Standard or “PCI DSS”. Despite the requirement for all e-commerce sites who accept payment cards to be compliant with the PCI DSS, levels of compliance continue to be low. Semi-structured interviews, with participants from across the PCI, were conducted to gain an understanding of why there continues to be a low level of compliance with the PCI DSS. The study concludes that the PCI DSS is regarded as a comprehensive Information Security standard which reduces the potential for a security breach. Organisations only adopt the standard if required to do so by their acquirer or a customer. The degree of adoption is dependent on the Information Security culture of the organisation. Those organisations with a strong Information Security culture adopt the standard broadly across all IT systems. Those organisations with a weaker Information Security culture implement the minimum requirements of the standard. There are several key factors which influence the adoption of the standard. The PCI DSS is costly to implement and maintain. The PCI DSS contains complex language and there is a need for dedicated IT staff to ensure compliance is maintained. Senior executives are more concerned about damage to their brand than concerned about fines from the PCI DSS. As the PCI DSS is managed by the acquirers, commercial factors may result in low levels of compliance. As PCI auditors are employed by the merchant, commercial factors may also impact levels of compliance. There are several recommendations resulting from this research. The PCI DSS should be managed by the PCI SSC and not by acquirers. QSAs should be limited to providing a single service to a merchant. Assessment of the PCI DSS should be undertaken quarterly. Data breach notification should be mandatory. The PCI DSS should be a legal requirement for all organisations who wish to process card data.

Keywords

PCI, credit card, e-commerce, security, cyber security, standards compliance

Table of Contents

1. INTRODUCTION	1
1.1 PAYMENT CARD HISTORY	1
1.2 RESEARCH OBJECTIVES	3
1.3 SCOPE AND LIMITS OF RESEARCH.....	4
1.4 BENEFICIARIES	4
1.5 ROADMAP	4
1.6 TIMEFRAME	5
2. LITERATURE REVIEW	6
2.1 INTRODUCTION	6
2.2 E-COMMERCE SECURITY AND FRAUD	6
2.3 ANATOMY OF AN ONLINE PAYMENT CARD TRANSACTION	8
2.4 RECENT IT SECURITY BREACHES.....	10
2.5 PCI DSS.....	14
2.6 PCI DSS LEVELS OF COMPLIANCE.....	14
2.7 PCI DSS REQUIREMENTS.....	17
2.8 ADVANTAGES / DISADVANTAGES OF PCI DSS COMPLIANCE FOR MERCHANTS	18
2.9 FUTURE OF THE STANDARD	22
2.10 SUMMARY	24
2.11 IS MODELS.....	25
2.12 SUMMARY OF THE FINDINGS OF THE LITERATURE REVIEW	27
2.13 THE RESEARCH QUESTION	27
3. METHODOLOGY AND FIELDWORK.....	29
3.1 INTRODUCTION	29
3.2 RESEARCH PHILOSOPHY.....	29
3.3 RESEARCH APPROACH	30
3.4 RESEARCH STRATEGY	31
3.5 METHODOLOGY SELECTION	32
3.6 INTERVIEW METHODOLOGY.....	33
3.7 LESSONS LEARNT.....	41
4. FINDINGS AND ANALYSIS.....	43
4.1 INTRODUCTION	43
4.2 FINDINGS	43
4.3 CRITICAL ANALYSIS AND DISCUSSION OF INTERVIEW FINDINGS	65
4.4 SUMMARY	69

5.	CONCLUSIONS AND FUTURE WORK	71
5.1	INTRODUCTION	71
5.2	CONCLUSIONS.....	71
5.3	LIMITATIONS OF RESEARCH AND FUTURE WORK.....	73
5.4	SUMMARY	75
6.	REFERENCES	76
7.	APPENDICES	87
7.1	INFORMATION SHEET FOR PARTICIPANTS	87
7.2	INFORMATION SHEET FOR SENIOR MANAGEMENT	90
7.3	INFORMED CONSENT FORM FOR PARTICIPANTS.....	93
7.4	INFORMED CONSENT FORM FOR SENIOR MANAGEMENT	96
7.5	EXTRACT FROM INTERVIEW.....	99

List of Figures

FIGURE 1.1 – NUMBER OF MAJOR BRAND CREDIT CARDS IN CIRCULATION IN 2012	1
FIGURE 1.2 – PERCENTAGE RATE OF COMPLIANCE WITH THE PCI DSS	3
FIGURE 2.1 – ANNUAL GLOBAL CARD LOSSES IN USD.....	7
FIGURE 2.2 – VOLUME OF CARD TRANSACTIONS IN IRELAND (IPSO 2013).....	7
FIGURE 2.3 – HOW DATA FLOWS IN A TYPICAL CREDIT CARD TRANSACTION (BUL 2011, P.1).	9
FIGURE 2.4 – SOPHISTICATION OF ATTACK METHODS USED.....	13
FIGURE 2.6 - COMPARISON OF THE BIG FIVE SECURITY STANDARDS	24
FIGURE 2.7 – THE SECURITY ACTION CYCLE (THEOHARIDOU ET AL. 2005).....	26
FIGURE 4.1 – QUALITATIVE DATA TAG CLOUD.....	43
FIGURE 4.2 – SERVICE PROVIDER LIST OF CERTIFICATIONS	62

List of Tables

TABLE 2.1 - COMPLIANCE REQUIREMENTS FOR EACH LEVEL OF PCI 16
TABLE 2.2 – PCI DSS CONTROL OBJECTIVES AND REQUIREMENTS (PCI SSC 2008) 17
TABLE 3.1 - INTERVIEW QUESTIONS 38

Glossary of Terms

ASV	Approved Scanning Vendor
B2C	Business to customer
CDE	Cardholder Data Environment
CEO	Chief Executive Officer
CISO	Chief IT Information Security Officer
CISP	Cardholder IT Information Security Program
CTO	Chief Technology Officer
COBIT	Control Objectives for Information and Related Technology
CVV	Card Verification Value. This is the 3 or 4-digit number on the back of a payment card.
DPC	Data Protection Commissioner
EU	European Union
FTC	Federal Trade Commission
HIPAA	Health Insurance Portability and Accountability Act
IaaS	Infrastructure as a Service
IS	Information Systems
IT	Information Technology
ISO	International Organisation for Standardisation
ISP	Internet Service Provider
ms	Milliseconds
PIN	Personal Identification Number
PCI	Payment Card Industry
PCI SSC	Payment Card Industry Security Standards Council
PSP	Payment Service Provider
SAS	Statement of Auditing Standards
SAQ	Self-Assessment Questionnaire
SQL	Structured Query Language
SSL	Secure Socket Layer
SOX	Sarbanes Oxley. A US Federal law governing the requirements for US company boards, management and public accounting firms.
QSA	Qualified Security Assessor
ROC	The PCI DSS Report On Compliance which is completed by the QSA as part of a PCI DSS Level one audit.
VERIS	Vocabulary for Event Recording and Incident Sharing

1. Introduction

1.1 Payment Card History

The first payment cards were published in the early 1920's. In 1958, Bank of America launched the first retail payment card, "BankAmericard" (Visa 2015). In 1966, a second retail payment card was launched called "Master Charge" (MasterCard 2015). In 1977, "BankAmericard" was renamed "Visa" (Visa 2015). In 1979, "Master Charge" was rebranded as "MasterCard" (MasterCard 2015). In 2012, it was estimated that Visa had approximately 883 million cards in use whilst MasterCard had 721 million cards in use as per FIGURE 1.1 below.

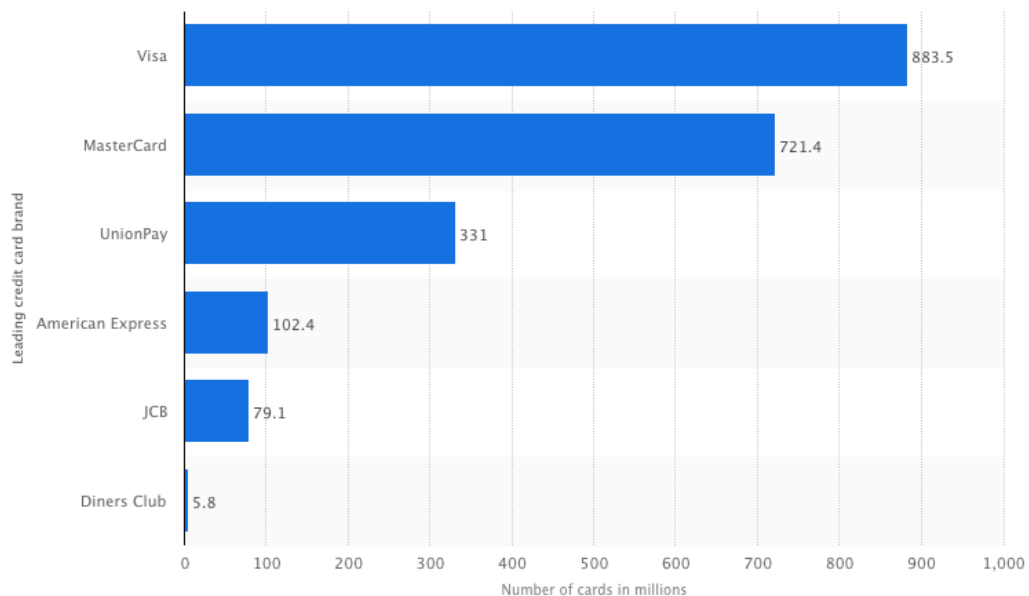


FIGURE 1.1 – Number of major brand credit cards in circulation in 2012

There are currently five major card brands MasterCard, Visa, JCB, Discover and American Express. As each card brand was operated independently, they supported their own distinct process, procedures and security accreditations for their respective merchants. Merchants struggled to meet the different security standards required by each card brand. "Between 1988 and 1998, both Visa and MasterCard reported card fraud losses at USD 750 million" (SearchSecurity Staff 2013, p.1). In 1999, in an attempt to combat this fraud, Visa launched the Visa approves Cardholder Security Program "CISP". Similarly, in 2001, MasterCard launched their Site Data Protection "SDP". Despite these new security programs, fraud

continued to rise. “In 2000, it was reported that online revenue lost due to fraud had reached USD \$1.5 billion” (SearchSecurity Staff 2013, p.1).

In 2004, in an effort to standardise payment card security Visa, MasterCard and others combined their respective security programs to launch PCI DSS v1.0. This required all merchants to implement a common security standard as described in the PCI DSS (SearchSecurity Staff 2013). “PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards, and to store, process and/or transmit cardholder data. It presents common-sense steps that mirror best security practices” (PCI SSC 2008, p.1). The standard imposes “a baseline set of technical and operational requirements designed to protect cardholder data” (PCI SSC 2010, p.5).

In addition to this common security standard, both Visa and MasterCard have attempted to enhance the security of online payments in other ways. Both brands have introduced additional payment card security measures “Verified by Visa” and “MasterCard SecureCode”. However, these security enhancements have been criticised as reducing the overall security of payment transactions (Murdoch & Anderson 2010). Ferguson (2011) explains how the “Verified by Visa” password can easily be reset, as many of the pieces of information required to reset the password are available on the card itself. These additional security enhancements have been un-popular with consumers. Market research indicates that 10% of transactions are not completed when “Verified by Visa” is in use on a website as users can often not complete the transaction (Chohen 2015).

Between 1997 and 2001 both Visa and MasterCard introduced further security measures called “card security code” or “card verification value”. This additional three-digit code was introduced on the back of payment cards to enhance the security of card not present transactions.

Despite the introduction of the PCI DSS, “Verified by Visa”, “MasterCard SecureCode”, “CVV” and other payment card security programmes there have been several significant security breaches, which have resulted in cardholder data being stolen. These breaches have occurred in both merchants (TJX, Loyaltybuild) and acquirers alike (Heartland Payment Systems).

Organisations who suffered a breach were subjected to a forensic audit by Visa. The findings of the Visa audits suggested that the breached organisations were not compliant

with the PCI DSS despite having completed successful PCI DSS audits in the previous twelve months (Oosten et al. 2014). Verizon research also supports this finding where they state “Of all the companies investigated by Verizon forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach” (Van Oosten et al. 2015, p.12).

Research by Verizon (2015) suggests that 4 out of 5 organisations are not fully compliant with the PCI DSS as per FIGURE 1.2 below.

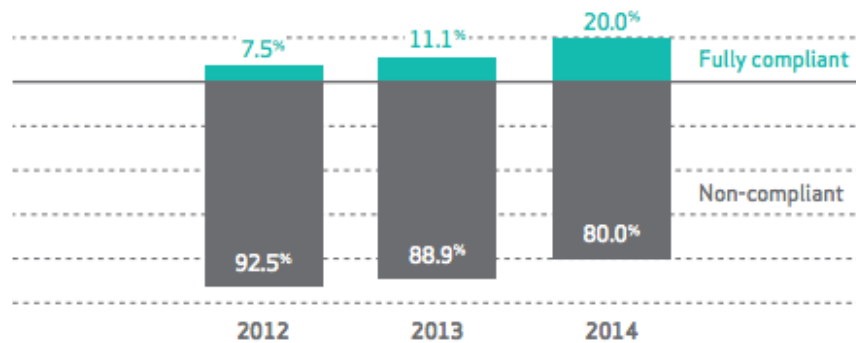


FIGURE 1.2 – Percentage rate of compliance with the PCI DSS

In summary, card security enhancements as well as IT security standards are used within the PCI to reduce the risks of a security breach. The PCI DSS is the standard that the card schemes use to ensure that participants in the payment card industry process payment card information securely. However, the number of merchants that are fully compliant with the PCI DSS continues to be low. This research investigates the factors that influence the adoption of the PCI DSS and why the rates of adoption continue to be low.

1.2 Research Objectives

The PCI DSS is a global standard, which needs to be adhered to by any organisation that processes payment cards. This research examines the reasons surrounding the low adoption rates of the PCI DSS in Ireland. What are the perceived advantages / disadvantages of the PCI DSS? What are the factors that influence an organisations adoption of the standard? What factors might improve adoption of the standard? What concerns are there in relation to the operation and management of the PCI DSS? Are there any conflicts of interest in the current operation / management of the PCI DSS? What are the current issues with the PCI DSS? Will larger fines encourage adoption of the PCI DSS?

1.3 Scope and Limits of Research

Although e-commerce payments can be made using several different technologies like Apple Pay, AliPay, Bitcoin, Google Wallet and PayPal etc. the scope of this research is limited to payments using debit/credit cards.

As an organisation's security strategy and commercial contracts are often sensitive in nature, obtaining consent from organisations to discuss their approach to IT, Information Security, PCI DSS and commercial contracts was difficult.

Notification of data breaches is not mandatory under Irish legislation. As a result, obtaining examples of data breaches in Irish organisations was difficult. The examples of data breaches are taken from US based organisations where data breach disclosure is mandatory and data breaches are more widely documented.

As the data collection mechanism selected was a semi-structured interview, it was not possible to interview a large number of people. This may limit how applicable the results are and prevent generalisations being drawn.

1.4 Beneficiaries

This research can be of benefit to commercial organisations as well as the academic community.

This research will be of benefit to any organisation considering adopting the PCI DSS. The study can also be of benefit to any organisation which is adopting or evaluating IT Information Security standards.

The research is also of academic value as it considers the commercial factors which impact the adoption of security standards. This research may assist in subsequent research into the factors influencing the adoption of security standards and specifically the factors influencing the adoption of the PCI DSS as it continues to evolve.

1.5 Roadmap

This document is organised as follows:

Chapter 1 - Introduces the research topic and provides some general background to the PCI DSS. The context for the study is presented. Research boundaries and beneficiaries are also detailed.

Chapter 2 - Is the literature review section which discusses available research on the PCI, the PCI DSS and recent large scale security breaches. It also details current research into perceived advantages and disadvantages of the standard as well as areas in which the standard could be improved.

Chapter 3 - Describes and justifies the methodologies chosen for this research. It also describes how the research participants were selected and the process under which the research was conducted. As organisation's Information Security policies are often sensitive in nature, consideration is also give to ethical concerns.

Chapter 4 - Describes the results of the semi-structured interviews. The data analysis and interpretation is also discussed. The chapter concludes with key findings.

Chapter 5 - Describes the research findings and the conclusions drawn. Limitations surrounding the research are discussed. The potential for further research is also discussed.

1.6 Timeframe

The research project was carried out between September 2014 and August 2015. The draft literature review was completed in January 2015 with on-going revisions throughout the project as new security breaches were highlighted, changes in the PCI DSS were published and additional literature became available. The School of Computer Science and Statistics at The University of Dublin granted approval for the semi-structured interviews in April 2015.

The semi-structured interviews were carried out between May and August 2015. The interview results were analysed during the interview process. Final analysis and conclusions were completed in August 2015. The research was submitted to The University of Dublin School of Computer Science on 1st September 2015.

2. Literature Review

2.1 Introduction

This literature review examines e-commerce website security and the role of the PCI DSS in enhancing the security of e-commerce transactions. It describes the origins of the PCI DSS and its objective of reducing fraud within the Payment Card Industry. Recent high profile security breaches are considered as context for the research question. Perceived advantages and disadvantages of the PCI DSS are examined as factors which may impact adoption of the standard.

The PCI DSS is a maturing standard and to date there is limited academic research available.

2.2 E-commerce Security and Fraud

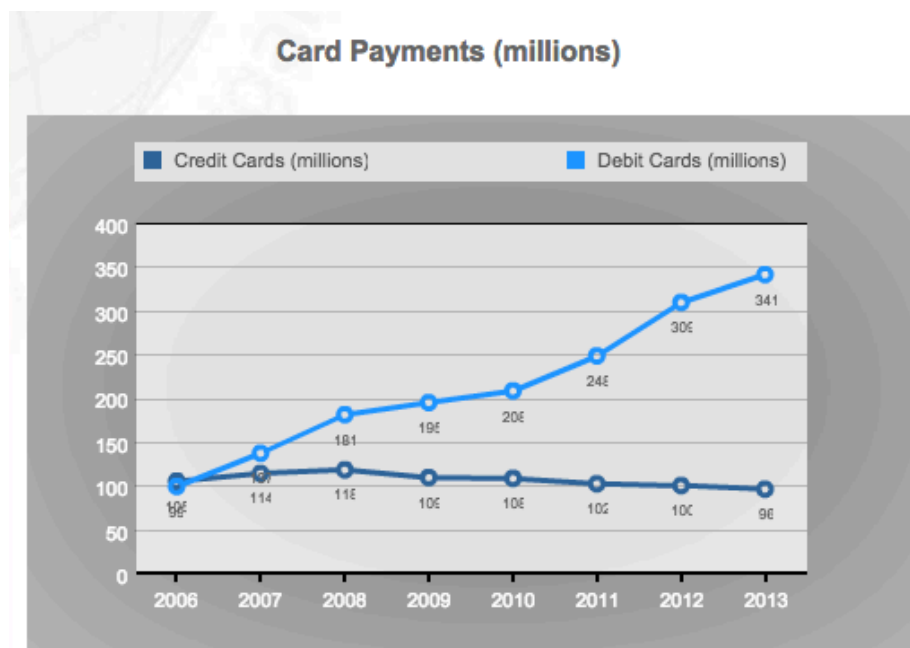
E-commerce website security is generally agreed to be the protection of e-commerce assets from unauthorized access, use, alteration, or destruction. Research suggests that website customers consider security as a critical concern in deciding whether or not to make a purchase (Hartono et al. 2014). Researchers describes e-commerce security as a customer's confidence that an e-commerce transaction is being made in confidence, with a high degree of integrity, that non-repudiation is maintained and that sufficient records remain to prove a transaction has taken place (Hartono et al. 2014; O'Raghallaigh 2010). Fraud is defined as the wrongful or criminal deception intended to result in financial or personal gain (Zorzini 2014).

The last number of years has seen a steady increase in the value of e-commerce transactions. The annual value of payment card transactions is now in excess of USD \$21 trillion globally (Kedgley 2014). The value of payment card losses is now approximately USD \$12 billion per annum as per FIGURE 2.1 below (Oosten et al. 2014).



FIGURE 2.1 – Annual global card losses in USD

The annual volume of payment transactions continues to increase as per FIGURE 2.2 below. In Ireland, during 2013, there were approximately 435 million card payments with a gross value of €21.7 billion (IPSO 2013). The value of fraudulent payments in Ireland in 2013 was estimated at €25.9 million.



	2006	2007	2008	2009	2010	2011	2012	2013
Credit Cards (millions)	105	114	118	109	108	102	100	96
Debit Cards (millions)	99	137	181	195	208	248	309	341

FIGURE 2.2 – Volume of card transactions in Ireland (IPSO 2013)

The PCI DSS looks to limit fraudulent transactions by requiring all merchants and acquirers to meet a minimum set of security requirements when processing card payments. However current evidence suggests that only 20% of companies meet all the requirements of PCI DSS (Van Oosten et al. 2015).

It has been observed that an e-commerce customer considers the security of e-commerce transactions important. It has also been shown that a significant volume of valid as well as fraudulent e-commerce transactions take place on an annual basis. It is the goal of the PCI DSS to reduce these fraudulent transactions, but compliance levels are low. Consideration in the next section will be given to how an e-commerce payment is processed, who the main participants are and how fraud may occur.

2.3 Anatomy of an Online Payment Card Transaction

Debit and credit card payments are the lifeblood of e-commerce. The processing of an e-commerce payment is a complicated process with several interactions between the customer, the merchant website, the acquiring bank, the payment card network and the customer's bank. All of these interactions take place in real-time and take only seconds to complete. In 2013, Worldpay (2014), one of the largest acquiring banks for merchants, stated that their average response time to all payment requests was 200ms.

The key participants in the PCI are:

- **Merchants** – the e-commerce site that processes the customer request.
- **Acquiring Bank** – the merchant's bank.
- **Card processors** – third party organisations that aid in card authorization and settlement processes.
- **Card issuers** – the cardholders' bank that issues cards and maintains a customer's account.
- **Card association network** – the main card brands that formed the PCI SSC.

(Capgemini 2013)

The following is a brief overview of how an e-commerce website authorizes a B2C payment, as per FIGURE 2.3 below.

- A customer inputs their payment card details into the merchant's e-commerce website.
- The merchant's e-commerce system connects to the merchant's acquiring bank, or payment processing service.

- The payment card network sends the request to the card-issuing bank where the customer has an account. The card-issuing bank verifies that the customer's account is valid and that sufficient funds are available to cover the transaction's cost.
- At this point, the funds are "held" and marked for deduction from the customer's credit limit, in the case of a credit transaction, or deposit balance, in the case of a debit card transaction. At this point, funds are not transferred to the merchant's bank accounts.
- An authorisation code is returned to the merchant's e-commerce website via the merchant's bank or payment processing service.
- The customer is notified that the payment is successful / un-successful.
- If the payment is successful, goods / services are then delivered to the customer.
- In the case of a credit card payment, the card issuing bank bills the customer for the transaction as part of their normal billing cycle.
- In the case of a credit card payment, the customer pays outstanding balance on their card.

(Metzger 2009)

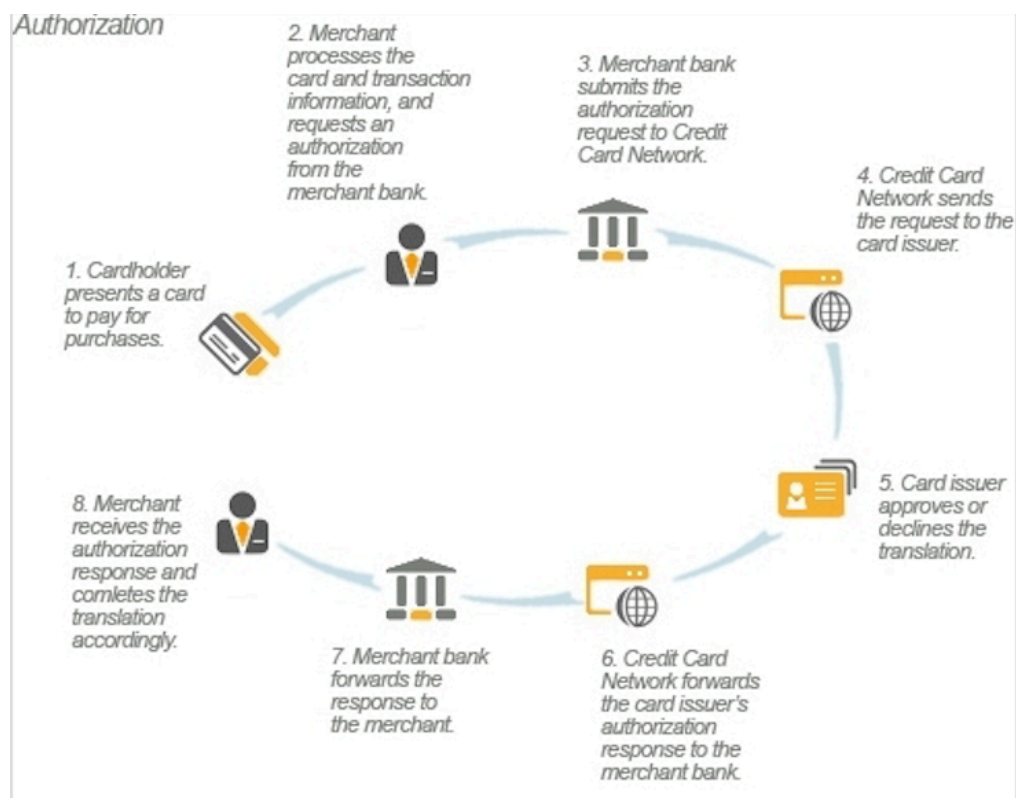


FIGURE 2.3 – How data flows in a typical credit card transaction (Bul 2011, p.1).

As has been observed, there are several different systems involved in validating a payment card transaction. A card data breach could be experienced at any of these points. The most

prevalent sources of payment card breaches are; an issue with the merchant's IT systems; an issue with the merchant bank or malware on the consumers personal computer (Krebs 2015).

In order to assess the potential value that PCI DSS compliance brings to an organisation, it is important to first review recent security breaches and the impact these breaches had on the organisation that suffered the breach.

2.4 Recent IT Security Breaches

Since the launch of the PCI DSS in 2004, there have been a number of high profile security breaches. These breaches have resulted in large amounts of customer data being compromised. The following examples describe significant data breaches since the launch of the PCI DSS. Where possible, the root causes of the breaches are also highlighted and how these root causes relate to the PCI DSS are considered.

2.4.1 Card Systems

In 2005, a merchant bank and payment processing company disclosed that approximately forty million payment cards had been compromised. Card Systems disclosed that they were improperly storing consumer card data for transactions that were not authorised. Card Systems was believed to be compliant with PCI DSS having completed an audit 11 months previously. However, as part of a forensic investigation after the breach, Visa identified that Card Systems was not compliant with PCI DSS (Zetter 2005). "The FTC charged that Card Systems engaged in a number of practices that, taken together, failed to provide reasonable and appropriate security for sensitive consumer information" (FTC Staff 2006, p.1). Specifically, the agency alleged that Card Systems:

- Created unnecessary risks to the information by storing it.
- Did not adequately assess the vulnerability of its computer network to commonly known or reasonably foreseeable attacks, including "Structured Query Language" injection attacks.
- Did not implement simple, low-cost, and readily available defences to such attacks.
- Did not use strong passwords to prevent a hacker from gaining control over computers on its computer network and access to personal information stored on the network.
- Did not use readily available security measures to limit access between computers on its network and between its computers and the Internet.

- Failed to employ sufficient measures to detect unauthorized access to personal information or to conduct security investigations.

(FTC Staff 2006)

Shortly after the breach, both Visa and MasterCard terminated their relationship with Card Systems. In 2005, Card Systems was acquired by a competitor Pay By Touch.

2.4.2 TJX

In December 2006, TJX uncovered a security breach which took place in 2005. The attack took place over a prolonged period of eighteen months (Vijayan 2008). The root cause of the breach was traced to the use of wireless networking which was configured with weak encryption. Hackers used the wireless network to penetrate TJX systems, create user accounts on TJX systems and steal the card data of up to forty five million customers (Haggerty & Ramasastry 2008). Shaw (2010) further explained that TJX stored all payment card data and that this data was not encrypted. Subsequent court filings suggest that TJX was not in compliance with PCI DSS at the time of the breach. In the twelve months following the breach, TJX disclosed that they set aside USD \$250 million to cover the costs related to the breach (Vijayan 2008). In addition the US FTC charged TJX with “failure to provide reasonable and appropriate security for personal information on its networks” (Shaw 2010, p.547). As part of the settlement with the FTC TJX agreed to external audits and changes to business practices.

2.4.3 Heartland Payment Systems

In 2008, the merchant bank, Heartland Payment Systems experienced a data breach. The source of the breach was traced to part of their website, which was developed eight years previously. This web page was vulnerable to SQL injection, which allowed the attacker access to Heartland’s corporate network. Over a period of six months the hacker accessed the more secure payments network. In this attack network sniffer software was used to capture data as it transited within the Heartland internal IT networks. Heartland was found to be compliant with PCI DSS at the time of the breach. Compliance had been certified on several occasions whilst the vulnerability had been present (Chenney 2010; Hays 2012). Heartland Payment Systems estimated that a net loss of USD \$170m was suffered as a result of the data breach. The company’s share price dropped 78% in the weeks following the breach. Visa also de-listed Heartland Payment Systems from processing transactions for a period of four months (Hays 2012).

2.4.4 Target

Between 27th November and 15th December 2013 Target had up to forty million payment cards stolen. Target systems were breached using credentials from a third party who was connected to Target's systems to provide electronic billing services, contract submissions and project management services (Munson 2014). Some reports suggest that the attack on Target was detected by IT monitoring systems and notifications were sent to Target IT staff (Munson 2014; Riley et al. 2014). However, no further steps were taken by Target staff following these notifications. Target have acknowledged that investigations into the breach only began once the US Department of Justice notified the organisation about the incident in mid-December 2013 (Riley et al. 2014). Recent reports suggest that Target is in the process of completing a settlement with MasterCard where Target will pay MasterCard USD \$19 million. Recent publications suggest that Target is negotiating a settlement with Visa that will reimburse card issuers up to USD \$67 million for fraud losses.

2.4.5 Home Depot

In April 2014 Home Depot's IT systems were breached. The breach was not identified until September 2014. Home Depot stated, "On September 8, 2014, we confirmed that our payment data systems have been breached, which could potentially impact customers using payment cards at our U.S. and Canadian stores. There is no evidence that the breach has impacted stores in Mexico or customers who shopped online at www.HomeDepot.com. Additionally, while we continue to determine the full scope, scale and impact of the breach, there is no evidence that debit PIN numbers were compromised. We apologize for the frustration and anxiety this causes our customers and we thank you for your patience and support as we work through this issue. Our investigation is focused on April forward, and we have taken aggressive steps to address the malware and protect customer data" (HomeDepot 2014b, p.1).

The root cause of the breach was traced to hackers accessing Home Depot systems using credentials of a third party contractor. The hackers then installed malware on Home Depot IT systems that allowed them to extract payment card details from Home Depot servers (HomeDepot 2014a). It is believed that up to fifty six million customers' credit card data was stolen. In addition, emails of fifty three million customers were also taken (Krebs 2014). Subsequent analysis of Home Depot IT systems suggested that antivirus software was not up to date, as required by section 5.2 of the PCI DSS. In addition IT networks were not monitored to identify suspicious behaviour as required by PCI DSS Section 10 (Miller 2014).

2.4.6 Summary

The previous examples have demonstrated how data breaches can occur. Recent research suggests that most security breaches are a result of simple security precautions not being in place. As shown in FIGURE 2.4 below, Verizon (2014) data suggests that nearly 70% of all breaches are a result of vulnerabilities that are relatively easy to exploit.

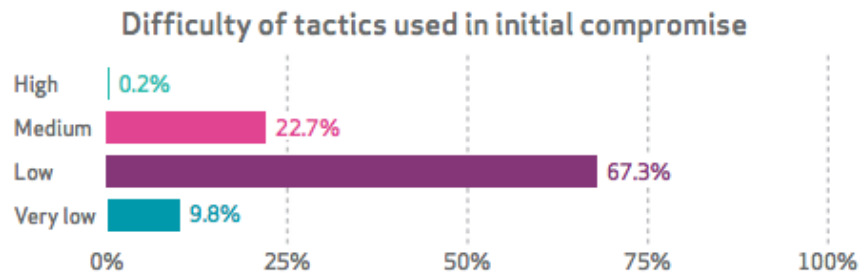


FIGURE 2.4 – Sophistication of attack methods used

A number of studies examining security of e-commerce websites suggest that there are recurring security issues which result in a data breaches. Verizon security researchers have compiled a list of common IT security vulnerabilities which resulted in card data breaches. Their research also shows the relevant section of the PCI DSS which mitigates these vulnerabilities (Van Oosten et al. 2015).

PCI Section 6 & 10. Companies who experience a breach have not applied security patches to breached systems, as required by PCI DSS Section 6 and do not have adequate monitoring in place to detect a breach, as required by PCI DSS Section 10 (Ponemon Institute 2011a).

PCI Section 7. This section states that access to sensitive data / systems are limited to those members of staff who require it for their job. In breached companies, access is often not restricted on a need to know basis (Oosten et al. 2014; Ponemon Institute 2011a).

PCI Section 1. Maintaining a security firewall. Research suggests that 71% of all Verizon customers fully meet the requirements of PCI DSS Section 1. However, analysis of data from breached organisations suggests that only 27% met all the requirements of PCI DSS Section 1. This suggests that inadequate perimeter security is a key contributor to the likelihood of suffering a breach (Van Oosten et al. 2015).

Having considered how an e-commerce payment is processed and observed several recent IT security breaches and how compliance with the PCI DSS may have prevented them, the PCI DSS itself must now be assessed. The following sections will review the PCI DSS, its history, its perceived advantages and disadvantages.

2.5 PCI DSS

The PCI DSS is a worldwide Information Security standard created by the PCI SSC.

The PCI SSC consists of a representative from each of the five major card brands. The PCI SSC Board of Advisors is made up of a single representative from the participating organisations of the PCI. These currently range from representatives from Bank of America, Cisco, Citigroup, FedEx, Walmart and Woolworths etc. This ensures that the standard is driven by those that enforce it, the acquiring banks and those that implement it, companies who process card payments (PCI SSC 2006).

The PCI DSS is the result of the merging of the similar, but independently managed, administered and enforced, security programs of the major payment card brands, Visa, MasterCard, American Express, JCB and Discover (Blackwell, Cian & Gahan 2009). The PCI DSS applies to all organisations that accept, transmit or store any cardholder data – including merchants, processors, acquirers, issuers, and service providers, as well as all other entities that store, process or transmit cardholder data (PCI SSC 2010). The focus of the standard is to reduce the number of incidents of payment card fraud. “The PCI DSS is a multifaceted security standard that includes requirements for security management, policies, procedures, network architecture, software design, and other critical proactive measures” (Gikas 2010, p.134). Kedgley summarises the latest version of the PCI DSS as an “on-going enhancement and refinement of the standard (Kedgley 2014, p.1).

2.6 PCI DSS Levels of Compliance

PCI DSS compliance is broken into four separate levels. The level of compliance an organisation needs to achieve is dependent on how card data is processed and the volume of card data processed per annum. Organisations who develop their own software, store card data or process more than six million card transactions per annum are audited at the highest level of compliance; level one. At PCI DSS level one, a QSA, an independent auditor, must audit a merchant against the PCI DSS. A QSA annually attests the merchant’s compliance to the merchant’s acquiring bank. At the other end of the spectrum, organisations who outsource card processing to specialist card processing companies, do not store card data or process fewer than twenty thousand transactions per annum are

audited at the lowest level of compliance; level four. At PCI DSS level four, a merchant completes a self-assessment questionnaire and self certifies compliance to their acquiring bank. Full details of the levels of compliance and the associated compliance requirements are in TABLE 2.1 below.

TABLE 2.1 - Compliance requirements for each level of PCI

PCI Level	Volume of Transactions	Compliance Requirement
1	6 million transactions per annum or Any merchant who has experienced a data breach	<ul style="list-style-type: none"> • Annual Report on compliance compiled by a qualified QSA • Quarterly network scan from a certified ASV • Attestation of compliance form
2	Between 1 million and 6 million transactions per annum	<ul style="list-style-type: none"> • Annual self-assessment questionnaire • Quarterly network scan from a certified ASV • Attestation of compliance form
3	Between 20 thousand and 1 million e-commerce transactions per annum	<ul style="list-style-type: none"> • Annual self-assessment questionnaire • Quarterly network scan from a certified ASV • Attestation of compliance form
4	Less than 20 thousand e-commerce transactions and all other merchants processing up to 1 million transactions per annum	<ul style="list-style-type: none"> • Annual SAQ (recommended) • Quarterly network scan from a certified ASV

		<ul style="list-style-type: none"> • Compliance validation requirements set by merchant bank
--	--	---

(Visa Europe 2015)

2.7 PCI DSS Requirements

The following section describes the detailed security requirements, processes and procedures which must be in place for an organisation to achieve PCI DSS compliance.

The PCI DSS is separated into six major objectives, twelve requirements and four hundred controls and sub-controls (Brocklehurst 2014). The details of the twelve requirements are detailed in TABLE 2.2 below.

TABLE 2.2 – PCI DSS Control Objectives and Requirements (PCI SSC 2008)

Control Objectives	PCI DSS Requirements
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 on all systems commonly affected by malware

	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 IT Information Security Policy	12. Maintain a policy that addresses IT Information Security

It has been observed that the PCI DSS is a complex standard with many requirements to be fulfilled. A merchant needs to make important decisions regarding the level of certification to undertake and decide if they can self-certify or if the services of a QSA need to be retained. The following section considers researchers perceptions of the advantages and disadvantages of the PCI DSS.

2.8 Advantages / Disadvantages of PCI DSS Compliance for Merchants

Current research suggests that a standardised security policy positively contributes towards the PCI's goal of reducing fraud and maintaining consumers trust in the PCI (Rees 2012; Coburn 2010; Blackwell, Cian & Gahan 2009). However, researchers believe there are both advantages and disadvantages to the PCI DSS.

2.8.1 Advantages

Despite the requirement to comply with the PCI DSS, there are several additional advantages to being compliant with the PCI DSS:

- Research suggests that organisations who are PCI DSS compliant are less likely to suffer a security breach. Verizon (2014) researchers suggest that 89% of organisations who suffered a data breach were not compliant with the PCI DSS when the breach occurred. Schwartz (2011) similarly suggests that 62% of companies who were not compliant with the PCI DSS suffered data breaches in the preceding two years. The Ponemon Institute (2011a) further suggest a correlation with Schwartz and Verizon data where 85% of non-compliant organisations had suffered one or more data breaches.
- Verizon (2014) researchers suggest that companies who are compliant with the PCI DSS detect and respond to breaches more quickly. PCI DSS section 10 details the requirement to actively monitor all access to cardholder data and network resources. Verizon research into breached organisations identified that only 9.4% of the organisations were fully compliant with section 10 of the PCI DSS. This 9.4% rate of compliance in organisations that suffered a breach is compared to an average of 34% of all Verizon research participants being fully compliant with section 10 of the PCI DSS. “This suggests that there is a correlation between a lack of effective log management and the likelihood of a data breach” (Oosten et al. 2014, p.36).
- In the event of a breach, an organisation may be given “Safe Harbour” and certain penalties and fines may be reduced if the merchant is compliant with the PCI DSS at the time of the breach (Ataya 2010).
- “The standard is still seen to try to promote pro-actively thinking about the security of card holder data and not just driving compliance with a standard” (Kedgley 2014, p.1). Kedgley (2014) suggests that the standard should not be a “box ticking” exercise or a process in satisfying administrative requirements. He argues that the standard is trying to promote best practice in IT security. Kedgley (2014) and Oosten (2014) suggest that in order to achieve the maximum benefit from the PCI DSS it should be considered as part of an on-going compliance program forming part of a strong IT governance model. Having assessed the latest version of the standard Kerner (2013) suggests that version three introduces enhanced requirements which will ensure that security is “enshrined as a business as usual activity” (Kerner 2013, p.1).
- Organisations who comply with the PCI DSS are more easily able to adopt other Information Security standards like HIPAA, SOX and ISO (Gikas 2010).
- PCI compliance can be used as a “trust assurance”. Trust assurances lead to increased willingness to purchase from a site (Kim & Benbasat 2010; Lansdale 2014). FIGURE 2.5 below shows an example of a trust assurance. Research shows that having several trust assurances increases a customer’s intention to purchase (Kaplan & Nieschwietz 2003).

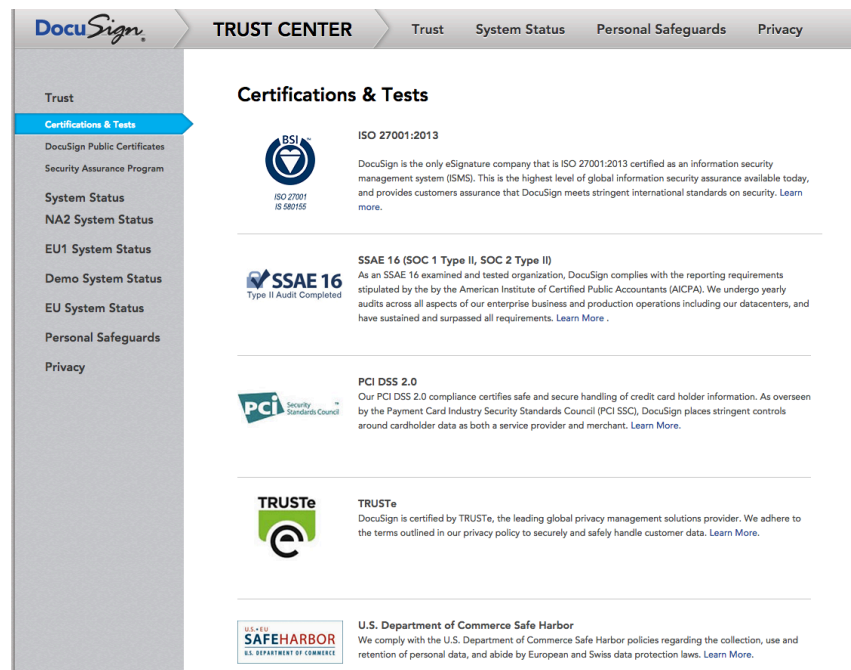


FIGURE 2.5 - Example of a trust assurance on DocuSign.com

2.8.2 Disadvantages

There are several perceived disadvantages to be the PCI DSS. As follows:

- A number of surveys report that attaining and maintaining PCI compliance is too difficult (Rees 2012; Ponemon Institute 2011b; Varian Foster et al. 2009). The Ponemon Institute (2011a) state that 53% of those surveyed agreed that obtaining PCI DSS compliance is more difficult than obtaining compliance under other standards like HIPAA, SOX and ISO.
- Several surveys have reported that the costs of compliance are too high (Rees 2010; Hovav & Gray 2014). On average PCI DSS level one firms spend approximately USD \$3 million per annum on maintaining compliance in 2008 (Morse 2012). Separate research from the Ponemon Institute suggests similar costs (Ponemon Institute 2011b).
- Shermach's (2012) research suggests that many merchants find the language used in the standard difficult to understand.
- Smaller merchants may not have sufficient IT expertise or staff to assist with obtaining and maintaining compliance (Shermach 2012).
- Merchants are confused about what level of compliance they are supposed to obtain (Shermach 2012).
- If the organisation is not PCI compliant and a data breach occurs the organisation may be subject to the following penalties:
 - The merchants acquiring bank may withdraw payment card processing services.

- The merchant will be required to cover the cost of the acquiring banks forensic investigations.
 - The merchant will be liable for the costs of the fraudulent purchases.
 - The merchant will be liable for the cost of replacing customers' stolen cards.
- Depending on the size of the breach fines of up to USD \$500,000 can be levied against the merchant for each identified breach (Braintree 2008).
- If a breach occurs and an organisation is not PCI DSS compliant, the organisation is subsequently assessed at PCI DSS level one.
- Damage to a brand / loss of reputation and loss of customer loyalty. Several websites who have suffered significant data breaches have suffered from negative press (RTE News 2013). In 2013, Loyaltybuild suffered a breach of their IT systems, which resulted in the payment card data of over one million customers being compromised. As part of their investigations into the data breach, the Office of the Data Protection Commissioner required Loyaltybuild to stop processing customer data. Loyaltybuild ceased trading for 4 months until the Office of the Data Protection Commissioner was satisfied that cardholder data was being processed securely (Weckler 2014). Loyaltybuild stored the payment card CVV, which is in violation of PCI DSS requirement 3.2. The cardholder data was not encrypted in violation of PCI DSS requirement 3.4. Loyaltybuild was also compelled by the Office of the Data Protection Commissioner to achieve PCI DSS compliance (Office of the Data Protection Commissioner 2013).
- Verizon (2015) research suggests that 69% of customers surveyed would be less likely to do business with a breached organisation. In Berezina's research, residents of a hotel were advised of several security scenarios where card data was breached. Berezina (2012) concluded that any card breach would result in negative re-visit sentiment to the hotel and negative sentiment to recommend the hotel to others.
- Sullivan (2014) argues that the objective of the PCI DSS is not to prevent fraud. Its objective is to ensure fraud is low enough so that consumers continue to actively use payment cards, as opposed to alternative means of payments (cash, cheque, other electronic payments) where Visa / MasterCard generate no revenue. Sullivan suggests the apparent unwillingness to address the root causes of payment fraud means that fraud will always be present.
- Segal (2011) argues that PCI DSS is fundamentally flawed. He states it is an effort by the card schemes to shift responsibility to merchants in terms of financial penalties without addressing the underlying reasons for e-commerce fraud. Segal explains this by example - If a merchant accepts a fraudulent payment, the merchant incurs most of the costs. The card schemes and acquiring banks receive the appropriate transaction

processing fees for both legitimate as well as fraudulent transactions. As the card schemes are insulated from the majority of the cost of fraud there is little impact to the card schemes revenue. There is therefore, little incentive for the card scheme to permanently address this fraud.

- Compliance with the PCI DSS is currently not a legal requirement. Cohen (2014) argues that in order to be truly successful, compliance with the PCI DSS must be a legal requirement. Cohen suggests that organisations will actively attempt to avoid becoming compliant with the PCI DSS. Cohen believes that other incentives to encourage compliance will generally not be effective. Only a legal statute will stop avoidance and force organisations to comply.
- Cohen (2014) also suggests that that firms should receive financial incentives to become compliant with the PCI DSS. Segal (2011) similarly suggests that firms should be incentivised to become compliant in the form of lower payment transaction charges.
- Verizon acknowledge that merchants often state that achieving PCI DSS does not encourage organisations to “build a comprehensive security program; it merely encourages it to achieve compliance for the relevant systems.” From its own research, Verizon respond “PCI Security standards improve their chances, both of avoiding a breach in the first place, and of minimizing the resulting damage if they are breached” (Oosten et al. 2014, p.8).

Several advantages and disadvantages to the standard have been detailed. It must be considered that over time, as the standard evolves that the disadvantages will be addressed. In the following section, the future of the standard is considered in the context of how the PCI SSC may address current perceived deficiencies in the standard.

2.9 Future of the Standard

In reviewing the future of the standard, researchers’ observations have been summarised into four sections. These suggested enhancements would represent new or amended requirements to address; changes in technology; ensuring that the standard continues to be appropriate; ensuring the adoption rate of the standard continue to improve; and consolidation of the standard.

2.9.1 Changes in Technology

Stapleton (2011), Williams (2010) and Sullivan (2014) suggest that using a technique called tokenisation is a an effective way to reduce PCI obligations. Tokenisation is the process where a piece of sensitive data is replaced by non-sensitive data. The merchant stores the token; the real card data is held in highly secure third party systems. In payment cards, the credit card number would be replaced by an appropriate token. These tokens have no

intrinsic or exploitable value. In the case of a merchants system being compromised, the loss of token data has no risk associated with it (Segal et al. 2011).

2.9.2 Enhancements to The standard

Despite focusing on larger merchants and penalties being issued, the PCI process has not prevented security weaknesses that allow large data breaches to take place (Sullivan 2014). Sullivan (2014) suggests that in order for PCI to be effective in reducing fraud that merchant banks need to more regularly monitor merchants for compliance and that larger fines should be imposed on banks whose merchants suffer a breach. The United States government may, in the near future, require US organisations to carry out continuous monitoring to ensure the security of their systems (Dempsey et al. 2011).

2.9.3 Improve Adoption Rates

Several researchers have also suggested that disclosure of data breaches be made mandatory to the wider public and not just to those customers directly impacted by the breach (Shaw 2010; Hartley 2009; Weiss 2011). Mandatory disclosure of a data breach is already required for US based HealthCare organisations as mandated by the HIPAA (Services 2009). Mandatory disclosure of breached organisations would allow customers to make a decision on whether to transact with sites that suffered a breach. This in turn may improve levels of compliance, as merchants will see PCI DSS compliance as an advantage or a trust assurance (Morse 2012).

Lindstrom (2014) suggests that PCI DSS should be treated more like an insurance premium. If a merchant has a low appetite for risk and are PCI compliant, their PCI premium is lower. If a merchant has a higher appetite for risk and as a result is not PCI compliant, they would pay a higher PCI premium.

2.9.4 Consolidation

Some researchers believe that given that there are many similar / competing standards such as ISO 27001, HIPAA and PCI DSS etc. the future of all these standards is a generic data security standard that can be adopted by any organisation (Gikas 2010; Rowlingson & Winsborrow 2006; Lovrić 2012). Comparative research by Susanto (2011) highlights that there are no significant differences between several of the major IT Security standards in use today. This can be seen in FIGURE 2.6 below where Susanto has compared eleven key aspects of IT security across multiple standards.

		ISO 27001	BS 7799	PCIDSS V2.0	ITIL V4.0	COBIT V4.1
1.	<i>Information Security Policy</i>	√	√	√	√	√
2.	<i>Communications and Operations Management</i>	√	√	√	●	√
3.	<i>Access Control</i>	√	√	√	√	√
4.	<i>Information Systems Acquisition, Development and Maintenance</i>	√	√	√	●	√
5.	<i>Organization of Information Security</i>	√	√	√	√	√
6.	<i>Asset Management</i>	√	√	√	√	√
7.	<i>Information Security Incident Management</i>	√	●	√	√	√
8.	<i>Business Continuity Management</i>	√	√	√	√	√
9.	<i>Human Resources Security</i>	√	√	√	●	√
10.	<i>Physical and Environmental Security</i>	√	√	√	●	√
11.	<i>Compliance</i>	√	√	√	√	√

FIGURE 2.6 - Comparison of the Big Five Security Standards

2.10 Summary

As has been observed, PCI compliance is a requirement for all organisations that process payment cards. Several large data breaches have been examined which have highlighted that basic security controls, required by the PCI DSS, were not in place at the time of the breaches. Where possible, the areas of the PCI DSS which address these security controls were detailed.

Despite the advantages of complying with the PCI DSS several disadvantages have also been highlighted. Some authors have argued that in order to be successful further changes to the standard are required. Other authors argue that the PCI DSS needs to be a legal requirement before it will be widely adopted. While other researchers argue that the PCI DSS needs to be merged with other international security standards like ISO before it is more widely adopted.

It is clear that there are several commercial implications for organisations if they suffer a breach and are not PCI DSS compliant. These range from fines, penalties, additional audit requirements, potential loss of customer loyalty and ultimately withdrawal of payment services.

It is important to now examine relevant Information Systems models, which are often used when evaluating the adoption of standards. This model is discussed in the next section.

2.11 IS Models

In considering the adoption of standards, IS research often refers to the deterrence model.

2.11.1 The Deterrence Model

The concept of “deterrence” can be defined as the use of threats by one party to convince another party to refrain from initiating some course of action (Huth 1999). Beccaria (1995) suggests that deterrence theory linked to the idea that people make logical decisions based on maximising their benefit and the minimising their cost. Theoharidou also describes deterrence as “when the possibility of punishment is high and the sanction is severe, potential criminals will be deterred from committing illegal acts” (Theoharidou et al. 2005, p.474). The general model of deterrence is stated by researchers to “deter” by having policies, procedure, guidelines and awareness programmes for IS Security. “Prevent”, by having physical as well as procedural controls to prevent abuse of information systems. “Detection”, by having monitoring and auditing of systems. “Remedies”, where an incident response plan is in place which details how to respond when a security incident occurs (Theoharidou et al. 2005). This cycle is referred to as the “Security Action Cycle” as described in FIGURE 2.7 (Straub & Welke 1998).

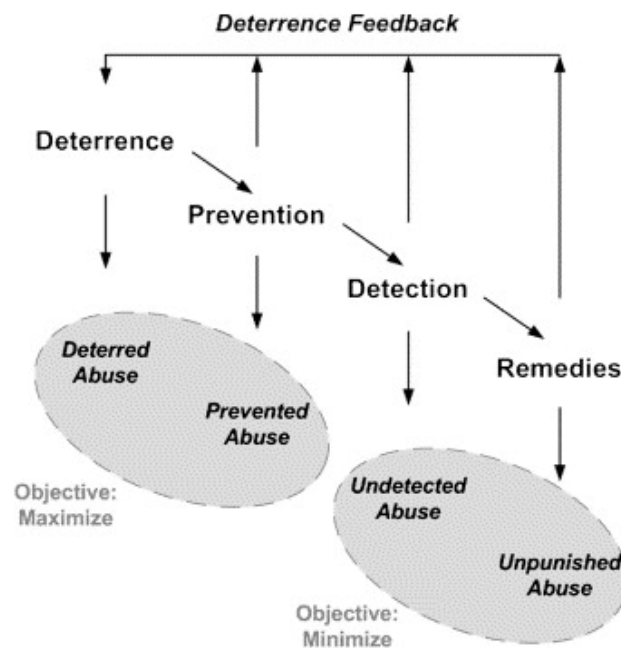


FIGURE 2.7 – The Security Action Cycle (Theoharidou et al. 2005)

Shaw (2010) argues that deterrence has a positive impact on companies data security which has lead to fewer data breaches.

There is extensive research into deterrence theory and the positive impact it has on the adoption of corporate IT policies and the reduced incidents of internal IT security breaches (HU et al. 2011; Willison & Warkentin 2013). However, there is little academic research into the impact of deterrence theory on the adoption of standards like PCI DSS.

Research by D’Arcy (2009) suggests that there are 3 key practices which deter breaching IS security policies. These are;

- User awareness of security policies.
- Security education.
- Monitoring.

D’Arcy’s research also suggests that the perception of sanctions is more effective than the certainty of sanctions in reducing IS policy misuse.

Research from Chen (2012) suggested reward enforcement, a remunerative control mechanism in the information systems security context, could be an alternative for organizations where sanctions do not successfully prevent violation.

Parker (1998) employs the core concepts from the Security Action Cycle for the theoretical grounding of the security framework. His model sets the following security goals: avoidance, deterrence, prevention, detection, mitigation, sanction, transference, investigation, recovery and correction. Many of these goals can be closely linked to specific areas of the PCI DSS.

During the analysis phase, consideration will be given to assess if deterrence theory can be applied to improve the rates of adoption of the PCI DSS.

2.12 Summary of the Findings of the Literature Review

This literature review examined the role of the PCI DSS as a standard that is designed to reduce fraud and to maintain consumers trust in the PCI. In considering the number of participants in processing a payment card transaction, it can be seen that there are many opportunities for a card data breach to occur. Some recent breaches were examined and where possible it has been highlighted how compliance with the PCI DSS could have reduced the chances of these breaches occurring.

Whilst the PCI DSS continues to be updated it is clear that many researchers now believe that mandatory disclosure of breaches, better enforcement, merchant incentives and stronger penalties for non-compliance are the key to the on-going success of the PCI.

The “Security Action Cycle” was introduced as a commonly used IS model which demonstrates how adoption of standards / policies can be improved.

It has been shown that the PCI DSS has advantages as well as disadvantages. In 2014, only 20% of organisations were found to meet all the requirements of the PCI DSS. Having observed that merchants who process card payments are required to be compliant with the PCI DSS the question as to why levels of compliance are so low needs to be considered.

2.13 The Research Question

Compliance with the PCI DSS is mandatory for any organisation that processes or stores card data. There are many documented advantages to being compliant with the PCI DSS. These advantages range from enhanced customer trust in an organisation’s services, confidence that the organisation’s e-commerce systems are more secure to having a stronger IT governance model within an organisation. Being compliant with the PCI DSS also makes further compliance programmes easier to attain. However, despite the

compliance requirement to comply with the PCI DSS, levels of compliance continue to be low. This research examines the factors influencing the adoption of the PCI DSS

This research will also address:

- What are the perceptions of the advantages / disadvantages of the adoption of PCI DSS?
- How does PCI DSS compare to other standards?
- What areas of the standard need to be improved to improve adoption rates?
- Are there operational / management issues with the standard which result in organisations avoiding implementation of the PCI DSS.
- How can adoption rates be improved?
- What role could deterrence theory have on the adoption of PCI DSS?

3. Methodology and Fieldwork

3.1 Introduction

This chapter reviews common research philosophies in use in IS research. It also gives a rationale for the research strategy selected for this project. This chapter will also discuss sampling, data collection, ethical concerns and limitations of the research methods selected.

3.2 Research Philosophy

A research philosophy can be defined as a researchers own personal view of what constitutes acceptable knowledge and the process by which this is developed (Saunders & Tosey 2012; Saunders et al. 2012). This knowledge is impacted by the researchers personal view as well as constraints like the time to carry out the research as well as funding and other practical considerations (Crotty 1998).

There are several common research philosophies or paradigms. These are often reported as: “Positivist”, “Interpretivist”, “Realist” and “Pragmatist” (Saunders et al. 2012). The selection of a research philosophy is often dictated by the research question and on the personal views of the researcher (Saunders et al. 2012).

The positivist position is derived from that of natural science. It is characterised by the testing of hypothesis developed from existing theory (Saunders et al. 2012). Positivism is a focus on facts and phenomena that can be observed and which will produce credible data (Saunders et al. 2012). As a result, positivism is often associated with experiments as “there is a need to identify and assess the causes that influence outcomes” (Creswell 2003, p.7). These facts are gathered through direct observation and experience. Measurement is usually carried out using quantitative methods. A general approach to positivist research starts with a theory, the researcher collects data that supports or refutes the theory. The researcher then makes necessary revisions and conducts further tests to make their theory stronger (Creswell 2003).

Interpretivists’ believe that individuals make sense of situations based upon several factors. These factors include individual experience, memories as well as expectations. As these factors are constantly evolving over time, the researchers response to situations also changes (Saunders et al. 2012). Using this paradigm, it is important to discover and understand these situations and the factors, which lead to individual decisions. Interpretivist research is said to be research among people as opposed to objects. Saunders (2012)

suggests that in order for an interpretivist approach to be successful, the researcher must be empathetic and be immersed in the research subject's point of view. As a result of this empathy and immersion, interpretivist research is often associated with qualitative techniques (Creswell 2003)

Realism was born from a frustration that positivism was deterministic due to the causal nature of the universe. As a result, realism inherits traits from both positivism and interpretivism. "The core philosophy of realism is that there is a reality independent of the mind" (Saunders et al. 2012, p.136).

"Pragmatists assert that concepts are only relevant where they support action" (Saunders et al. 2012, p.130). This suggests that the most important determinant in the selection of a research philosophy is the research question itself. A pragmatist view is that unless the research question unambiguously suggests one philosophy, it is appropriate for the researcher to work with different philosophical positions. As a result, pragmatism is often associated with mixed method research.

Having considered common research philosophies, the second important decision in a research project is the consideration of an appropriate research approach. Several common approaches are described in the next section.

3.3 Research Approach

The research approach can be qualitative, quantitative or mixed methods (Creswell 2003).

Quantitative research is a data based approach, which provides statistical and numerical insight into people's thoughts about a subject. By association, quantitative research is often characterised by determinism (Saunders et al. 2012). This "suggests that examining relationships between and among variables is central to answering questions and hypotheses (Creswell 2003, p.155). This is often the case when highly structured data collection techniques are used (Saunders et al. 2012).

By comparison, Creswell describes "qualitative research as an approach for exploring and understanding the meaning individuals or groups ascribe to a social or human problem" (Creswell 2003, p.246). Qualitative research is a method of inquiry employed in many different academic disciplines. Traditionally qualitative research is associated with the social sciences, but is also used in market research and further contexts (Denzin & Lincoln 2005). It is the role of the researcher to seek to understand those who are being

studied and the subjective reality of those participants in the research “in order to understand motives, actions and intentions in a meaningful way” (Saunders et al. 2012, p.109). As a result, qualitative research is generally associated with the interpretivist philosophy (Saunders et al. 2012).

Mixed methods research is often referred to as a blended approach, which involves both quantitative and qualitative data. Both pragmatists and realists can use mixed methods. Mixed methods is becoming popular in business and management research, as it is likely to overcome weaknesses associated with using one single approach. It is also argued that using a mixed method allows for a richer approach to data collection, analysis and interpretation (Saunders et al. 2012). How and when the mixing of quantitative and qualitative methods occurs is at the discretion of the researcher. However, there are several common approaches, which vary from sequential mixed methods to concurrent mixed methods (Creswell 2003).

Having considered common research approaches, the next important area to be considered in a research project is the research strategy. Common research strategies will be considered in the next section.

3.4 Research Strategy

The research strategy describes the research methods that will be used to gather and analyse data for the research project. Saunders (2012) suggests that the choice of strategy is also guided by the research question. There are several popular research strategies or research methods in use today. Examples of these strategies are experiment, surveys, archival research, case study, ethnography, action research, grounded theory and narrative inquiry. Many research strategies are associated with quantitative research (experiment and survey). Several strategies can be associated with both quantitative and qualitative research (archival research, case study). The remaining strategies are usually associated with qualitative research.

- Experiments are based on examining hypotheses as opposed to research questions. An experiment is the study of the probability of change in an independent variable causing change in another dependant one. (Saunders et al. 2012)
- Surveys are associated with deductive research. The approach is popular in both management and business research. A survey is often useful in answering ‘what’, ‘who’ and ‘where’ questions.

- Archival research is a type of primary research that uses data from archival data sources. It is important to ensure that when doing archival research that primary data sources are used and not secondary sources.
- A case study explores a topic in a real-life situation. A case study is useful in answering questions like ‘why?’, ‘what?’ and ‘how?’ (Saunders et al. 2012).
- Ethnography is used to study groups. This form of research usually involves researchers being closely involved and interacting with the research group to better answer the research question.
- Action research is generally research to resolve a “real organisational problem” (Saunders et al. 2012). The researcher is closely involved in identifying the problem and helping to resolve it.

3.5 Methodology Selection

As observed previously, the selection of the appropriate research methodology is often driven by the research question itself (Saunders et al. 2012). This study examines the factors that influence the adoption of the PCI DSS; there are several items that should be considered:

- Compliance with IT security standards and the PCI DSS are often considered commercially sensitive in nature.
- An organisation’s approach to IT security and the PCI DSS may be driven by competitive commercial factors.
- An organisation’s approach to IT security and the PCI DSS may depend on the size of the organisation or the size of the IT department.
- An organisations attitude to PCI DSS compliance may be based on a risk based approach where an organisation considers the costs of compliance to the cost of penalties should a breach occur.
- An organisation, or senior members of staff, may have previously been involved in an IT security incident, which would result in a change to their views on Information Security and the PCI DSS over time.
- The organisation may not have sufficient skills or IT staff to obtain compliance.
- An organisation’s approach to IT security is unique to that organisation.
- An organisation’s approach to IT security may depend on their commercial sector or be required because of commercial contracts with suppliers / customers.

The purpose of interpretive inquiry is to gain an understanding of human experience through establishing the meanings of phenomena. The intention of the interpretative approach is to

objectively interpret the meanings of phenomena that hide behind expressions of experience. As the research question considers human factors influencing the adoption of the PCI DSS, an interpretative philosophy was considered appropriate for this project.

Having adopted an interpretivist philosophy, an appropriate research approach needs to be selected. In considering qualitative versus quantitative approaches a qualitative approach was selected. The research question suggests a need to understand why people react in certain ways and their feelings about their actions. The research question further suggests a need to understand each participant's unique experiences in relation to Information Security and the PCI DSS. A qualitative approach was chosen to ensure that the researcher understands the particular and possibly unique circumstances of each participant and their views on the PCI DSS.

In considering appropriate qualitative approaches to data collection again, the research question is considered. Selection of a semi-structured interview had distinct advantages over other methods. The semi-structured interview approach encourages two-way conversation between the researcher and the participant. During a semi-structured interview, participants are more willing to discuss sensitive issues (Kvale 2007), as might be the case in discussing IT security and PCI DSS compliance. The majority of questions are created during the interview, allowing both the interviewer and the person being interviewed the flexibility to probe for details or discuss issues in more depth.

A semi-structured interview was selected to elicit the maximum amount of information from participants as to their perceptions of the PCI DSS.

3.6 Interview Methodology

Careful consideration was given to the interview process. This was to ensure that the maximum information was elicited from the interviewees, information was recorded accurately and findings were reported in an ethical manner. As suggested by Kvale the "quality of the interview is decisive for the quality of subsequent analysis, verification and reporting of the interview findings" (Kvale 2007, chap.7). Kvale (2007) further suggests that the quality of an interview is dependent on 3 key criteria:

- The interview is interpreted throughout the interview.
- The interviewer attempts to verify his / her interpretations of the subject's answers in the course of the interview.
- The interview is "self-reported", it should be a self-reliant story that requires little additional explanation.

In designing the interview process, Kvale's 7 stages approach was used (Kvale 2007). This approach considers all aspects of the interview process starting with the consideration of the goals of the interview to the final reporting of findings.

- Themazing – What is the theme of the interview? Kvale suggests that the researcher needs to understand the objectives of the interview and keep these objectives in mind throughout the interview process.
- Designing – The researcher keeps a systematic record of the design procedure. Keep the final report in mind when designing the study, ensuring that ethical issues and informed consent are included.
- Interviewing – The goal of the interview is to ensure that the interview can be reported to readers once the recorder is turned off. This suggests that the interview can be read as a narrative on its own with little additional explanation.
- Transcribing – Kvale suggests that the researcher keeps in mind the readability of the finally published interviews and that the confidentiality of the interviewee is always maintained.
- Analysing – Based on the appropriate type of investigation.
- Verifying – Check the validity, reliability and generalizability of the findings
- Reporting – Communicate findings in a scientific and ethical manner.

(Kvale 2007)

3.6.1 Themazing

The goal of the interview is to speak to subject matter experts in the payment card industry. As part of these conversations, the goal is to understand what factors impact an organisation's adoption of the PCI DSS.

The researcher needed to become immersed in the area of research. To assist with this, additional background research was carried out on each interviewee and the organisation they represented in advance of each interview. This allowed for an in-depth interview as the researcher already had a basic understanding of the role of the interviewee in the organisation and of the organisation itself.

3.6.2 Designing

In ensuring that the overall theme of the interview is consistent, several additional factors must be considered. The following sections detail the other considerations in deciding the overall theme of the interview.

3.6.2.1 Time Horizon

There are generally two time horizons to consider as part of any research project, these are: cross-sectional and longitudinal. This research is cross-sectional in nature. This is primarily due to time constraints. A cross-sectional approach to the research question is appropriate as the research question considers an organisations current approach to the PCI DSS.

3.6.2.2 Ethical Issues

As qualitative research is often personal in nature where the researcher interviews a subject or observes a subject, the question of ethics must be considered. Kvale (2007) suggests that completing an interview to a high degree of scientific quality, with the interviewees' answers probed and interpretations checked, may conflict with ethical concerns of not harming the interviewee. This is relevant in the context of the research question as participants may disclose details of their organisation's Information Security strategy or disclose information about card data breaches experienced by a firm. The following concerns were considered as part of the ethics review:

- Anonymity – all interview results are presented anonymously, neither the interviewee nor the organisation they represent are mentioned.
- Risk of unanticipated harm – There is a potential that a participant may disclose commercially sensitive information relating to a data security breach in their organisation.

In order to address these concerns an informed consent document advising participants of ethical obligations was produced and given to each interviewee. A supplemental management consent document was also produced. These documents advised the interviewee and their manager of the interview process and the steps taken to ensure the ethical guidelines of the University of Dublin were maintained. A copy of these are presented in Appendix 1 and 2.

3.6.2.3 Recruitment Strategy & Sample Size

"In-depth interviews are used to discover shared understandings of a particular group. The sample of interviewees should be fairly homogenous and share critical similarities related to the research question" (DiCicco-Bloom & Crabtree 2006, p.1). As a result, the accuracy of the work is dependent on the appropriate recruitment strategy.

As previously noted, the key participants in the PCI are:

- The merchant
- Security Auditors

- The acquiring bank
- The PCI SSC
- The Card Schemes

In practical terms, it is not possible to collect data from every member of a community in order to get comprehensive valid findings. In qualitative research, a sample of a population is selected in any given study.

Purposive sampling is one of the most commonly used sampling strategies (Palinkas et al. 2013). Participants are grouped according to pre-selected criteria. Purposive sampling is also useful when there is limited time and resources, as is the case with this research question. In the case of this research question, sampling from a population outside of the PCI would add little value to answering the research question.

A sample of thirteen participants was chosen. This number was chosen as a reasonable balance between the time available to complete the research and the time intensive nature of one to one interviews.

Interview participants were selected from across all aspects of the PCI. Participants were sought from PCI DSS level one merchants as this is the strictest level of compliance under the PCI DSS. Participants were also sought from the acquiring banks. The acquiring banks maintain the legal contract with the merchant and are responsible for the day-to-day implementation of the PCI DSS. Participants were also sought from the PCI council. This is the body that represents the Card Schemes and are entrusted with managing the standard.

It would also be beneficial to have participation from the Card Schemes, but due to limitations in time, resources and lack of access to any participant in the Card Schemes it was not possible to include them in the sample.

3.6.3 Interviewing

In ensuring that the ethical guidelines from The University of Dublin were met, ethical approval was received before any interview could take place. Interviews were conducted at a suitable time and location for the participant.

The following is representative of the major sections of the interview.

Once initial introductions were completed, the research question was explained to participants.

As suggested by Kvale (2007), to ensure no ethical issues arise, informed consent was received from all participants. In line with ethical guidelines from The University of Dublin, the participant was given a copy of the “Informed Consent” form (see Appendix 1). Any questions from the participant were answered at this time. The participant was also requested to have a member of senior management within the company sign the “Management Consent” form (see Appendix 2). Permission was also sought to record the interview. Once the appropriate consent forms were completed, the interview proper began.

The interview took the form of a semi-structured interview which contained a core set of questions. As suggested by Wengraf (2001), the questions were open ended in nature allowing for as much relevant information as possible to be elicited from participants.

TABLE 3.1 represents the major questions asked of all participants. The structure of the questions were derived from Kvale (2007) and Wengraf (2001). As suggested by Kvale, the research interview questions were designed in consideration of the following recommendations:

- Introducing questions – “Can you tell me about?”
- Follow-up questions – Direct questions based on what has just been said.
- Specifying questions – “What did you think then?”
- Direct questions – “Have you ever experienced a data breach?”
- Indirect questions – “How do you believe other organisations regard the PCI DSS?”
- Structuring questions – When a theme has been examined in detail, directing the conversation in a new direction.
- Silence – Allowing the interviewee to consider their answers and to progress the conversation himself or herself.
- Interpreting questions – “You mean that?” “Is it correct to say that?”

(Kvale 2007)

TABLE 3.1 - Interview Questions

Questions
Q1. Please describe the structure of your IT organisation.
Q2. Can you describe who is responsible for IT security and Compliance within the organisation and why?
Q3. Could you explain your / your organisation's attitude to Risk?
Q4. Can you explain your approach to IT Security?
Q3. Can you describe the standards you use to benchmark your IT Security model?
Q4. Can you discuss the data protection requirements within your organisation?
Q5. Describe your approach PCI DSS compliance?
Q6. How would you approach IT Security if you were not required to meet the PCI DSS? (Cisco 2011)
Q7. Were there areas of PCI DSS that you found more difficult to comply with and why? (Cisco 2011)
Q8. Are there areas of the PCI DSS which you believe need improvement and why?
Q9. How do you respond when you hear about a similar organisation that has experienced a security breach?
Q10. What are the benefits of PCI DSS to your organisation?
Q11. Do you think there are reasons that the PCI DSS is not adopted more widely?
Q12. How would you ensure that PCI DSS is adopted more widely?
Q13. Do you have any additional comments about IT Security or the PCI DSS?

In order to ensure clarity, the researcher adopted an approach summarising key responses to each question to the interviewee. These clarifications were phrased as, “Can I summarise your response as?” As suggested by Kvale (2007)., this ensured that each interview was of high quality as the approach ensured that the researcher had a full understanding of each response. It also ensured that the interviewer verified interpretations and that the interview could be “self-reported”.

As part of completing the interview participants were reminded that they could receive an electronic copy of the dissertation after its submission in September 2015. Participants were thanked for their contribution and time.

3.6.4 Transcribing

Thirteen interviews were undertaken as part of this research. One interviewee requested a copy of the interview transcript. None of the interviewees refused to be recorded. All interviewees requested a copy of the final dissertation.

The interview transcripts were read and compared against Kvale’s quality criteria for an interview (Kvale 2007). These criteria are as follows:

- “The extent of spontaneous, rich and specific answers from the interviewee.”
 - “The shorter the interviewer’s questions and the longer the participants’ answers, the better.”
 - “The degree to which the interviewer follows up and clarifies the meanings of the relevant aspects of the answers.”
 - “To what extent the interview is interpreted as the interview takes place”
 - “The interviewer attempts to verify his own interpretations of the subject’s answers in the course of the interview.”
 - “The interview is ‘self-reported’; the interview should not require additional explanation.”
- (Kvale 2007)

Interview transcripts once anonymised, were transferred to NVivo software for additional analysis.

3.6.5 Analysing

As suggested by Folkestad (2008) the qualitative interview data was analysed as a continuous process. This ongoing analysis required transcripts to be read several times as the researcher became aware of new insights into the qualitative data.

NVivo is software suitable for unstructured data analysis and is used in qualitative data analysis. This software was selected due to its intuitive interface allowing the researcher to spend as much time as possible analysing the data.

All transcripts were loaded into the NVivo software. Each transcript was read and each key sentence was coded using an open coding approach. At this first level of coding, distinct concepts and categories in the data were identified. These formed the basis for the initial data analysis. Once initial open coding was completed, an axial coding approach was then used (Creswell 2003). The concepts and categories identified from open coding were used while re-reading the text to confirm that the concepts and categories accurately represent interview responses and to explore how concepts and categories are related.

NVivo “tag clouds” were used to extract words repeated throughout the interview transcripts that were not identified by open or axial coding. Word clouds or tag clouds are graphical representations of word frequency that give greater prominence to words that appear more frequently in a source text. The larger the word in the visual the more common the word was in the document(s).

Tag clouds are useful in analysing qualitative data as they:

- Make an impact.
- Are easy to understand.
- Can be easily shared.

(Cidell 2010)

However, whilst a tag cloud is useful for clarifying findings, they do not analyse the data (Cidell 2010). The tag cloud in turn lead to further insights into the factors that influence an organisation’s adoption of the PCI DSS.

3.6.6 Verifying

“Without rigour research is worthless, becomes fiction and loses its utility” (Morse et al. 2008, p.2). “Research is only as good as the investigator. It is the researcher’s creativity, sensitivity, flexibility and skill in using the verification strategies that determines the reliability and validity of the evolving study” (Morse et al. 2008, p.17). As the interviews were conducted over several months, consideration was given to ensure that the interview approach, tone and data collection were carried out in a consistent manner. This was to ensure that findings could be more easily verified. The interviewer questioned the interviewees further by using probing questions like “is this true?” As suggested by Morse

(2008), validity was further ensured by interviewing different participants from across the PCI.

3.6.7 Reporting

Care was taken to ensure that all quotations did not refer to the interviewees or the organisations they represented. Care was also taken to ensure that all quotations were contextual. The analysis is presented in a “story format” to aid readability. Kvale (2007) highlights the importance of communicating findings in a scientific and ethical manner. He also highlights the need to ensure that the report is a readable product and that it is the personal output of the researcher. "The interview report is itself a social construction in which the author's choice of writing style and literary devices provide a specific view on the subjects' lived world" (Kvale 1996, p.235).

3.7 Lessons Learnt

The following section describe lessons learnt during the course of the research interview process.

As there were a limited number of interviewees, it was understood that the maximum benefit would have to be gained from each interview. In anticipation of this, trial interviews were undertaken to address any issues with the recording technology being used, the style/tone of questioning and to build up confidence in managing the interview process.

Despite these trial interviews, the initial interviews were not as valuable as subsequent interviews. This issue arose as a result of the interviewer's lack of confidence and lack of experience in carrying out research interviews. In initial interviews the interviewer was uncertain how to ask additional probing questions which may have resulted in some details not being fully uncovered. However, each interview built on the knowledge gathered from the previous interviews.

As the later interviews were more detailed, follow-up questions were also asked of the early interviewees to ensure that all participants were asked the same questions e.g. “Did interviewees have any contact with the PCI council in relation to PCI DSS?” or “Had they ever been asked for input into enhancing the standard?” This resulted in a more comprehensive insight into the research question and highlighted key insights not previously considered.

As requested by some interviewees, a number of interviews were conducted using Skype. As a result some of the visual interaction between the interviewer and the interviewee was lost as the interviewer was not able to interpret the body language of the interviewee. As a result some details may not have been fully uncovered. In each instance, face-to-face interviews were found to be a more complete interview where more probing questions were asked when compared to telephone or Skype interviews.

4. Findings and Analysis

4.1 Introduction

The following chapter analyses the qualitative data from interviews which were conducted with participants who are part of the PCI. The interviewees consisted of the PCI SSC, acquirers, level one merchants, PSPs and other members of the PCI. The following section will analyse the organisation, the organisational culture in relation to Information Security and other considerations that arose from the interviews in relation to factors that influence the adoption of the PCI DSS.

4.2 Findings

4.2.1 Introduction

The following tag cloud represents the frequency of words used by interviewees and displays them graphically. These key words define the context for the subsequent analysis.



FIGURE 4.1 – Qualitative Data Tag Cloud

4.2.2 The Interviewees

There were thirteen interviewees who took part in in-depth one-to-one semi-structured interviews. The interviewees were selected from a cross section of the PCI. The

interviewees represented CEO's, CFO's, CTO's, CISO's, Company Directors, IT Systems Managers, Compliance Officers and PCI DSS QSAs. A common trait across all the interviewees was that they all were interested in the broader area of IT Information Security.

The organisations that the interviewees represented are as follows:

- One of the interviewees is an employee of the PCI Council, who actively maintain and evolve the PCI DSS on behalf of the major card schemes.
- One of the interviewees represented acquirers. These acquirers have the responsibility of ensuring that the merchants maintain the appropriate level of compliance with the PCI DSS.
- One of the interviewees represented web hosting companies. Web hosting companies are often certified with a wide range of security standards to ensure that their customers can demonstrate to their respective auditors that the hosting companies operate in a secure manner on behalf of the merchant.
- Two of the interviewees represented an auditing firm who specialise in Information Security services and have a division that specialises in PCI DSS compliance and auditing.
- Eight of the interviewees represented merchants and service providers who are required to be PCI DSS Level one compliant.

4.2.3 Organisational view of the PCI DSS

The organisations that took part in this research came from a diverse background.

The PCI is composed of the card schemes, the PCI SSC, acquirers, merchants and auditors (see section 2.3). Careful consideration was given to selecting organisations that were representative of each area of the PCI (see section 3.6). Some of the organisations were large multinationals, some were indigenous Irish organisations. Other organisations had several thousand employees and others had several dozen.

All the interviewees observed that being PCI DSS compliant was a necessary cost of doing business. In each instance, there were commercial factors that required each organisation to achieve PCI DSS compliance. It was required by their acquiring bank, or was required by their own customers. None of the organisations undertook PCI DSS compliance as a security enhancement of their own accord.

Some of the organisations saw PCI DSS compliance as an opportunity to enhance the overall security of their IT systems. Other organisations saw no advantage to their business in achieving PCI DSS certification. One CEO commented,

"I am often confused by the inconsistencies of the PCI DSS, some banks want us to be compliant others don't. Some banks want us to be independently audited, some banks don't. It's all very inconsistent"

One interviewee commented,

"The PCI DSS is a good IT security baseline and it's good for our customers to know that we meet a recognised independent security standard".

Whilst another interviewee commented,

"If our customers didn't require us to be PCI DSS compliant, I wouldn't have a job here".

All of the interviewees described that their organisation had dedicated IT staff that ensured their organisation complied with the PCI DSS. The majority of interviewees agreed that merchants who did not have dedicated staff to manage the PCI DSS would find it difficult to comply it. One interviewee described,

"It must be a nightmare to comply with the PCI DSS if you are anything other than a level one merchant with dedicated staff to support compliance".

Many of the organisations invested significant resources in Information Security. These organisations appear to have embraced the PCI DSS as contributing of their overall Information Security strategy. They leveraged the cost and effort in becoming PCI DSS compliant to achieve efficiencies in other areas of IT. These organisations used the security principles of the PCI DSS across all areas of IT, even where cardholder data was not stored and PCI DSS was not strictly required. One interviewee stated,

"Having all our IT systems operate to the same minimum security standard makes life easier. IT developers, IT operations and all staff only have a single set of rules to use. There's no ambiguity as to what's in scope for PCI and what's out of scope for PCI. We treat all the IT systems the same. Monitoring systems, installing systems and upgrading systems and a lot of the day to day IT tasks are easier as a result of this consistent view of security".

Other organisations did not invest significant resources in Information Security. These organisations saw little value in the PCI DSS. One interviewee stated,

“Compliance is a pain”.

Two organisations opted to be certified at PCI DSS level one, the highest level of certification, as they believed the PCI DSS significantly enhanced their ability to attract new business. One interviewee commented,

“It’s better for our business that our customers see we take the security of their data seriously”.

As has been observed, none of the interviewees adopted the PCI DSS of their own accord. From the interview analysis, the reasons an organisation would adopt the PCI DSS were;

- It is required by the merchant’s bank.
- It is required by a customer contract.
- It is required by their industry, for example an acquiring bank or PSP.

The next section will analyse if the management of the compliance program within each organisation has any impact on the adoption of the PCI DSS.

4.2.4 Managing Compliance

Having analysed the interview data, it was observed that a range of different employees were responsible for managing or delivering the organisation’s PCI DSS programme. In some organisations, the management of PCI DSS compliance resided with the CFO or a dedicated compliance department. In other organisations, the CTO or IT Director was responsible for the management and delivery of the PCI DSS compliance programme. In one organisation, a company director was responsible for IT, PCI DSS compliance and also managed the relationship with the acquiring banks.

Larger organisations, with sufficient staff, tended to separate the roles of standards management and standards implementation. Several organisations valued a structure where those responsible for delivering the PCI DSS programme and those implementing the standard had separate reporting lines. These organisations also believed that this separation ensured that PCI DSS and other Information Security standards would be met in a consistent manner. When the interviewees were asked to explain why the role of

management of standards was separated from the role of implementing the standards one interviewee explained that,

“Foxes and hounds can become very good friends”.

The security consultants interviewed believed that those organisations that had no clear owner for PCI DSS compliance had more difficulty in meeting the standard. They further described their first task on engaging with a new customer as identifying who “owned” the PCI DSS compliance programme or agreeing with the customer who should “own” the programme.

All of the interviewees agreed that having a nominated person or department responsible for the PCI DSS programme made it easier to adopt the standard. Many interviewees suggested that the more senior the person responsible for the programme, the quicker compliance was achieved.

It has been observed that there are many approaches to managing a compliance programme. This research did not suggest a common approach to compliance management. However, the interviewees did highlight the need to have a nominated senior individual responsible for the PCI DSS programme. In the next section, the role and perceptions of the interviewees in relation to the adoption of the PCI DSS are examined.

4.2.5 Perceptions of the PCI DSS

The C-level executives interviewed who valued Information Security, valued the PCI DSS. Also, those senior executives that had a low appetite for risk described the PCI DSS as a good way to improve IT security and reduce risk of a card data breach. These C-level executives adopted the PCI DSS quickly in their respective organisations. One interviewee, who had a positive view of the PCI DSS estimated,

“Our private equity backers and our CFO have a very low appetite for risk. We see the PCI DSS as a way to reduce risk. I don’t want to be the CEO that wakes up on Monday morning only to read that our customer credit card details are all over the Internet”.

Another said,

“The initial PCI DSS compliant release of our software was only six months in development”.

Many of the interviewees had previous experience of the PCI DSS, risk management, health and safety or other compliance standards. Those interviewees that held senior management positions and had previous experience in standards adoption were also the organisations that adopted PCI swiftly.

The less senior interviewees, who did not have previous experience of the PCI DSS or of other standards were also in favour of the PCI DSS. One Systems Administrator, with little experience of other security standards, commented,

“If someone was to ask me to come up with a good way to ensure you have a good security posture, I’d say that the PCI DSS would be a good standard to work to, even if you didn’t touch a single credit card.”

Another interviewee, when asked if he believed being compliant with the PCI DSS made his organisation more secure he responded,

“I suppose it can be used as a tool to enhance security. But by itself it doesn’t. Like any tool, it can be misused”.

Eight of the interviewees believed that the PCI DSS was a strong basis on which to build a comprehensive Information Security model. One interviewee described that the core principles, which are critical to the PCI DSS, should be applied by organisations to all data, not just cardholder data. The interviewee explained,

“We tend to generalise the principles. We try to handle all data as if it was broadly speaking like cardholder data. So that means, gift cards get handled as if they were credit cards. Debit cards are the same. We want to keep the best practice aspects of PCI. It means less strangeness, more common code parts, easier audits. For our own purposes we can actually be sure that there is unlikely to be fraud on gift cards or employee fraud on gift cards because they can’t decrypt them.”

The interviewees agreed that complying with the PCI DSS made their organisations more secure and less likely to suffer a card data breach. However, the interviewees suggested that this is only true where the PCI DSS is seen in a positive manner contributing to an overall Information Security standard. The interviewees suggested a clear distinction between organisations adopting the principles of the PCI DSS being less likely to suffer a

breach and those organisations who see the standard as a constraint on the development of their organisation.

All of the interviewees strongly argued that complying with the PCI DSS did not mean that the organisation's IT systems were completely secure. All of the interviewees agreed they were less likely to experience a data breach but that they all believed their organisation could suffer a breach in the future.

In general, most of the interviewees believed that the PCI DSS was a security standard that improved their organisations Information Security. However, one interviewee saw the standard as a tool, which if not used properly, would not enhance the security of an organisation. The next section considers organisational culture. This section is closely linked to the interviewees, as those interviewees with more senior positions within their organisation often dictated the entire organisations view of Information Security and the PCI DSS.

4.2.6 Role of Organisational Culture

Each of the interviewees described a different culture in their organisation with regard to Information Security. There were three discernible cultures. The first was where C-level management had a positive view of the PCI DSS and of Information Security. The second was where some C-level management viewed PCI DSS positively and some viewed it negatively. The third was where C-level management viewed the PCI DSS negatively.

Those organisations, whose C-level managers had previously held positions where Information Security was valued, continued to see the value of operating secure IT systems and to value the PCI DSS. One interviewee described that all the key owners of the business were,

"Positively aligned in relation to standards adoption".

This organisation readily implemented the PCI DSS and other standards required by their industry. This organisation quickly adopted the PCI DSS as compliance was seen as necessary to develop and grow their business. The culture of Information Security, which was encouraged by C-level management, was instilled across the entire organisation. Another interviewee described that his organisation, with a positive approach to Information Security,

“Welcomed the enhanced security that complying with recognised standards, brought the organisation”.

The second culture identified was where some C-level executives held differing views on the value of the PCI DSS. These C-level executives saw complying with the PCI DSS as a barrier to productivity and as,

“Someone else’s problem”.

This organisation has, as a result, only implemented the PCI DSS in the minimum required areas of its IT systems.

This interviewee also cited the recent Irish economic recession as a key factor why his organisation had not invested more widely in Information Security. Investment in additional Information Security had not been undertaken, but his organisation continued to invest in PCI DSS compliance. This was despite pressure from co-owners to reduce operational costs within the business. The interviewee further described that as the Irish economy has started to recover, his organisation is now actively investing in additional security initiatives. He explained that the organisation recently started implementing the ISO 27001 standard. The ISO standard was being implemented by this organisation to compliment the PCI DSS compliance that was already held. The ISO standard will

“Force other areas of the business, not covered by PCI DSS, to come to a similar standard”

The interviewee also described that standards adoption was being used as

“A lever to ensure that all IT systems became more secure”.

This interviewee, as a part owner of his organisation, championed the program for PCI DSS. It was his seniority within the organisation that ensured that compliance with the PCI DSS was achieved despite lack of support from other co-owners. As a result of the focus on achieving PCI DSS compliance, this organisation also adopted the standard quickly.

The final culture identified is characterised by an organisation whose senior management see limited value in Information Security and the PCI DSS. One interviewee described,

"The attitude of senior management in here, I wouldn't say was anti-PCI DSS, but they see it as a cost and as something to be overcome as opposed to be something that could be of benefit to the company".

He also described that his organisation placed limited value on Information Security and little value in the PCI DSS. On several occasions, he described the organisation as,

"Very cost focused".

The interviewee described it as a very difficult experience to introduce the necessary improvements to IT processes and procedures, required under the PCI DSS. The interviewee described in detail that he had little support from C-level management and little authority to improve security outside of the limited number of systems covered by the PCI DSS. The interviewee commented that he was often seen as,

"The guy who has to say 'No', it can't be done in that way as it doesn't meet the requirements of the PCI DSS, we should meet the customer requirement this way which will address PCI DSS concerns".

As a result, he believes he is seen as,

"Not being a team player".

However, he strongly believes he has the best interests of the organisation at heart by ensuring their obligations under the PCI DSS are met.

This organisation took the longest to achieve compliance with the PCI DSS. This interviewee also described that the PCI DSS was only applied to the minimum number of IT systems to reduce IT costs. As a result of aggressively managing these costs, other areas of the organisation's IT infrastructure were not secured to the same standard as those systems covered by the PCI DSS. When asked why other systems were not secured in a similar manner, the interviewee responded,

"The value of IT security can't be quantified".

As a result, those systems are less secure. The interviewee believes that he will continue to encourage the adoption of the security principles of the PCI DSS in all areas of the

business. However, he believes the PCI DSS or other security standards are unlikely to be adopted more widely in his organisation. This is due to cost factors and the perception that the PCI DSS and enhanced Information Security reduces the organisation's ability to respond positively to customer requirements.

It has been observed that the organisation's culture is a key factor in determining an organisation's response to the adoption to the PCI DSS. Those organisations who value Information Security appear to have readily adopted the PCI DSS. Additionally, those organizations whose C-level executives view Information Security in a positive light also appear to have readily adopted the PCI DSS. Interviewees employed by organisations that have not invested in Information Security describe it as a very difficult experience in achieving PCI DSS compliance as they do not have the appropriate support and encouragement from C-level management. The next section will consider the interviewees IT systems and assess if there are any technology related decisions that might impact the adoption of the PCI DSS.

4.2.7 Role of Technology

Just as each organisation had no common organisational structure in relation to managing their respective PCI DSS programmes, neither did they have a common approach to technology.

One interviewee described that whilst his organisation developed their own software, in order to reduce the overall operational costs of IT, he outsourced his IT infrastructure requirements to third parties. As a result, his organisation was an early adopter of cloud-based services where he benefits from Infrastructure as a Service "IaaS". By comparison, the majority of interviewees owned and managed their own IT infrastructure. Several interviewees described that their organisations owned and operated all the technology necessary to run their businesses and they were dependent on a limited number of third parties. As a result, they believed they had more control of the security of his systems. One interviewee commented,

"I only have a limited number of people to worry about who have access to cardholder data they all work for my organisation and we all have the same security culture".

Some interviewees built their technology with PCI DSS and other security standards in mind. These organisations achieved compliance with the PCI DSS more quickly when compared to organisations that had to retrospectively introduce the PCI DSS into their

technologies. Those interviewees who designed their software / infrastructure with PCI DSS in mind achieved compliance within six to twelve months. Other companies who had pre-existing technologies took two to three years to achieve compliance. One interviewee described his technology as being, an older system, which was not initially designed with the PCI DSS in mind. This interviewee's technology was initially developed in 2000, prior to the existence of the standard. While the technology had many security features, significant IT development and infrastructure enhancements had to be carried out, at various times, to ensure that the technology continued to meet the requirements of the PCI DSS. The interviewee suggested that several areas of the technology stack had to be re-written to address the requirements of the PCI DSS. This interviewee's organisation took the longest to achieve compliance with the PCI DSS.

Whilst there were no common technology decisions in relation to the factors influencing the adoption of the PCI DSS it was observed that the timing of the initial development of the organisation's IT systems was a factor in the overall cost of meeting the requirements of the PCI DSS. Those organisations who had older IT systems, which were developed prior to the standard being implemented in 2004, took longer to adopt the standard and incurred greater costs in ensuring the requirements of the PCI DSS were met. Those IT systems that were developed after 2004, which included the requirements of the PCI DSS in the initial design, adopted the standard more quickly and at a lower initial cost. However, no technology had a significant advantage when subsequent changes or enhancements to the PCI DSS were considered.

Having considered the organisation, the culture, the staff and the technology, the following section will consider the role of the PCI DSS auditor and what impact their role might have on factors influencing the adoption of the PCI DSS.

4.2.8 Role of the Auditor

Many of the merchants interviewed described that they had a close relationship with their PCI DSS auditors. In several instances, this relationship had evolved over many years.

The majority of the merchants interviewed agreed that the relationship with their QSA was key to their success in achieving compliance with the PCI DSS. One interviewee explained,

"I consider the QSA as being an extension of our IT department and a valued member of the team".

Many of the merchants interviewed received multiple additional services from the same Information Security firm. These services included QSA services and they also received a mixture of the following;

- PCI DSS consulting services.
- Website security penetration testing services.
- Managed services.
 - Secure log management services.
 - Software analysis software.
 - Website monitoring services.

Whilst interviews with merchants suggested strong relationships with their QSA, the interviews with the PCI Council, the acquirers and three merchants suggested a concern related to the rigour of the PCI DSS audits carried out by QSAs. These interviewees raised concerns about the accuracy of a QSA's interpretation of the PCI DSS and the commercial relationship that the QSA had with the merchant. One interviewee explained that the PCI DSS is often open to interpretation. In some instances, what one QSA considers acceptable in meeting the PCI DSS another QSA may not. The QSA's interpretation of the standard may result in merchants receiving incorrect advice on how to comply with the PCI DSS. When this concern was raised with the QSAs they agreed that this scenario could occur. The QSAs further described that within their organisation, when confronted by an unfamiliar situation / technical scenario, they often sought consensus amongst fellow QSAs to mitigate these customer concerns. The QSAs believed that this consensus based approach, based on the wisdom of crowds, should reduce the chances of inaccurate advice or misinterpretation of the PCI DSS occurring.

One interviewee described a scenario where two different auditors, from the same auditing firm, certified his organisation as PCI DSS compliant in year one with QSA "A". The following year, QSA "B" raised a number of serious concerns which QSA "A" had previously accepted as complying with the PCI DSS. Similarly another interviewee described engaging a new QSA who identified a serious security vulnerability, which previous QSAs had failed to identify. When the QSAs were questioned about this issue, they responded that consistency is always a concern for QSAs. The QSA's suggested that,

"The standard is a lot better with version 3.0 and now version 3.1. I think prior to version 3 there were a lot of opportunities to fudge answers. It is now very difficult to misinterpret a question. The ROC requirements are now also very explicit."

Both QSAs agreed that they had experienced audit consistency issues as they worked with different customers. The QSAs believe that recent changes in the PCI SSC where QSAs are randomly and periodically audited should reduce the chances of these issues occurring. The QSA described a recent 2014 audit as follows,

“They [The PCI SSC] examined my recent ROC’s. They went through each item of the ROC, questioned me and suggested I should also check this and I should word this finding differently. I actually found it very useful. I am always happy to be reviewed as it improves customer’s confidence in the PCI DSS”.

In addition, both QSAs agreed that the latest version of the PCI DSS 3.1 made it less likely that inconsistent interpretations of the PCI DSS would arise. They ascribed this to the significant amount of additional documentation that QSAs now need to provide and the improved wording of the PCI DSS version 3.1.

One interviewee defended the quality of QSA audits by comparing a QSA audit to other audits which the interviewee had participated in. The interviewee explained,

“On occasion, I have had to explain to some types of auditor what a Unix operating system is. I have seen auditors that just read from a list, provided by someone else. They have no real IT experience. At least QSA’s have IT experience and were previously developers or systems administrators before they became auditors”.

It is clear that there is a close relationship between the auditor and the merchant. The quality and diligence of the auditor is key to ensuring a comprehensive audit is carried out. Due to lack of clarity and poor structure of earlier versions of the PCI DSS it is apparent that errors have been made and incorrect compliance decisions have been uncovered. However, recent versions of the PCI DSS appear to have addressed many of these concerns.

4.2.9 Role of the Acquirer

As has been observed, the acquirer is responsible for ensuring that the merchant attains the appropriate level of PCI DSS certification. The acquirer is also tasked with ensuring that the PCI DSS is administered on a day-to-day basis.

Several interviewees raised concerns about the implementation, operation and management of the PCI DSS by the acquirers. These interviewees argued that the relationship between the acquirer and the merchant is subject to rent seeking behaviour.

One interviewee suggested that if acquirers actively pursue their merchants to attain PCI DSS compliance, the merchant might move their business to an alternative acquirer.

Several interviewees believe that merchants actively seek out acquirers who do not require their merchants to achieve PCI DSS compliance. One interviewee suggested that an acquirer, in an attempt to maintain business with a merchant might agree a “long-term compliance programme” with a merchant. The interviewee described that in these situations compliance will be attained via a PCI DSS compliance project lasting several years. During this period, the merchant will not be compliant, but the acquirer will offer payment services to the merchant due to the size of the merchant’s business. The acquirer has won a new customer; the customer is processing payments and the acquirer gains financially from this new customer’s business. There is no risk to the acquirer as under the PCI DSS the merchant bears all the costs associated with a data breach. The merchant may be willing to take the risk of non-compliance, as they can potentially defer the costs of compliance for several years.

It is apparent that the role of the acquirer in administering the PCI DSS is key in the relationship between the merchant and the acquirer. It is also apparent that commercial factors may supersede the acquirer’s obligation to ensure the PCI DSS is properly administered.

4.2.10 Recent Breaches

All of the interviewees were aware of recent IT security breaches. The majority of interviewees detailed that when they became aware of a security breach that they considered if their own organisation was potentially vulnerable.

One of the interviewees discussed the Loyaltybuild breach. It was clear that careful consideration had been given to the causes surrounding the Loyaltybuild breach and that the incident had been thoroughly risk assessed in relation to the interviewee’s organisation. The interviewee described how he had researched the nature of the breach and using a risk based approach, considered if his own organisation might be exposed in similar ways.

Another interviewee discussed the Target data breach and how his organisation actively considered not only PCI data breaches, but all types of data breach. This interviewee described that he was frustrated that technical details, related to specific breaches were often not disclosed as a result of legal proceedings following a breach. As a result,

“Any potential Information Security benefit from identifying security vulnerabilities, which could have been identified by analysis of the data breach would be lost”.

The interviewee further described

“Responding to security issues often has a time dimension associated with it. It’s often crucial to identify a vulnerability quickly and develop a patch or enhanced security procedure to mitigate its impact to IT systems”.

If that information on the breach is not disclosed, its value to the wider IT community is lost.

The same interviewee suggested that as the PCI DSS is enhanced based on data gathered from recent breaches, that anonymised technical details related to breaches should be disclosed. This, he argued, would give maximum benefit to the security community and minimise any impact to pending legal proceedings.

4.2.11 Data Protection

The interview with the PCI Council detailed that the role of the DPC and the role of the PCI SSC are often aligned. The DPC is primarily focused on protecting personal data whilst the PCI SSC is focused on card data. This topic was discussed with both merchants and acquirers. The merchants believed that if they suffered a breach, that they would be more concerned about the response of the DPC than they would about the response of the PCI SSC. One interviewee offered,

“My concern around the whole security piece is actually data protection”.

The merchants believe that the Irish DPC has greater power to impact their business and is more likely to respond to a security breach when compared to the PCI SSC. They also believe that penalties and fines from the DPC are more likely than penalties and fines from the PCI SSC. Again, interviewees referred to the example of Loyaltybuild where the DPC took action against Loyaltybuild following their data breach.

The merchants were also aware that pending European legislation relating to data protection might impact their business operations to a greater extent than the potential impact of complying with the PCI DSS. One merchant is implementing ISO 27001 to address these concerns. He described it as follows,

“This is where we’re again looking at the whole ISO 27001 piece and the general need to comply with data protection legislation can all be done with one sweep”.

As the DPC regularly disclose their findings on national media, the following section will assess the impact to an organisations brand in relation to a breach and factors that may influence adoption of the PCI DSS.

4.2.12 Impact on Brand Identity

All of the merchants operated in e-commerce businesses where payment processing is their sole source of revenue. Without payment processing facilities, these organisations would cease trading.

Each organisation had differing views in relation to the impact a disclosed data breach would have on their brand and the organisation’s ability to recover from a negative customer reaction to a disclosed data breach. One CEO described,

“If we get fined by the PCI SSC, we have a bad year, profits are impacted, but we’ll continue. If we have a negative customer response to a breach and the brand is damaged, we might never recover”.

This organisation described itself as risk averse and had a positive view of the PCI DSS and Information Security.

Another interviewee described,

“If we had a breach, the impact to our trading relationship with those key customers could be damaged very badly. That would not be good news economically for the company. So, what the PCI DSS does, it gives our customer a degree of comfort. We are following the standard that’s required by the recognised authority”.

It has been observed that the potential damage to an organisations brand is of greater concern to C-level executives than the potential impact of a fine or other penalty from the PCI SSC should a breach occur. In the following section, other potential impacts will be considered in terms of the DPC and how its reaction to a security breach may impact organisations adoption of the PCI DSS.

4.2.13 View of the PCI DSS

All of the interviewees view the PCI DSS in a positive light. However, as has been observed this positive view is dependent on the culture of the organisation. All of the interviewees broadly agreed that adopting the PCI DSS would reduce card fraud. However, all the interviewees agreed that there are issues with the standard which need to be addressed if the standard is to be widely adopted. There are several perceived advantages and disadvantages to being compliant with the PCI DSS. The interviewees were asked for their opinions on the advantages and disadvantages (see section 2.7).

4.2.13.1 Costs & Effort

All of the interviewees agreed that complying with the PCI DSS resulted in significant costs. These costs were accepted as necessary and were factored into annual budgets. Some interviewees suggested that in the current economic climate that they had considered reducing their expenditure on some areas of Information Security. However, the interviewee's organisations had not reduced expenditure on their PCI DSS compliance programmes.

Some interviewees thought that the cost of audit services were too high, relative to the value it brought to their organisation. One interviewee described the costs of a PCI DSS level one audit,

"As a little bit crazy. The reason why is because there's huge costs attached to PCI DSS. The money is crazy, €16,000 to €20,000 for an audit".

This same organisation ascribed limited value the PCI DSS in terms of enhancing the security of card data.

One organisation described that they spend approximately €50,000 - €60,000 per annum on auditing and security penetration testing. The interviewee in question described this as a necessary cost, and believed that there was sufficient competition amongst auditing companies to keep costs competitive. The same interviewee further argued that if costs got too high, his organisation could readily obtain auditing services from several other companies.

4.2.13.2 Communication

Communication between all stakeholders in the PCI was repeatedly raised by interviewees as an area of concern.

One interviewee described that the PCI SSC was making efforts to improve communication between the different stakeholders in the PCI. She explained that seminars, extensive online documentation and an active communications programme were in place. These documents, seminars and communications programmes are dedicated to assisting organisations in adopting the PCI DSS and to keep merchants updated on changes to the standard. However, none of the merchants had ever participated in an event organised by the PCI SSC.

However, one interviewee described a recent attempt to communicate with the PCI SSC as frustrating as he waited several months for a response to a question on an upcoming enhancement to the DSS. The interviewee stated,

“So my last email to them [The PCI SSC] was when the new P2PE standard is coming out. I wait and wait and wait and wait. I receive a reply, ‘hoping to have it out in June’. I respond, ‘Can I get my name on an announcement list?’ Then radio silence. I mean, maybe I am doing it wrong. Why wouldn’t they just answer?”

All the merchants described that they had reasonably good communication with their acquirer in relation to the PCI DSS. However, the merchants described that they had almost no relationship with the PCI SSC.

4.2.13.3 Language

One interviewee described that an area of concern for the PCI SSC was in relation to localised translations of the PCI DSS. She described the issue as follows,

“The language is an issue for a lot of people. The standard is a global standard, but there are a lot of merchants where English is not their first language. If they are Polish / German merchants they say, ‘give us our version of the standard’. But because the standard is complex written instructions, translating to other languages may lose the nuances of the language on their own. So it needs to be written in English. We do have translations on the site, but the main English one is always the one that’s used. You cannot rely on the local translated version. We get feedback from industry what we wrote isn’t what we intended and we change it to make it clearer”.

The interviewees were asked about the clarity of language in the standard. The language was often described as vague, confusing or ambiguous. Several interviewees described having to read supporting documentation to gain a full understanding of the requirement. Other interviewees asked their QSA for guidance on certain items. The QSAs interviewed

also described having difficulty interpreting the language in the standard. They both explained that they augmented the PCI DSS with additional documentation provided by Visa. They explained that despite being a core member of the PCI SSC, Visa continue to maintain a large amount of comprehensive standards documentation independent of the PCI DSS. The QSAs stated that in many instances, the Visa documentation was clearer and more precise when compared to the documentation in the PCI DSS. When they were asked why the Visa documentation is clearer they suggested that the PCI SSC has to balance the needs of all the five major card brands which might lead to requirements being softened or being overly complicated in the DSS.

However, the majority of the interviewees did note a significant improvement in the clarity of the language used in PCI DSS v3.0 and subsequently in PCI DSS v3.1.

4.2.14 Marketing Compliance

All the merchants used their PCI DSS compliance status to attract new business. However, when asked if they actively marketed their compliance with the PCI DSS on their websites, all the merchants advised that they did not actively advertise their compliance status with logos or other references to the PCI DSS. They believed that it was likely to raise their profile amongst hackers and make them a potential target for hacking. One interviewee stated,

"I'll never show it. I don't need to attract attention".

Further questions were then asked probing the inconsistency between these merchants being compliant with the PCI DSS level one with an associated higher level of security versus their reluctance to publicly advertise this compliance. Both merchants responded that despite being compliant, compliance did not guarantee their security and they did not want to attract or have to deal with a potential cyber-attack.

By comparison, the ISP interviewed actively promoted all their certifications as they believed it was required to attract new business. One ISP, as in FIGURE 4.2, lists 6 different certifications from ISO27001, PCI DSS to environmental management certifications as ways of attracting new business.



FIGURE 4.2 – Service Provider List of Certifications

4.2.15 Further Enhancements

All of the interviewees agreed that the standard needs to continue to be prescriptive in nature. One interviewee suggested that the prescriptive nature of the standard is one of its key advantages over other IT security standards.

The PCI SSC bases DSS enhancements on information sourced from actual breaches. The interviewees suggested that the PCI SSC need to constantly enhance the standard to keep it up to date and ensure that merchants are protected from the latest threats. Several interviewees agreed that in the past the PCI SSC might not have responded quickly enough to recent IT security vulnerabilities being announced to ensure that merchants were protected. One interviewee, whose technology systems are hosted by a cloud services company, found it very difficult to achieve compliance with the PCI DSS. When his

organisation began their program to become PCI DSS compliant the PCI SSC had not published recommendations on how to achieve compliance in the cloud.

The PCI SSC also agreed that they had been too slow to respond to significant security events in favour of publishing the agreed upgrade to the standard every two years. One interviewee described it as follows,

“The PCI DSS has to evolve, it constantly has to evolve. It’s something we got as a serious wakeup call with the SSL scare. So the new version of the standard came out in January and then in June which you know, we went to PCI 3.1 in less than 6 months”.

Several interviewees stated that the recent upgrades to the standard from version 3.0, launched in early 2015 to version 3.1 in April 2015 reflected the SSC’s changing response to being more proactive in reflecting the rapid changes in the security vulnerability landscape.

One interviewee believes that future versions of the PCI DSS will require all merchants to use tokenisation services. He argued that merchants should focus on their core business. The merchants should de-value their card data by replacing it with tokens. The payment card storage should be centralised with specialist firms whose purpose is to secure the card data. This will allow merchants to focus on growing their business and not on securing data.

Several interviewees stated that the PCI DSS focused on a wide range of security related risks and was to be commended for its prescriptive approach to card security. However, they also stated that the standard focused, inappropriately on specific areas. As the conversation evolved, one interviewee described his frustration in relation to the latest version of the PCI DSS, version 3.1 and its focus on documentation. Extensive additional documentation is required to comply with PCI DSS 3.1, which has not been required in earlier versions of the standards. The interviewee argued that the PCI DSS should focus on preventing breaches and improving requirements around prevention and detection as opposed to documentation.

4.2.16 Summary

Overall the interviewees see the PCI DSS as a valuable standard in minimising the chances of suffering a data breach and improving the overall security of IT systems. However, the relevance of the PCI DSS in an organisation depends on the organisations overall view of IT Information Security. An organisation’s approach to IT Information Security is often based

on its overall culture. This culture starts with the C-level management of a firm and is then reflected within the rest of the organisation.

Obtaining PCI DSS compliance is a difficult undertaking. It can cost significant amounts of time, financial investment and dedicated IT staff to ensure compliance is achieved and maintained.

The PCI DSS is a complicated standard which can be difficult to understand and if interpreted incorrectly can have negative consequences for the business.

The PCI DSS is still evolving, recent revisions of the standard appear to have made significant improvements in terms of clarity and appear to be encouraging a stronger security stance amongst merchants. It is clear that recent high profile security incidents have prompted the PCI SSC to update the standard more frequently.

The PCI SSC are attempting to improve communication amongst all stakeholders within the PCI. However, to date this research suggests that merchants are still unaware of many of the initiatives which the PCI SSC are undertaking to improve security within the industry.

This research suggests clear distinction is emerging between the PCI SSC and their operation, management and evolution of the PCI DSS and the standard itself. It appears that organisations value the PCI DSS but have concerns about how the standard is being managed by the acquirers and the PCI SSC. They are concerned about the potential conflict of interest between merchants and acquirers. There are concerns where the acquirer is mandated to ensure the merchant is PCI DSS compliant but where the acquirer also benefits from the revenue the merchants brings irrespective of PCI DSS compliance. Significant merchants may pressure their acquirers to not mandate them to become PCI DSS compliant thereby potentially undermining the PCI. Concerns have also been raised in relation to QSA's and their ability to remain objective when auditing a customer and also being paid by the customer to carry out the audit. Again, this may ultimately undermine the entire PCI DSS.

These concerns will be analysed in the next section as it is these issues which appear to influence an organisations adoption of the PCI DSS.

4.3 Critical Analysis and Discussion of Interview Findings

There were several key findings which emerged from the qualitative interview analysis. In the next section these findings will be related to previous research and critically analysed.

There are several aspects of this research which are closely connected. The interviewees and existing research agree that the PCI DSS is a good approach to reducing fraud in the payment card industry (Rees 2012; Coburn 2010; Blackwell, Cian & Gahan 2009). This and existing research suggest the benefits of complying with the PCI DSS are greatest when part of a broader IT governance model (Kedgley 2014; Oosten et al. 2014). By contrast, this and other research suggests that the PCI DSS does not help building a “comprehensive security program” (Oosten et al. 2014, p.8). Organisations correctly interpret the PCI DSS as a compliance standard which applies to those IT systems that process or store card holder data (see section 1.1 and 2.5). In most e-commerce systems, the number of systems that the PCI DSS applies to may only be a fraction of the total IT infrastructure. As a result, if the PCI DSS is adopted in isolation, without additional standards applied to other IT systems, it is reasonable to assume the PCI DSS systems will be more secure than others. As the PCI DSS compares favourably to other standards like COBIT and ISO (see section 2.9.4), if the PCI DSS was adopted across all systems or in conjunction with another standard, as is the case with some interviewees (see section 4.2.6), it is reasonable to believe that an organisation would have a very comprehensive and mature hybrid IT governance model in which to securely operate their IT systems. The use of the PCI DSS across all IT systems or a hybrid model where both the PCI DSS and other standards are used is an approach which was observed in this research in organisations that have a positive view of Information Security (see section 4.2.3 and 4.2.6). It is clear that some organisations, who place a lower value on Information Security adopt a minimalist approach to the PCI DSS. In these organisations, the PCI DSS is applied to to a limited set of IT systems. However, given the significant dependence of e-commerce organisations on their technology (see section 4.2.12) it is surprising to think that organisations will still use a minimalist approach to the PCI DSS.

This research has found that the language in the standard is complex and in previous versions was also confusing. This is consistent with findings from several different researchers (Rees 2012; Ponemon Institute 2011b; Varian, Foster *et al.* 2009). This research suggests that the complicated language is a contributing factor to the lack of adoption of the PCI DSS as organisations struggle to understand how to implement the PCI DSS. There has been an effort within the EU to make legal documents, mortgages,

insurance policies easier to understand (Weiss 2011). It appears that the PCI DSS is adopting a similar approach (see section 4.2.13.3). The current version of the PCI DSS seems to be easier to understand, but the positive impact of this will only become evident in the coming twelve to eighteen months as organisations complete their first audit cycle with the PCI DSS version 3.1.

This research highlights the need for dedicated IT staff to ensure compliance (see section 4.2.3). It also suggests that QSA's are often used to help interpret the requirements of the standard (see section 4.2.8). Needing additional IT resources and additional consultancy results in increased costs. It has been demonstrated that the cost of adopting the PCI DSS is a significant cost for some organisations (see section 4.2.6). This finding is also consistent with existing research (Rees 2010; Hovav & Gray 2014) (see section 2.8.2). The fact that researchers and interviewees both highlight cost as a concern suggests that they believe these costs can be reduced. This may be linked to why none of the interviewees undertook the PCI DSS of their own accord. It also suggests organisations do not view comprehensive IT security as a requirement within their organisations and will only implement improved security measures if required to do so by others. Given the significant weight all interviewees placed on the cost of implementing and maintaining the standard, this is seen as a key reason that the standard is not adopted more widely.

Whilst one interviewee suggested ways in which to reduce costs, the existing research has suggested several financial incentives to reduce costs and make adopting the PCI DSS more cost effective. These are highlighted in section 2.8 (Segal et al. 2011; Cohen 2014; Sullivan 2014) and in section 2.11.1 by Chen (2012). As current rates of adoption of the PCI DSS are low, reducing the costs of compliance may be a positive way in which to incentivise organisations to adopt the standard. However, a cost reduction incentive is unlikely to happen as any financial incentives to increase rates of compliance would have to be funded by the PCI SSC and as it has already been observed the PCI SSC actively push all costs of compliance back to the merchant (see section 2.8.2).

The interviewees suggested that if they did experience a breach they would probably identify it quickly as a result of complying with the PCI DSS (see section 4.2.10). This is consistent with existing research carried out by O'Raghallaigh (2010). However, the interviewees belief of quickly identifying a breach contradicts several examples of recent breaches (see section 2.4). Several breaches in section 2.4 went un-detected for several months. This research further suggests that early detection of a breach is only possible

where the PCI DSS is part of a businesses usual activities which was also suggested by Kerner (2013) (see section 2.8.1). It is important to note that detecting an attack is closely linked to PCI DSS section 10, which has been shown to be difficult to comply with (see section 2.4.6 and 2.8.1). It is therefore possible that the organisations, who are PCI DSS compliant could be under a false sense of security in terms of identifying an attack. This is backed up by the comments of one interviewee whose organisation is PCI DSS compliant,

“How can I be absolutely sure I am monitoring the right stuff? What should I monitor? I can’t monitor everything. I look at the logs, I make a judgement call”.

This might be a strong reason to consider carrying out audits more frequently as was suggested by Sullivan (2014) (see section 2.9.2).

It is surprising that basic security issues continue to be a cause for concern given the wide focus that security breaches now receive in the media (see section 2.4). This analysis suggests that end user education is a key issue yet to be addressed by the PCI DSS. One interviewee, raised similar concerns as existing Verizon (2014) research (see section 2.4.6). One interviewee said,

“I ask new staff how often they change their passwords for things like Gmail or Facebook. They never change them. I also ask them if they ever change the PIN code on the ATM cards, same answer”.

This highlights a concern that despite the current requirement to educate users, existing training may not be effective and increase the risk of a data breach.

It has been observed in this research that C-level executives are more concerned about the potential damage to their brand than the potential fines from the PCI SSC (see section 4.2.12). These executives are also more concerned about the potential impact to their organisations of the DPC than the PCI SSC (see section 4.2.11). This may be related to the current situation where the DPC actively publishes details of fines and penalties whereas the PCI SSC do not. Deterrence theory (see section 2.11.1), as suggested by D’Arcy (2009), could be effectively employed to enhance adoption rates of the PCI DSS. If there is a fear of damage to a brand it is apparent that companies will respond and adopt the standard. The PCI SSC should consider making breach announcements mandatory. They also have to consider publishing their fines, assuming that the value of the fines are sufficiently large to encourage organisations to adopt the PCI DSS. However, this is unlikely

to happen. Analysis of existing breaches suggests that financial settlements are made on a regular basis between the PCI SSC and the breached merchants as was observed in the Target and TJX breaches (see 2.4.2 and 2.4.4). These fines are unlikely to be large enough to encourage adoption of the PCI DSS when current research suggests the cost of the fines are too low (see section 2.9.2). The respondents to this study were also of a similar opinion.

The positive impact of trust assurances is often reported as a way to improve the adoption of the PCI DSS (see section 2.9.3) (Kim & Benbasat 2010; Kaplan & Nieschwietz 2003). This research contradicts this. The interviewees argued that they would not place PCI DSS logos on their websites for fear of attempted breaches taking place (see section 4.2.14). Neither Kim nor Kaplan considers the potential increased likelihood of cyber-attack as part of their research. Considering that C-level management are sensitive to the impact a breach may have on their brand (see section 2.8.2) it is reasonable to expect that PCI DSS logos are unlikely to be used as a trust assurance on e-commerce sites.

Most of the interviewees agreed that the PCI DSS is not marketed effectively and is not understood by consumers as a standard that improves card data security (see section 4.2.13.2). It has been observed that website security is understood to be a significant component in a customer purchase decision (see section 2.2). The interviewees agreed that improving the awareness of the PCI DSS in consumers could help the adoption of the PCI DSS. The current lack of consumer awareness is surprising. If the PCI SSC's goal is to reduce fraud (see section 2.2) they should be actively marketing the standard to retail consumers. The interview with the PCI SSC suggested a comprehensive marketing / communication program was in place, but only to merchants and acquirers (see section 4.2.13.2). The consumer who supports the PCI by continuing to use payment cards instead of alternative methods of payments appears not to be included in any awareness programmes. The interviewees suggested that rates of adoption of the PCI DSS may improve if consumers were advised that certain websites were more secure than others.

Concerns were raised about the operation and management of the PCI DSS by the acquiring banks. Whilst all the interviewees and existing research agree that the standard is aimed at reducing fraud, concerns about potential conflicts of interest were raised in section 4.2.9 and by Segal (Segal et al. 2011) as a result of economic rent seeking by acquirers. It has to be considered that the potential commercial conflict of interest detailed in 4.2.9 could negatively impact levels of compliance. One way to address this conflict of interest, is to pass the management of the PCI DSS to the PCI SSC, removing the acquirer

from the process. Some may raise concerns that this would place additional overheads on the PCI SSC, but these would be minimal. The PCI SSC currently collect compliance data from the acquiring banks, this data would just be collected directly from the merchant. Similarly, PCI DSS compliance documentation would be submitted by a merchant directly to the PCI SSC instead of to the merchant bank. A similar concern, which was not identified by previous research is the commercial relationship between the QSA and the merchant. This is discussed in section 4.2.8. Similar concerns were raised within the financial community following the 2002 Enron scandal where the US auditing system failed to deliver true independence (Moore et al. 2006). The Enron scandal highlighted how organisations can become morally compromised as a result of significant conflicts of interest.

The interviewees suggested that compliance levels would improve if the PCI DSS was a legal requirement. This sentiment was also echoed by Cohen (Cohen 2014) as highlighted in section 2.8.2. This is unlikely to happen as payment card fraud is only one aspect of security which would have to be considered as part of any fraud legislation. Personal data would also have to be considered. As the DSS is a requirement of the PCI, it is unlikely that governments will interfere and make the PCI DSS a legal obligation. Ensuring consistency of the law across international borders would also make legal adoption unlikely.

4.4 Summary

Compliance with the PCI DSS is required by any merchant who processes or stores payment card data. It has been observed that the PCI DSS is a positive approach to reducing the potential for data breaches. However, the PCI DSS is a complex standard with several hundred requirements, it can be difficult to understand, require dedicated IT staff to implement and costly to attain / maintain. Having implemented the standard there is no guarantee that your organisation is safe from data loss.

It has been observed that the PCI DSS is most effective when it is part of a larger Information Security governance model. However, adoption of the standard is often dependent on the culture of the organisation. Some organisations who see value in Information Security implement the PCI DSS and other security standards across all their systems. Those who do not value Information Security implement the PCI DSS on the minimum number of systems required to pass a PCI assessment.

It is clear that the PCI is committed to reducing fraud by actively enhancing the standard. The latest version of the PCI DSS is the most comprehensive version of the standard to date which continues to reflect the changing ecosystem of Information Security. However,

it has also been observed that basic security issues like regularly changing passwords and Information Security awareness continue to be causes of concern. This may highlight the need for more effective end user security training.

This, and other research has suggested that financial incentives could be used to improve compliance. This is not likely to occur as the PCI SSC actively push costs to merchants are unlikely to fund such incentives.

C-level executives are more concerned about the damage a data breach would cause to their brand than they are about fines from the PCI DSS. The current level of fines and penalties do not encourage organisations to adopt the standard.

This research has raised concerns about rent seeking amongst acquirers. This research also highlights similar rent seeking concerns relating to QSA's. These rent seeking activities could undermine the credibility of the standard.

It has also been observed that financial settlements are agreed between the breached organisation and the PCI SSC. These settlements are often for a low financial value relative to the size of the data breach. These low value settlements as opposed to fines may discourage organisations from implementing the PCI DSS as they may believe they can negotiate a lower financial settlement if they suffer a breach.

It is unlikely that the PCI DSS will become a legal requirement due to the nature of individual sovereign countries respective legal systems.

It has been observed that the PCI DSS continues to evolve and issues with the standard continue to be addressed. However, several factors remain which continue to influence an organisations adoption of the PCI DSS, these will be discussed in the next chapter.

5. Conclusions and Future Work

5.1 Introduction

The objective of this research was to determine the factors that can influence a merchant's adoption of the PCI DSS. This chapter concludes this research, demonstrates that the research question has been answered, identifies the key findings and also acknowledges the limitations of the research and describes options for potential further research in this area.

5.2 Conclusions

All interviewees agreed that if it was not required by their acquirers or by their customers that they would not formally obtain PCI DSS certification. There were several factors influencing the interviewees' adoption of the PCI DSS.

Organisational culture.

Some organisations value Information Security more than others (see section 4.2.6). Those that value Information Security implemented the PCI DSS quickly across all their IT systems. Other organisations who do not value Information Security implement the PCI DSS in the minimum IT systems.

Impact on brand.

Senior executives are more concerned about the long term impact of a breach on their brand than they are of the potential fines or penalties from the PCI SSC. The current fines are insufficient to encourage organisations to adopt the standard. Many organisations are more concerned about the impact the DPC might have on their organisation and brand than the PCI SSC (see section 4.2.11).

Cost of implementing the PCI DSS.

There are significant ongoing costs in achieving and maintaining PCI DSS compliance (see section 4.2.13.1). In the current economic climate, some organisations have considered cost savings by reducing their investment in the PCI DSS and in Information security in general.

Language in the standard is complex.

The language in the standard is complex (see section 2.8.2, 4.2.13.2) as it attempts to convey complicated technical security requirements in plain text. International translations of the standard are also complicated as they lose subtle technical detail in translation.

This complexity often leads organisations to engage additional consultancy services from QSAs to explain the standard (see section 4.2.8). This leads to further increased costs.

Complexity of meeting the requirements of the standard.

The PCI DSS is a complex standard with over four hundred requirements (see section 2.7). Implementing the PCI DSS often requires dedicated IT staff (see section 4.2.3). Organisations often have to contract additional PCI consultancy services to ensure they meet all the requirements of the PCI DSS (see section 4.2.8).

Rent seeking between acquirers and QSA's.

It has been demonstrated that due to the current management of the PCI DSS there are opportunities for rent seeking amongst QSAs and acquirers (see sections 4.2.8 and 4.2.9). This rent seeking could undermine the credibility of the PCI DSS and it could lead to organisations either avoiding complying with the standard or being inappropriately certified as compliant.

Lack of Communication.

This research shows that the PCI SSC, as a result of not requiring breaches to be published and not publishing details of penalties and fines lose an opportunity where use of deterrence theory would actively encourage more organisations to become compliant (see section 2.11, 2.12, 4.2.11, 4.3). It has also been demonstrated that organisations only engage with their QSA and their acquiring bank. There is very little engagement between merchants and the PCI SSC. This has led to frustration from some merchants as highlighted in this research (see section 4.2.13.2).

Several recommendations have been suggested in this research, these have been summarised into four categories as follows:

• **Operation of The PCI DSS**

- The PCI SSC should require acquirers to more strictly enforce compliance or the enforcement of the PCI DSS should revert to the PCI SSC (see sections 4.2.9 and 4.3).
- PCI DSS assessments need to take place more frequently (see sections 2.9.2, 4.2.16 and 4.3).
- The role of the QSA needs to be reviewed where a company must alternate between different QSA's periodically to avoid conflicts of interest or rent seeking (see sections 4.2.8 and 4.3).

- **Penalties**
 - The fines resulting from a data breach need to be larger and published widely (see sections 4.2.11 and 4.3).
- **Communication**
 - Disclosure of data breaches should be mandatory (see sections 4.2.10, 4.2.11, 4.2.12 and 4.3)
 - The PCI SSC need to ensure that consumers are aware that organisations that implement the PCI DSS are more secure and less likely to suffer a breach.
 - The PCI SSC need to improve communication to merchants and respond to requests for information in a timely manner.
- **Relevance**
 - The standard needs to continue to be technically relevant by accurately reflecting current Information Security vulnerabilities.
 - The language employed in the PCI DSS needs to be simplified to make it easier to adopt.

5.3 Limitations of Research and Future Work

Due to financial and time constraints a small number of thirteen participants were interviewed. This small sample size may impact the generalisation of the findings. A small sample size is also subject to bias which the researcher cannot control (Saunders et al. 2012). The bias was minimised by interviewing several different e-commerce organisations from different commercial sectors. Some organisations were engaged in marketing, some in retail and others were hospitality. Some of the organisations had an international customer base, whilst others only had customers in Ireland.

As an organisation's security strategy is often considered to be sensitive in nature, obtaining consent from organisations to discuss their approach to Information Security and the PCI DSS was difficult (see section 1.3). It would also be beneficial to have participation from the Card Schemes, but due to limitations in time, resources and lack of access to any participant in the Card Schemes it was not possible to include them in the sample.

Again, due to financial and time constraints, interviews focused on e-commerce organisations which were required to be PCI DSS level one compliant. Despite the PCI DSS applying to all organisations that process and manage cardholder data other types of organisation were excluded. Future research could be carried out to include non-e-commerce organisations who were required to be PCI DSS compliant. Merchants from PCI DSS level two, three and four could also be included in further research.

The interviews were semi-structured in nature and took over an hour to complete. This limits the number of organisations that can take part in the study. The generalisation of the findings could be improved if this researches findings were used as part of a subsequent online, email or postal survey. These surveys could be further enhanced by including organisations outside of e-commerce websites. Combining qualitative and quantitative research methods would result in a mixed methods approach. A mixed method approach would compensate for the limitations in a purely qualitative research approach (see section 3.3) (Creswell 2003) as is the case with this research.

This research was undertaken at a time when the PCI DSS was going through unusual change. In January 2015, the standard went through a normal cycle of enhancement from PCI DSS version 2.1 to 3.0. However, in April 2015, an unscheduled enhancement was introduced following several significant Information Security issues with internet encryption technology (SSL). This caused the standard to undergo an update to version 3.1 which may have impacted the generalisation of the findings due to the unscheduled nature of the update. Previous research indicates that when a new version of the standard is released, levels of compliance drop as companies adjust to enhancements and new requirements in the latest version of the DSS (Oosten et al. 2014). However, this may also provide an opportunity for future study where the findings from this research could be re-evaluated as part of the normal update cycle of the PCI DSS to see if the findings are consistent over time.

The research was conducted in Ireland with several Irish based or Irish Headquartered organisations. Further research would need to be undertaken to ensure that the findings of this research were applicable to other countries. To minimise the impact of this limitation, organisations from a several commercial sectors were included in the interview process.

To address the limitations of this research and provide opportunities for future research additional research projects should be undertaken which would include:

- Inclusion of the Card Schemes.
- A larger sample of participants in the PCI DSS.
- Inclusion of merchants from PCI DSS level two, three and four.
- Adopt a mixed methods approach to minimise the impact of a purely qualitative or quantitative analysis (Creswell 2003).
- Inclusion of more merchants outside of Ireland.

Despite these limitations, this research has clearly highlighted several factors which can influence an organisation's adoption of the PCI DSS and has highlighted several opportunities for future research.

5.4 Summary

The objective of this research was to investigate the factors which impact the adoption of the PCI DSS.

This research has demonstrated that the implementation and management of a global Information Security standard is complex. The management of the PCI DSS is further complicated as it attempts to improve the security of e-commerce systems which are constantly evolving as technology advances.

The key factors which influence an organisation's adoption of the PCI DSS are organisational culture, cost, the need for specialist staff to manage a compliance programme and the complexity of the standard. A lack of data breach notification may deter organisations from implementing the PCI DSS as C-level executives do not appear to be concerned about the imposition of fines / penalties from the PCI SSC. C-level executives are more concerned about the impact to their corporate brand. Other factors which impact rates of adoption are rent seeking from both acquirers and merchants which may discourage organisations from implementing the PCI DSS.

Organisations must ultimately accept the responsibility of protecting their customer data. All organisations have a duty of care to their customers to ensure that cardholder data and any other data is processed and stored securely.

Given the current structure of the PCI with a lack of breach notification and lack of notification of penalties it is not possible to assert with confidence that the rates of adoption of the PCI DSS will increase significantly in the near future unless that are significant changes within the PCI in relation to the management and operation of the PCI DSS.

6. References

- Ataya, G., 2010. PCI DSS audit and compliance. *Information Security Technical Report*, 15(4), pp.138–144. Available at:
<http://www.sciencedirect.com/science/article/pii/S136341271100015X>.
- Beccaria, C., 1995. *On crimes and punishments and other writings*, Available at:
<http://books.google.com/books?id=xUBpHrnc7E8C>.
- Berezina, K. et al., 2012. The impact of information security breach on hotel guest perception of service quality, satisfaction, revisit intentions and word-of-mouth. *International Journal of Contemporary Hospitality Management*, 24(7), pp.991–1010. Available at: 10.1108/0959611211258883.
- Blackwell, Cian & Gahan, M., 2009. PCI DSS compliance — meeting the demands. *Data Protection Ireland*, (6), pp.0–3. Available at:
[http://www.grantthornton.ie/db/Attachments/Media_And_Events/Grant Thornton Data Protection article Feb 2010 CB & MG.pdf](http://www.grantthornton.ie/db/Attachments/Media_And_Events/Grant%20Thornton%20Data%20Protection%20article%20Feb%202010%20CB%20&%20MG.pdf).
- Braintree, 2008. PCI DSS Compliance Basics. *braintreepayments.com*. Available at:
<https://www.braintreepayments.com/blog/pci-compliance-basics-for-credit-card-security/> [Accessed July 29, 2015].
- Brocklehurst, K., 2014. PCI DSS Compliance is No Security Guarantee. *Tripwire.com*. Available at: <http://www.tripwire.com/state-of-security/regulatory-compliance/pci-dss-compliance-security-guarantee/> [Accessed July 30, 2015].
- Brown, T., 2015. Banks seek to block Target's deal with MasterCard over data breach. *Reuters*.
- Bul, U., 2011. 9 Steps to Processing Card-Not-Present Transactions. *UniBul Credit Card Blog*. Available at: <http://blog.unibulmerchantservices.com/9-steps-to-processing-card-not-present-transactions/> [Accessed April 19, 2015].
- Capgemini, 2013. What you need to know Global Trends In The Payment Card Industry 2013. *Cap Gemini*.
- Chen, Y., Ramamurthy, K. & Wen, K.-W., 2012. Organizations' Information Security Policy Compliance: Stick or Carrot Approach? *Journal of Management Information*

Systems, 29(3), pp.157–188. Available at:

<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=85985309&site=eds-live>.

Chenney, J.S., 2010. Heartland Payment Systems: Lessons Learned from a Data Breach. *Payment Cards Centre, Federal Reserve Bank of Philadelphia*. Available at:

<http://www.phil.frb.org/consumer-credit-and-payments/payment-cards-center/publications/discussion-papers/2010/d-2010-january-heartland-payment-systems.pdf>.

Chohen, F., 2015. Here's why Verified by Visa is officially the worst thing ever. *The Daily Edge*. Available at: <http://www.dailyedge.ie/verified-by-visa-is-the-worst-thing-ever-1261755-Jan2014/> [Accessed April 6, 2015].

Cidell, J., 2010. Content clouds as exploratory qualitative data analysis Cidell Content clouds as exploratory qualitative data analysis. *Area*, 42(4), pp.514–523. Available at: 10.1111/j.1475-4762.2010.00952.x.

Cisco, 2011. *Organizations See PCI as a Benefit, Not a Burden*, Available at:

http://www.cisco.com/c/dam/en/us/products/collateral/enterprise-networks/pci-compliance/white_paper_c11-642025.pdf.

Coburn, A., 2010. Fitting PCI DSS within a wider governance framework. *Computer Fraud & Security*, 2010(9), pp.11–13. Available at:

<http://www.sciencedirect.com/science/article/pii/S1361372310701214> [Accessed January 2, 2015].

Cohen, B., 2014. THE LAW OF SECURING CONSUMER DATA ON NETWORKED COMPUTERS. *Journal of Internet Law*, 18(2), pp.3–12. Available at:

<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=97435737&site=eds-live>.

Creswell, J.W., 2003. Research Design: Qualitative, Quantitative, and Mixed Methods Approaches. *Research design Qualitative quantitative and mixed methods approaches*, p.398.

Crotty, M., 1998. *The foundations of social research: Meaning and perspective in the research process*,

- D'Arcy, J., Hovav, A. & Galletta, D., 2009. User awareness of security countermeasures and its impact on information systems misuse: A deterrence approach. *Information Systems Research*, 20(1), pp.79–98.
- Dempsey, K. et al., 2011. *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, Available at:
<http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>.
- Denzin, N. & Lincoln, Y., 2005. The Sage handbook of qualitative research. In *Sage Publications*. pp. 85–91.
- DiCicco-Bloom, B. & Crabtree, B.F., 2006. The qualitative research interview. *Medical Education*, 40(4), pp.314–321. Available at: <http://dx.doi.org/10.1111/j.1365-2929.2006.02418.x>.
- Ferguson, R., 2011. Loopholes in Verified by Visa & SecureCode. *Krebsonsecurity.com*.
- Folkestad, B., 2008. Analysing interview data: Possibilities and challenges. *Eurosphere Working Paper Series*, (Online working paper 13). Available at:
http://eurospheres.org/files/2010/08/Eurosphere_Working_Paper_13_Folkestad.pdf.
- FTC Staff, 2006. CardSystems Solutions, Inc., and Solidus Networks, Inc., d/b/a Pay By Touch Solutions, In the Matter of. *Federal Trade Commission*. Available at:
<https://www.ftc.gov/enforcement/cases-proceedings/052-3148/cardsystems-solutions-inc-solidus-networks-inc-dba-pay-touch> [Accessed April 26, 2015].
- Gikas, C., 2010. A General Comparison of FISMA, HIPAA, ISO 27000 and PCI-DSS Standards. *Information Security Journal: A Global Perspective*, 19(3), pp.132–141. Available at: 10.1080/19393551003657019.
- Haggerty, N.R.D. & Ramasastry, C., 2008. Harvard Business Review. *Harvard Business Review*. Available at: <https://hbr.org/product/security-breach-at-tjx/908E03-PDF-ENG> [Accessed January 1, 2015].
- Hartley, D., 2009. Secure e-commerce web application design principles, beyond PCI DSS. *Computer Fraud & Security*, 2009(6), pp.13–17. Available at:
<http://www.sciencedirect.com/science/article/pii/S1361372309700740>.

Hartono, E. et al., 2014. Measuring perceived security in B2C electronic commerce website usage: A respecification and validation. *Decision Support Systems*, 62, pp.11–21. Available at: [10.1016/j.dss.2014.02.006](https://doi.org/10.1016/j.dss.2014.02.006).

Hays, S., 2012. A Famous Data Security Breach & PCI Case Study: Four Years Later. Available at: <http://www.secureworks.com/resources/blog/general-pci-compliance-data-security-case-study-heartland/> [Accessed April 6, 2015].

HomeDepot, 2014a. *Home Depot Reports Findings in Payment Data Breach Investigation*, Available at: [https://corporate.homedepot.com/MediaCenter/Documents/Press Release.pdf](https://corporate.homedepot.com/MediaCenter/Documents/Press%20Release.pdf).

HomeDepot, 2014b. *Notice to our customers*, Available at: [https://corporate.homedepot.com/MediaCenter/Documents/Important Customer Notice.pdf](https://corporate.homedepot.com/MediaCenter/Documents/Important%20Customer%20Notice.pdf).

Hovav, A. & Gray, P., 2014. The Ripple Effect of an Information Security Breach Event: A Stakeholder Analysis. *Communications of the Association for Information Systems*, 34, pp.893–912. Available at: <http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=94902951&site=eds-live>.

HU, Q. et al., 2011. Does Deterrence Work in Reducing Information Security Policy Abuse by Employees? *Communications of the ACM*, 54(6), pp.54–60. Available at: [10.1145/1953122.1953142](https://doi.org/10.1145/1953122.1953142).

Huth, P.K., 1999. DETERRENCE AND INTERNATIONAL CONFLICT: Empirical Findings and Theoretical Debates. *Annual Review of Political Science*, 2(1), pp.25–48.

IPSO, 2013. Card Payments Volume. *Irish Payment Services Organisation Limited*. Available at: <http://www.ipso.ie/?action=statistics§ionName=IrelandStatistics&statisticCode=IE&statisticRef=IE06>.

Kaplan, S.E. & Nieschwietz, R.J., 2003. A Web assurance services model of trust for B2C e-commerce. *International Journal of Accounting Information Systems*, 4(2), pp.95–114. Available at: <http://www.sciencedirect.com/science/article/pii/S1467089503000058>.

- Kedgley, M., 2014. PCI DSS Version 3.0: new standard, but same problems? *Computer Fraud & Security*, 2014(1), pp.5–9. Available at:
<http://www.sciencedirect.com/science/article/pii/S1361372314700053> [Accessed November 3, 2014].
- Kerner, S.M., 2013. PCI-DSS 3.0 Security Compliance Gets Stronger. *eWeek*, p.5. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=89867578&site=eds-live>.
- KIM, D. & BENBASAT, I., 2010. Designs for Effective Implementation of Trust Assurances in Internet Stores. *Communications of the ACM*, 53(2), pp.121–126. Available at:
10.1145/1646353.1646386.
- Krebs, B., 2014. Home Depot: Hackers Stole 53M Email Addresses. *Krebsonsecurity.com*. Available at: <http://krebsonsecurity.com/tag/home-depot-breach/> [Accessed May 20, 2015].
- Krebs, B., 2015. How Was Your Credit Card Stolen? *Krebs On Security*. Available at:
<http://krebsonsecurity.com/2015/01/how-was-your-credit-card-stolen/> [Accessed May 4, 2015].
- Kvale, S., 2007. *Doing Interviews*, Available at: <http://srmo.sagepub.com/view/doing-interviews/SAGE.xml>.
- Kvale, S., 1996. The 1,000 Page Question. In *InterViews: An Introduction to Qualitative Research Interviewing*. pp. 176–209.
- Lansdale, T., 2014. PCI compliance - how basic website hygiene can add business value. *SC Magazine*. Available at: <http://www.scmagazineuk.com/pci-compliance--how-basic-website-hygiene-can-add-business-value/article/346777/>.
- LINDSTROM, P., 2014. Is the PCI Data Security Standard Working? *Information Security*, 16(5), p.30. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edb&AN=96403350&site=eds-live>.

Lovrić, Z., 2012. Model of Simplified Implementation of PCI DSS by Using ISO 27001 Standard. *ceciis.foi.hr*, pp.347–351. Available at:
<http://www.ceciis.foi.hr/app/public/conferences/1/papers2012/iss8.pdf>.

MasterCard, 2015. About Mastercard.

Metzger, T., 2009. How credit card transactions work. *creditcards.com*. Available at:
<http://www.creditcards.com/credit-card-news/how-a-credit-card-is-processed-1275.php>.

Miller, J.A., 2014. PCI Compliance Under Scrutiny Following Big Data Breaches. *cio.com*. Available at: <http://www.cio.com/article/2836035/data-breach/pci-compliance-under-scrutiny-following-big-data-breaches.html> [Accessed April 19, 2015].

Moore, D.A. et al., 2006. Conflicts of interest and the Case of Auditor Independence: Moral Seduction and Strategic Issue Cycling. *Academy of Management Review*, 31(1). Available at: http://faculty.haas.berkeley.edu/tetlock/vita/philip_tetlock/phil_tetlock/2004_current/2005_conflicts_of_interest_and_auditor_independencepageproofs.pdf.

Morse, E.A., 2012. Private Ordering in Light of the Law: Achieving Consumer Protection Through Payment Card Security Measures. *DePaul Business & Commercial Law Journal*, 10, p.213. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=edslex&AN=edslex320F4E39&site=eds-live>.

Morse, J.M. et al., 2008. Verification Strategies for Establishing Reliability and Validity in Qualitative Research. *International Journal of Qualitative Methods*, 1, pp.13–22. Available at: <https://ejournals.library.ualberta.ca/index.php/IJQM/article/view/4603>.

Munson, L., 2014. Target data breach: Why UK business needs to pay attention. *ComputerWeekly.com*. Available at: <http://www.computerweekly.com/feature/Target-data-breach-Why-UK-business-needs-to-pay-attention> [Accessed May 20, 2014].

Murdoch, S.J. & Anderson, R., 2010. Verified by Visa and MasterCard SecureCode: or, How Not to Design Authentication. *University of Cambridge*. Available at:
<http://www.cl.cam.ac.uk/~rja14/Papers/fc10vbwsecurecode.pdf> [Accessed April 6, 2015].

O'Raghallaigh, E., 2010. Security Issues in E-Commerce. *Webscience*. Available at:
<http://webscience.ie/blog/2010/security-issues-in-e-commerce/> [Accessed April 19, 2015].

Office of the Data Protection Commissioner, 2013. Office of the Data Protection Commissioner - Case Studies 2013. *Office of the Data Protection Commissioner*. Available at: <https://dataprotection.ie/docs/CASE-STUDIES-2013/1441.htm#CS14> [Accessed January 1, 2015].

Oosten, C. van et al., 2014. *Verizon 2014 PCI Compliance Report*, Available at:
http://www.verizonenterprise.com/resources/reports/rp_pci-report-2014_en_xg.pdf.

Van Oosten, C., Baritchi, A. & van Koten, R., 2015. *Verizon 2015 PCI Compliance Report*, Available at: http://www.verizonenterprise.com/resources/report/rp_pci-report-2015_en_xg.pdf.

Palinkas, L.A. et al., 2013. Purposeful sampling for qualitative data collection and analysis in mixed method implementation research. *Administration and Policy in Mental Health and Mental Health Services Research*. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=psyh&AN=2013-39278-001&site=eds-live>.

Parker, D.B., 1998. *Fighting Computer Crime: A New Framework for Protecting Information*,

PCI SSC, 2008. Getting Started With PCI Data Security Standard. , p.5. Available at:
https://www.pcisecuritystandards.org/pdfs/pcissc_getting_started_with_pcidss.pdf.

PCI SSC, 2010. PCI DSS Requirements and Security Assessment Procedures. *PCI Security Standards*. Available at:
https://www.pcisecuritystandards.org/documents/pci_dss_v2.pdf.

PCI SSC, 2006. PCI Organisational Structure. Available at:
https://www.pcisecuritystandards.org/organization_info/index.php.

Ponemon Institute, 2011a. *2011 PCI DSS Compliance Trends Study*, Available at:
http://www.imperva.com/docs/ap_ponemon_2011_pci_dss_compliance_trends_study.pdf.

Ponemon Institute, 2011b. *The True Cost of Compliance*, Available at:

http://www.ponemon.org/local/upload/file/True_Cost_of_Compliance_Report_copy.pdf.

Rees, J., 2012. Tackling the PCI DSS challenges. *Computer Fraud & Security*, 2012(1), pp.15–17. Available at:

<http://www.sciencedirect.com/science/article/pii/S136137231270009X> [Accessed January 2, 2015].

Rees, J., 2010. The challenges of PCI DSS compliance. *Computer Fraud & Security*, 2010(12), pp.14–16. Available at:

<http://www.sciencedirect.com/science/article/pii/S1361372310701561> [Accessed October 19, 2014].

Riley, M. et al., 2014. The Epic Hack. (cover story). *Bloomberg Businessweek*, (4371), pp.42–47. Available at:

<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=rgm&AN=95007328&site=eds-live>.

Rowlingson, R. & Winsborrow, R., 2006. A comparison of the Payment Card Industry data security standard with ISO17799. *Computer Fraud and Security*, 2006, pp.16–19.

RTE News, 2013. Credit card details of 500,000 European customers may have been hit by loyalty scheme breach. *RTE.ie*. Available at:

<http://www.rte.ie/news/2013/1112/486081-loyaltybuild/>.

Saunders, M., Lewis, P. & Thornhill, A., 2012. *Research Methods for Business Students*,

Saunders, M. & Tosey, P., 2012. The Layers of Research Design. *Rapport*, Winter, pp.58–59. Available at:

http://www.academia.edu/4107831/The_Layers_of_Research_Design.

Schwartz, M.J., 2011. 67% Of Companies Fail Credit Card Security Compliance. , pp.1–2.

SearchSecurity Staff, 2013. The-history-of-the-PCI-DSS-standard-A-visual-timeline @ searchsecurity.techtarget.com. Available at:

<http://searchsecurity.techtarget.com/feature/The-history-of-the-PCI-DSS-standard-A-visual-timeline>.

- Segal, L., Ngugi, B. & Mana, J., 2011. CREDIT CARD FRAUD: A NEW PERSPECTIVE ON TACKLING AN INTRANSIGENT PROBLEM. *Fordham Journal of Corporate & Financial Law*, 16(4), pp.743–781. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=67362688&site=eds-live>.
- Services, U.S.D. of H. & H., 2009. Health Information Privacy. *hhs.gov*.
- Shaw, A., 2010. Data breach: from notification to prevention using PCI DSS. *Columbia Journal of Law & Social Problems*, 43(4), pp.517–562. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=ofm&AN=502172567&site=eds-live>.
- Shermach, K., 2012. ISOs Still Face A Major Task Of Prepping Merchants For PCI. *ISO & Agent Weekly*, 8(8), pp.40–46. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=74201301&site=eds-live>.
- Stapleton, J. & Spencer Poore, R., 2011. Tokenization and Other Methods of Security for Cardholder Data. *Information Security Journal: A Global Perspective*, 20(2), pp.91–99. Available at: 10.1080/19393555.2011.560923.
- Straub, D.W. & Welke, R.J., 1998. Coping With Systems Risk: Security Planning Models for Management Decision Making. *MIS Quarterly*, 22(4), pp.441–469. Available at:
<http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=1649969&site=ehost-live>.
- Sullivan, R.J., 2014. Controlling Security Risk and Fraud in Payment Systems. , pp.5–36. Available at:
<http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=eoh&AN=EP98764805&site=eds-live>.
- Susanto, H., Nabil Almunawar, M. & Chee Tuan, Y., 2011. Information Security Management System Standards: A Comparative Study of the Big Five. *International Journal of Electrical & Computer Sciences*, Vol: 11 No. Available at:
http://www.researchgate.net/profile/Heru_Susanto/publication/228444915_Information_Security_Management_System_Standards_A_Comparative_Study_of_the_Big_Five/links/09e4150cffd3cf062d000000.pdf.

- Theoharidou, M. et al., 2005. The insider threat to information systems and the effectiveness of ISO17799. *Computers and Security*, 24(6), pp.472–484. Available at: <http://www.sciencedirect.com/science/article/pii/S0167404805000684>.
- Varian Foster, H., Grannis, K. & Taylor, D., 2009. RESEARCH FINDS PCI DSS AWARENESS HIGH AMONG SMALL RETAILERS, LACK OF UNDERSTANDING REMAINS HUGE HURDLE. *Souvenirs, Gifts, & Novelties*, 48(7), pp.198–199. Available at: <http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=45005579&site=eds-live>.
- Verizon Enterprise, 2014. *2014 Data Breach Investigations Report*, Available at: http://www.verizonenterprise.com/DBIR/2014/reports/rp_Verizon-DBIR-2014_en_xg.pdf.
- Vijayan, J., 2008. One year later: Five takeaways from the TJX breach. *Computerworld.com*. Available at: <http://www.computerworld.com/article/2538711/cybercrime-hacking/one-year-later--five-takeaways-from-the-tjx-breach.html> [Accessed April 26, 2015].
- Visa, 2015. History Of Visa. Available at: <http://usa.visa.com/about-visa/our-business/history-of-visa.jsp> [Accessed April 6, 2015].
- Visa Europe, 2015. Merchant levels and compliance validation requirements. Available at: <http://www.visaeurope.com/receiving-payments/security/merchants>.
- Weckler, A., 2014. Loyaltybuild: Firm at centre of hacking breach back in business. *Independent.ie*. Available at: <http://www.independent.ie/business/technology/loyaltybuild-firm-at-centre-of-hacking-breach-back-in-business-30084088.html>.
- Weiss, M.-A., 2011. TOWARDS MANDATORY DATA BREACH NOTIFICATION LAWS IN THE EUROPEAN UNION. *Journal of Internet Law*, 14(12), pp.24–29. Available at: <http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=61167092&site=eds-live>.
- Wengraf, T., 2001. *Qualitative Research Interviewing: Biographic Narrative and Semi-Structured Methods*, Sage Publications Ltd.

Williams, B.R., 2010. How tokenization and encryption can enable PCI DSS compliance. *Information Security Technical Report*, 15(4), pp.160–165.

Willison, R. & Warkentin, M., 2013. BEYOND DETERRENCE: AN EXPANDED VIEW OF EMPLOYEE COMPUTER ABUSE. *MIS Quarterly*, 37(1), pp.1–20. Available at: <http://elib.tcd.ie/login?url=http://search.ebscohost.com/login.aspx?direct=true&db=bth&AN=85640558&site=eds-live>.

Worldpay, 2014. *Worldpay 2013 Annual Report*, Available at: http://www.worldpay.com/sites/default/files/pictures/Worldpay_2013_annualreport_final.pdf.

Zetter, K., 2005. CardSystems' Data Left Unsecured. *wired.com*. Available at: <http://archive.wired.com/science/discoveries/news/2005/06/67980> [Accessed January 1, 2015].

Zorzini, C., 2014. Fraud. *e-commerce Platforms*. Available at: <http://e-commerce-platforms.com/glossary/fraud> [Accessed August 13, 2015].

7. Appendices

7.1 Information Sheet for Participants

TRINITY COLLEGE DUBLIN

Information Sheet for Participants

Background of the research

The Payment Card Industry Data Security Standard has been in place for approximately 10 years. The standard has gone through several enhancements and as of January 2015, merchants need to comply with PCI DSS version 3.0 and in April 2015 PCS DSS version 3.1. Whilst there are perceived advantages to achieving PCI compliance as well as perceived issues with the standard, adoption rates continue to be low. This research intends to consider the factors that influence the low rates of adoption of the standard.

Your contribution to this research will assist with our understanding of the adoption of standards and what factors which influence a organisation's decision to adopt these standards.

Selection Criteria

You were selected for this interview on the basis of recommendation from a mutual commercial acquaintance as someone who has responsibility for ICT/Compliance within your organisation.

Risks / Benefits

- Due to the anonymous nature of the interview, there are no risks to the participant or the organisation with whom they are employed
- The participant may be interested in the results of the dissertation as significant time / money can be spent on achieving compliance with the PCI DSS, the research may assist in ensuring on-going investment in security within the organisation
- The research may secure funding in an organisation to initially invest in a security programme
- The participant may benefit from the research, as it will include input from several other organisations and their experiences with achieving compliance with PCI DSS.

This may reduce efforts required by the organisation to achieve or maintain compliance with the PCI DSS in the future.

The Interview Process

Please note the following:

- Participation in the process is voluntary and anonymous.
- You have the right to stop and withdraw from the interview process at any time without penalty.
- You may refuse to answer any question without penalty.
- The interview process will take approximately 1 hour.
- In order to ensure accuracy of the interview, I will ask for consent to use an audio recorder during the interview.
- If you do not permit an audio recording to take place, I will take handwritten notes.
- I will request that the notes are initialled and dated on completion of the interview.
- As interview questions are open ended, please be aware that you should not name third parties.
- Subsequent follow-up may take place after the initial interview to verify direct quotations and to ensure their contextual relevance. This follow-up can take place via e-mail.

Results

Once the interviews have been completed, your answers will be analysed and interpreted. No source, individual or organization will be identified in the findings.

Debriefing

Upon completion of the dissertation, you may receive an electronic copy of the research dissertation by contact me on – bnoonan@tcd.ie. The dissertation will be available after 1st September 2015.

Additional Information

This interview is being carried out as part of the requirement of the MSc Management of Information Systems in Trinity College Dublin 2014/2015.

The relevant Data Protection Act 1988 and the Data Protection Amendment Act 2003 will govern all aspects of this research.

In line with the Data Protection Act Rule 7, the data gathered as part of this research shall not be held for longer than the purpose for which it was collected. In order to complete this research, data will be held for no longer than 6 months from which it was collected. After which all electronic copies of the data will be securely erased.

I have no conflict of interest with regard to the research topic. However, some participants selected are current / previous colleagues.

All information from this interview will be held securely. Audio files will be encrypted on my computer network. Only I will know the passphrase. Audio recording will only be used as part of this dissertation. The audio recordings will never be re-played in any public forum or as part of any other work. You or your organisation will not be identified as part of this research. A number will be used to represent you. Eg Organisation number 1 or participant number 1.

I am required by Trinity College Dublin to inform you that during the course of the interview, if you inadvertently reveal any illicit activities, I am required to report them to the relevant authority.

7.2 Information Sheet for Senior Management

TRINITY COLLEGE DUBLIN

Information Sheet for Senior Management

Background of the research

The Payment Card Industry Data Security Standard has been in place for approximately 10 years. The standard has gone through several enhancements and as of January 2015, merchants need to comply with PCI DSS version 3.0 and PCI DSS version 3.1 since April 2015. Whilst there are perceived advantages to achieving PCI compliance as well as perceived issues with the standard, adoption rates continue to be low. This research intends to consider the factors that influence the low rates of adoption of the standard.

The organisations contribution to this research will assist with our understanding of the adoption of standards and what factors which influence a organisation's decision to adopt these standards.

Selection Criteria

The participant, who is employed in the organisation, was selected for this interview on the basis of a recommendation from a mutual commercial acquaintance as someone who has responsibility for ICT/Compliance and where the organisation may approve participation of the participant in this research.

Risks / Benefits

- Due to the anonymous nature of the interview, there are no risks to the participant or the organisation with whom they are employed
- The organisation may be interested in the results of the dissertation as significant time / money can be spent on achieving compliance with the PCI DSS, the research may assist in ensuring on-going investment in security within the organisation
- The research may secure funding in an organisation to initially invest in a security programme
- The organisation may benefit from the research, as it will include input from several other organisations and their experiences with achieving compliance with PCI DSS.

This may reduce efforts required by the organisation to achieve or maintain compliance with the PCI DSS in the future.

The Interview Process

Please note the following:

- Participation in the process is voluntary and anonymous.
- The participant has the right to stop and withdraw from the interview process at any time without penalty.
- The participant may refuse to answer any question without penalty.
- The interview process will take approximately 1 hour.
- In order to ensure accuracy of the interview, I will ask for consent to use an audio recorder during the interview.
- If the participant does not permit an audio recording to take place, I will take handwritten notes.
- I will request that the notes are initialled and dated on completion of the interview by the participant.
- As interview questions are open ended, please be aware that the participant should not name third parties.
- Subsequent follow-up may take place after the initial interview to verify direct quotations and to ensure their contextual relevance. This follow-up can take place via e-mail.

Results

Once the interviews have been completed, answers will be analysed and interpreted. No source, individual or organization will be identified in the findings.

Debriefing

Upon completion of the dissertation, you or your organisation may receive an electronic copy of the research dissertation by contact me on – bnoonan@tcd.ie. The dissertation will be available after 1st September 2015.

Additional Information

This interview is being carried out as part of the requirement of the MSc Management of Information Systems in Trinity College Dublin 2014/2015.

The relevant Data Protection Act 1988 and the Data Protection Amendment Act 2003 will govern all aspects of this research.

In line with the Data Protection Act Rule 7, the data gathered as part of this research shall not be held for longer than the purpose for which it was collected. In order to complete this research, data will be held for no longer than 6 months from which it was collected. After which all electronic copies of the data will be securely erased.

I have no conflict of interest with regard to the research topic. However, some participants selected are current / previous colleagues.

All information from this interview will be held securely. Audio files will be encrypted on my computer network. Only I will know the passphrase. Audio recording will only be used as part of this dissertation. The audio recordings will never be re-played in any public forum or as part of any other work. You or your organisation will not be identified as part of this research. A number will be used to represent you. Eg Organisation number 1 or participant number 1.

I am required by Trinity College Dublin to inform you that during the course of the interview, if you inadvertently reveal any illicit activities, I am required to report them to the relevant authority.

7.3 Informed Consent Form for Participants

TRINITY COLLEGE DUBLIN

Informed Consent Form for Participants

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- Consent to take part in this interview process has been received from appropriate management.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that my data is used for scientific purposes and I have no objection that my data is published in scientific publications in a way that does not reveal my identity.
- I understand that if I make illicit activities known, these will be reported to appropriate authorities.
- I understand that I may stop electronic recordings at any time, and that I may at any time, even subsequent to my participation have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I freely and voluntarily agree to be part of this research study, though without prejudice to my legal and ethical rights.
- I understand that I may refuse to answer any question and that I may withdraw at any time without penalty.
- I understand that my participation is fully anonymous and that no personal details about me will be recorded.
- I have received a copy of this agreement.

Participant's Name:

Participant's Signature:

Date:

Statement of investigator's responsibility:

I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the participant understands my explanation and has freely given informed consent.

RESEARCHERS CONTACT DETAILS

eMail: bnoonan@tcd.ie

Mobile Phone: +353 87 3684118

Researcher's Name: Barry Noonan

Researchers Signature:

Date:

7.4 Informed Consent Form for Senior Management

TRINITY COLLEGE DUBLIN

Corporate Consent Form

DECLARATION:

- I am 18 years or older and am competent to provide consent.
- I have read, or had read to me, a document providing information about this research and this consent form. I have had the opportunity to ask questions and all my questions have been answered to my satisfaction and understand the description of the research that is being provided to me.
- I agree that data gathered is used for scientific purposes and I have no objection to that data being published in scientific publications in a way that does not reveal identity of the participant or the identify of the organisation.
- I understand that if the participant makes illicit activities known, these will be reported to appropriate authorities.
- I understand that the participant may stop electronic recordings at any time, and that the participant may at any time, even subsequent to participation in the interview have such recordings destroyed (except in situations such as above).
- I understand that, subject to the constraints above, no recordings will be replayed in any public forum or made available to any audience other than the current researchers/research team.
- I agree that the participant voluntarily agrees to be part of this research study, though without prejudice to their legal and ethical rights.
- I understand that the participant may refuse to answer any question and that the participant may withdraw at any time without penalty.
- I understand that participation is fully anonymous and that no personal details about the participant or their employers will be recorded.
- I have received a copy of this agreement.

I agree that _____ is authorized to participate in the research interview "A study of the factors influencing the adoption of Payment Card Industry Data Security Standard".

Company Name:

Company Representative Name:

Company Representative Signature:

Date:

Statement of investigator's responsibility:

I have explained the nature and purpose of this research study, the procedures to be undertaken and any risks that may be involved. I have offered to answer any questions and fully answered such questions. I believe that the senior manager understands my explanation and has freely given informed consent for the participant to take part in the research project.

RESEARCHERS CONTACT DETAILS

eMail: bnoonan@tcd.ie

Mobile Phone: +353 87 3684118

PARTICIPANT'S NAME: Barry Noonan

PARTICIPANT'S SIGNATURE:

Date:

7.5 Extract from Interview

Note: In areas where organisations were identified, the transcript has been altered to remove the name of the organisation. The name of the organisation was replaced with "XXXXXX".

Interviewer

How do you guys approach the PCI aspects of all of this. There's risk, information security and data protection. There are so many overlapping components. I get a very mature flavour of a very mature, well organised approach. The assumption, and we'll chat about it, how that's reflected in your compliance program as you have merchants, and a relationship will be built between acquirers and merchants and you in turn have a relationship to the card schemes. You guys are in the awful position of having the judge and jury in some respects in terms of a merchant's compliance and equally an organisation working towards compliance. How do you approach that?

Interviewee

Well, PCI DSS is our license to operate. Right? And we treat it as such. PCI DSS is not a bad standard. It exists in, lets say, a less optimal environment, in which the card schemes and the SSC are involved. And the reason for that is all about liability shift isn't it. Retrospective non-compliance. So it's a kind of a license that can be removed at any moment. It really doesn't protect you. We treat information security as something rather more fundamental. You can be compliant but not secure. And you can be secure but non-compliant. So we want to be both.

Interviewer

So, you want to be compliant in reality as well as in theory.

Interviewee

Yeah, but that's not secure. We would like to be secure. We would like to be secure but we would also like to be compliant. Those two things have different focuses. And yeah, you have to be realistic about that.

Interviewer

Does that come back to your pragmatic approach and that might also suggest that the PCI DSS is potentially addressing the wrong problem?

Interviewee

Or its very focused... And sometimes its very focused on very strange things. I'll give you one an example, It's in requirement 11. It's related to scanning for open Wi-Fi Aps. If you don't use Wi-Fi, why do you do this.

Interviewer

We don't use Wi-Fi, but we still do it.

Interviewee

Yeah, because it's mandated.

Interviewer

Exactly.

Interviewer

I suppose it's because we need to be seen to be addressing the items in the standard. Whether or not it's relevant to our organisation...

Interviewee

Exactly, whether or not it enhances cardholder security. So that's just one example. I'll give you another that uses MVS mainframes. You do checks every day. It's a checkbox culture that's not a good match to reality.

Interviewer

Again, because other standards are looking to be boxes to be ticked, they aren't necessarily looking for boxes to be ticked. So you can be issued with a certificate.

Interviewee

We approach compliance with a very pragmatic view. We need a licence to operate. We need to keep our regulators happy. We do everything that our regulators ask of us. We also undertake certain additional audits which are appropriate for a party that is handling other people's money. So for example ISAE 3402 which I have some involvement in from the IT controls side. And that's effectively financial integrity. Which is a very important thing to demonstrate to our merchants. And the exercise is a very valuable thing for us to engage in every quarter.

Interviewer

Is it also reasonable to suggest that those additional levels of accreditation, in inverted commas, give your private stakeholders more comfort to know that you are going above and beyond?

Interviewee

No, it's all for our merchants. It's for our merchants to say there are financial controls and management in place. It's really important. If you have a NPL for a merchant, they want to know they will get a pay-out eventually. There's a deposit. They want to know that we aren't going to forget to pay them or caught in fraud or any other kinds of things. So the exercise is valuable on two sides, one is to demonstrate to very important stakeholders, our customers, that we take their money seriously, the second is to our keep our internal processes on our toes. And to some extent we do that for PCI DSS as well. PCI DSS is very focused on cardholder data. We tend to generalise the principles. We try to handle all data as if it was broadly speaking like cardholder data. So that means, gift cards get handled as if they were credit cards. Debit cards are the same. We want to keep the best practice aspects of PCI. It means less strangeness, more common code parts, easier audits. For our own purposes we can actually be sure that there is unlikely to be fraud on gift cards or employee fraud on gift cards because they can't decrypt them.

Interviewer

Is it fair to say that having a consistent playing field, ignoring the PCI focus on cardholder data? If you applied the principles to the standard across the organisation, consistency, operational overhead, you are all singing from the same hymn sheet? All data is encrypted; life is actually easier having implemented the principles of the standard?

Interviewee

Yeah, and it makes it very much easier to have architectural discussions. Because we are coming from the same position.

Interviewer

And everyone is away of the underlying principles? For encrypted data whether it be debit, credit, vouchers etc.

Interviewee

Exactly

Interviewer

Would your approach to Information Security be significantly different if your organisation wasn't involved in PCI DSS?

Interviewee

That's a very difficult question to answer that's because XXXXX was formed I think around the time of PCI DSS 1.0 2004 – 2005. Therefore, the design of our platform is very much focused on the principles of PCI DSS. We didn't have to retrofit, we were actually look at the principles there and trying to build something to meet those principles.

Interviewer

And I think the key word I am getting is "principle" as opposed to the individual dictates or box ticking of the standard? Could I paraphrase it then and suggest that your distilled the the standard down to broad principles and made sure that they were honoured and respected within the XXXXXX architecture?

Interviewee

And then as our organisation and the deployment of our infrastructure grew to non European Economic Area progressed then we started to think about exactly the same one-way cryptography which we use for sensitive data for all PII as in the EEA. Then we have one way hashes, we generate HMACs so then I guess then that there is no significant exposure, even for our US data subjects. Contracting with US merchants and US acquiring which is totally not covered by the European Data Protection principles, but we are still fully compliant with the principles in which we operate and we try to keep to best practice and I guess the leading standard in Europe with data protection, we've got it.

Interviewer

So in theory, having these principles in place actually made interaction with new markets easier?

Interviewee

Absolutely, I think it must be very difficult for any US based payment providers to enter into the European market. It must be bizarre and frightening

Interviewer

But XXXXXX have it built into their DNA as an organisation, so you know, transplanting the seed to another field, wouldn't have been a huge culture shift for ye?

Interviewee

Yeah, yeah

Interviewer

You mentioned earlier that you thought that PCI wasn't a "bad" standard. Eh, with the underlying principles you used, I guess that you believe that the organisation is more secure having adopted those core principles as distinct from just PCI or guiding rules

Interviewee

Yes, it's a good way to do business when you are dealing with cardholder data. And that's very important especially with the monetisation risks that exist with the various entities where you deal with lots of data. And it's the trust that shoppers give us.

Interviewer

Cause there's a huge amount of implicit trust in terms of efficacy and non-repudiation of any transaction is transparent

Interviewee

Yep, yeah

Interviewer

Were there any particular areas of the standard that you and your experience that organisations find more difficult, or because of the genesis of the business and the initial approach that it wasn't a problem?

Interviewee

I think that we had a far less pain than any other place in the industry to get certification every year. But it's certainly quite a lot of work. I've certainly noticed in the last 2 years a very different level of detail required by assessors. And I think that's very dangerous for tier 1 merchants more than for acquirer's payments for a merchant are less interesting than purchasing and only marginally more interesting than logistics. All the effort goes into sales / marketing you know and product mix. So the compliance around payments is even less interesting than payments and it's just this huge cost / effort / hassle and I think it's quite

dangerous. I think that the card schemes could be killing the goose that lays the golden eggs if they aren't careful.

Interviewer

In terms of organisations like us where payment processing isn't our core business, obviously we are here to push hostels and bookings and payment processing is a way that we allow that to happen, do you use the changes in the standard accelerating the adoption of full PSP services like XXXXXX offer, as opposed to what we currently do in terms of holding all of our own cardholder data.

I certainly see that and that's potentially good for XXXXXX, but we'd far prefer those merchants wanted to join us as opposed to the fact that it was so expensive to do anything else that they were forced to.

Interviewer

Right, but again that assumes a mature approach to a risk / governance perspective as opposed to a more legislative approach, where someone goes we know better