Compliance Standards in Data Security

Why PCI DSS and ISO/IEC 27001 Should Be Integrated

Georgia Institute of Technology
College of Computing
&
eFortresses Inc.

By
Monika Blount
Masters of Science in Information Security
Practicum Project

April 30, 2010

Abstract

A primary concern in businesses today is the protection of information and critical data. There are a number of laws, regulations, and standards that address the issue of security. The Payment Card Industry has published their own standards in order to protect customer information from theft and fraud. PCI DSS has become a significant standard in the protection of sensitive and confidential data but it only covers data that pertains to credit cardholder information. Because security is so broad it encompasses a variety of issues, this is why it is important for businesses to practice an approach to security that will include all aspects of their critical systems. This paper discusses PCI DSS, its use in different industries, how PCI DSS can be integrated with another security standard, ISO/IEC 27001, for a comprehensive, effective and sustainable information security program. This paper also includes an analysis and discussion of reported security breaches from the past five years, if the breach was credit card related, if the company had been compliant with the PCI DSS Standard at the time of the breach and what it means to the effectiveness of PCI DSS and if it is practical to have it as the lone security program.

Glossary

Acquirer – Bankcard association member that imitates and maintains relationships with merchants that accept payment cards

Approved Scanning Vendors (ASVs) – Organizations that validate adherence to certain data security standards requirements by performing vulnerability scans of Internet facing environments of merchants and service providers

Cardholder– Customer to whom a card is issued or individual authorized to use the card

Cardholder data – Full magnetic stripe or Cardholder name, expiration date, or service code

Card Validation Value or Code – Data element on a card's magnetic stripe that uses secure cryptographic process to protect data integrity on the stripe, and reveals any alteration or counterfeiting. May be referred to as CAV, CVC, CVV, or CSC

> **Type II** – Three digit values printed to the right of the credit card number in the signature panel area on the back of the card. This code is uniquely associated with each individual piece of plastic and ties the card account number to the plastic, May be referred to as CID, CAV2, CVC2, or CVV2

Consumer – Individual purchasing goods, services, or both

Information Security – Protection of information to ensure confidentiality, integrity, and availability (C.I.A)

Information System – Discrete set of structured data resources organized for collection, processing, maintenance, use, sharing, dissemination, or disposition of information

PAN: Primary Account Number is the payment card number (credit or debit) that identifies the issuer and the particular cardholder account. Also called Account Number

PCI DSS Self-Assessment Questionnaire (SAQ) – Validation tool intended to assist merchants and service providers in self-evaluating their compliance with the Payment Card Industry Data Security Standard

Qualified Security Assessors (QSAs) – Companies qualified by the PCI council to validate an entity's adherence to the PCI DSS

Service Provider – Business entity that is not a payment card brand member or a merchant directly involved in the processing, storage, transmission, and switching or transaction data and cardholder information or both. Includes companies that provide services to merchants, services providers or members that control or could impact the security of cardholder data

1. Introduction

"Information is power; those who have the information have the power" holds true in many facets of today's society, especially when it comes to technology and information systems. As technology advances more and more information is becoming available through mediums such as the Internet for easy access to the masses. Information security is a major concern for organizations of all sizes in all industries, particularly the Payment Card Industry. The Payment Card Industry Data Security Standard (PCI DSS) emerged from the security issues the industry was experiencing. This specialized data security standard has proven to be effective with those who are fully compliant but the PCI DSS standard is not broad enough to protect other types of sensitive information. Because data security is so important to the survival of a business, it is imperative that businesses guarantee all parts of their information systems and networks are protected and secure against any breach that may occur.

The objective of this project is to examine why integrating PCI DSS with another data security standard, namely ISO/IEC 27001 is a reasonable step to strengthen security practices and policies. This paper discusses the importance of PCI DSS, its application across industries, results from the analysis of reported security breaches over the past five years, and why the integration of PCI DSS and ISO/IEC 27001 is important and beneficial to organizations that handle cardholder information.

2. What is PCI DSS?

The PCI DSS is a set of policies and procedures for enhancing security of payment account data launched by the major credit card brands Visa International, MasterCard Worldwide, American Express, Discover Financial Services, and JCB International. In 2006 these brands joined together to form the PCI Data Security Standards Council, the governing body over the PCI Data Security Standard. The standard was designed as a uniform approach for the Payment Card Industry to enhance data security and to protect sensitive data of credit, debit and cash card transactions.

Who must be compliant?

Any organization or merchant, including e-commerce sites and retailers, regardless of size that process, stores, or transmits credit card data must comply with the PCI DSS.

Why PCI DSS?

Because the rate of credit card fraud and identity theft is rapidly increasing every year, millions of customers and businesses are affected every day. Demonstrating compliance with PCI DSS helps to maintain good business relationships between the service providers, merchants, and acquiring banks. The development of the PCI DSS is important to the Payment Card Industry because it minimizes the chances of compromise, it can be used as a measuring stick that gauges data security at the merchant level (GFI), limit risk, may increase revenue, protect consumer data, and help to gain consumer confidence in the industry.

Consequences of Non-Compliance

Credit card companies may enforce fines on institutions when they are found to be non-compliant with PCI DSS. When a security breach occurs, there are risks of reputation damage, financial risks, operational risks, and compliance risks. Consequences other than financial loss are cardholder data loss, and legal action taken by cardholders which could lead to loss of business.

3. Components of PCI DSS

Framework

The PCI DSS consists of twelve requirements and organized into six functional areas also known as the Control Objectives. Each of the control objectives has specific requirements that must be put in place in order to meet the PCI DSS objective. The various elements involved in the storage, processing, or transmission of cardholder data will customarily have different requirements and standards to meet, based on a number of parameters. Below are the Control Objectives and requirements for PCI DSS compliance.

Build and Maintain a Secure Network

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

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

Protect Cardholder Data

Requirement 3: Protect stored cardholder data

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

Maintain a Vulnerability Management Program

Requirement 5: Use and regularly update anti-virus software

Requirement 6: Develop and maintain secure system and applications

Implement Strong Access Control Measures

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

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

Requirement 9: Restrict physical access to cardholder data

Regularly Monitor and Test Networks

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

Requirement 11: Regularly test security systems and processes

Maintain an Information Security Policy

Requirement 12: Maintain a policy that addresses information security

Merchant Requirements and Levels

PCI DSS requirements (Appendix A: Merchant Levels and Requirements) for merchants are dependent upon the level the organizations falls into. There are currently four Merchant Levels for PCI DSS compliance and the Merchant Levels[1](Appendix A: Table 1) are based on the volume of cardholder transactions. However, the different payment brands have defined their own respective merchant levels based on transaction volume and what the requirements are. The requirements for service providers can be found on the PCI Council's website.

4. Real World Applications of PCI DSS

Higher Education

PCI DSS requires all merchants including Colleges and Universities to comply with the PCI requirements. Academic campuses worldwide accept credit and debit cards as a form of payment for tuition, bookstore purchases, tickets for events, and goods and services sold to the public, however, this acceptance of payment cards comes with the responsibility of protecting all transactions and consumer data. Many educational institutions have been unfortunately slow to achieve PCI DSS compliance (Reddy and Conway). Colleges and Universities are outstandingly vulnerable to confidential data being compromised due to open networks and/or insufficient security policies and procedures. Consequently, credit card companies and financial institutions view educational venues as risky merchants. In 2006 the

[1] http://usa.visa.com/merchants/risk_management/cisp_merchants.html
http://www.mastercard.com/us/sdp/merchants/merchant_levels.html
http://www.jcb-global.com/english/jdsp/index.html
http://www.discovernetwork.com/fraudsecurity/disc.html

education sector counted for 26% of data breaches but only 2%were credit card related (Reddy and Conway) and in 2008 31% and higher education counted for 79% of breaches within the education sector (Joseph E. Campana Ph.D).

Larger learning establishments practically always fall into PCI merchant levels 1-3 because they process so many credit card transactions for the variety of services mentioned above. The requirements ensure that colleges and universities implement specific policies and operating procedures surrounding their payment card infrastructure (Humphrey). In order to be considered compliant with the regulations, each department that processes cards must verify they are not storing cardholder data either intentionally or unintentionally and if any information must be retained, the data held must meet rigorous encryption standards identified in the PCI DSS standard. Colleges and universities benefit from being compliant with the PCI DSS standard such that they have the confidence of customers, sensitive information is protected, and if a breach of their credit card processing server does occur, they are not susceptible to the severe penalties that would be incurred if they were not compliant.

Healthcare

Healthcare institutions including hospitals, private practices, rehabilitation centers, and other healthcare facilities, are also included in the PCI DSS world, although most are not aware that the data security standards apply to the healthcare industry and even fewer are verifiably compliant. In both 2006 and 2008 the healthcare industry counted for 11% of reported security breaches in the U.S. but in 2006 only 2% were related to credit card and other financial information (Reddy and Conway) (InfoSecurityAnalysis.com). According to Jim Lacy, CFO of ZirMed “In 2009, virtually all healthcare providers take credit cards and virtually none of them are PCI compliant” but the in healthcare industry, data privacy and security standards are not foreign concepts. Other regulations such as HIPPA are mandated in order to protect patient data, but at the same time the greater part of the industry is not PCI compliant, why is this? First, some in the industry believe that they do not have any incentive to comply, but many of the larger credit card processors are strictly imposing PCI DSS compliancy and if a merchant is not found to be compliant, their ability to process credit cards will be denied. Second, healthcare officials believe it is too expensive, but there are several web-based PCI DSS services provided by PCI DSS certified security assessors for less than $200 a year. Thirdly, some believe that because they process a small amount of credit cards so PCI does not apply to them which is untrue. Companies that process any volume of credit cards must still meet the PCI DSS standards. Fourth, is the misconception that being HIPPA compliant is enough to secure all privacy and security entities; while HIPPA is one of the strongest mechanisms for ensuring security it is largely meant for the protection of

health information and being PCI DSS identifies risks and process gaps in other areas of security for added protection against potential compromises. Finally, experts within the healthcare industry suffer from a lack of awareness or misinterpreting the standard. In order to solve this dilemma this group of merchants needs to be properly educated on the risks, liabilities, costs, and processes (Lacy).

Although the healthcare industry counts for the least percent of reported breaches, it is still necessary that there is an awareness of PCI DSS and the industry as a whole begins to comply alongside the small portion of health providers. Along with HIPPA, PCI DSS protects the patients' sensitive data against credit card fraud and identity theft, which in turn allows the patient to feel confident and trust that their information is safe against criminals. Compliancy also minimizes the risk and costs that are incurred if a breach does occur and allows for the continued use of credit cards as a form of payment.

Business

Retailers, finance companies, banks, insurance companies, technology companies, e-commerce, hotels and other leisure companies large or small are a major part of the credit card industry worldwide. They process credit cards in a number of ways such as manual/offline credit card processing, real time credit card processing, and the use of payment services. Manual credit card processing is the use of a physical POS terminal which is mostly popular in retail environments. The real time processing method is usually used in companies that have a high volume of credit cards being processed, it is usually used with a payment gateway and the transaction is done instantaneously. Finally, the use of payment services such as PayPal is recognized worldwide, and is used for e-commerce transactions.

It is more obvious than not that the business sector must comply with PCI DSS, unfortunately as in other industries, a portion of the sector has not grasped PCI DSS and therefore is not yet compliant. The business sector has the greatest number of security breaches over all and greatest percentage of credit card compromises. In the U.S., in a survey done by the National Retail Federation, ControlScan, and the PCI Knowledge Base in 2009 it was discovered that there is a high awareness of the standard among small businesses but some are still not compliant. The majority of the respondents also believe that they were at low risk and safe from a data-loss breach (ControlScan, National Retail Federation, PCI Knowledge Base); this is a misguided response because small businesses are more likely to be compromised because they do hold cardholder information and most likely have less security for their systems. In other parts of the world being PCI compliant is just as important as in the United States. In the United Kingdom (U.K.) approximately 90% of retail, finance, and hospitality companies are still not compliant or may not be ready for compliance anytime soon. According to Guy Washer, Redshift

Research Managing Director, “all level one merchants understand that they must be compliant, but the smaller firms have more difficulty understanding what needs to be done.” (Bailey).

The business sector processes the majority of credit card transactions, and account for a large number of security breaches involving credit cards. A few reasons for this besides not being PCI DSS compliant are the use of weak processing software (i.e. point-of-sale software), outsourced IT companies and other third parties that are not very security conscious, and poor security practices by the merchant itself. These industries within the business sector use some critical information regarding credit cards such as the CVV2/CVC2 security codes and the PAN which are the keys to credit card fraud. While the PCI standard is a significant step in protecting credit card information, the merchant, and the service provider from a successful data breach many firms are having trouble becoming compliant.

Government

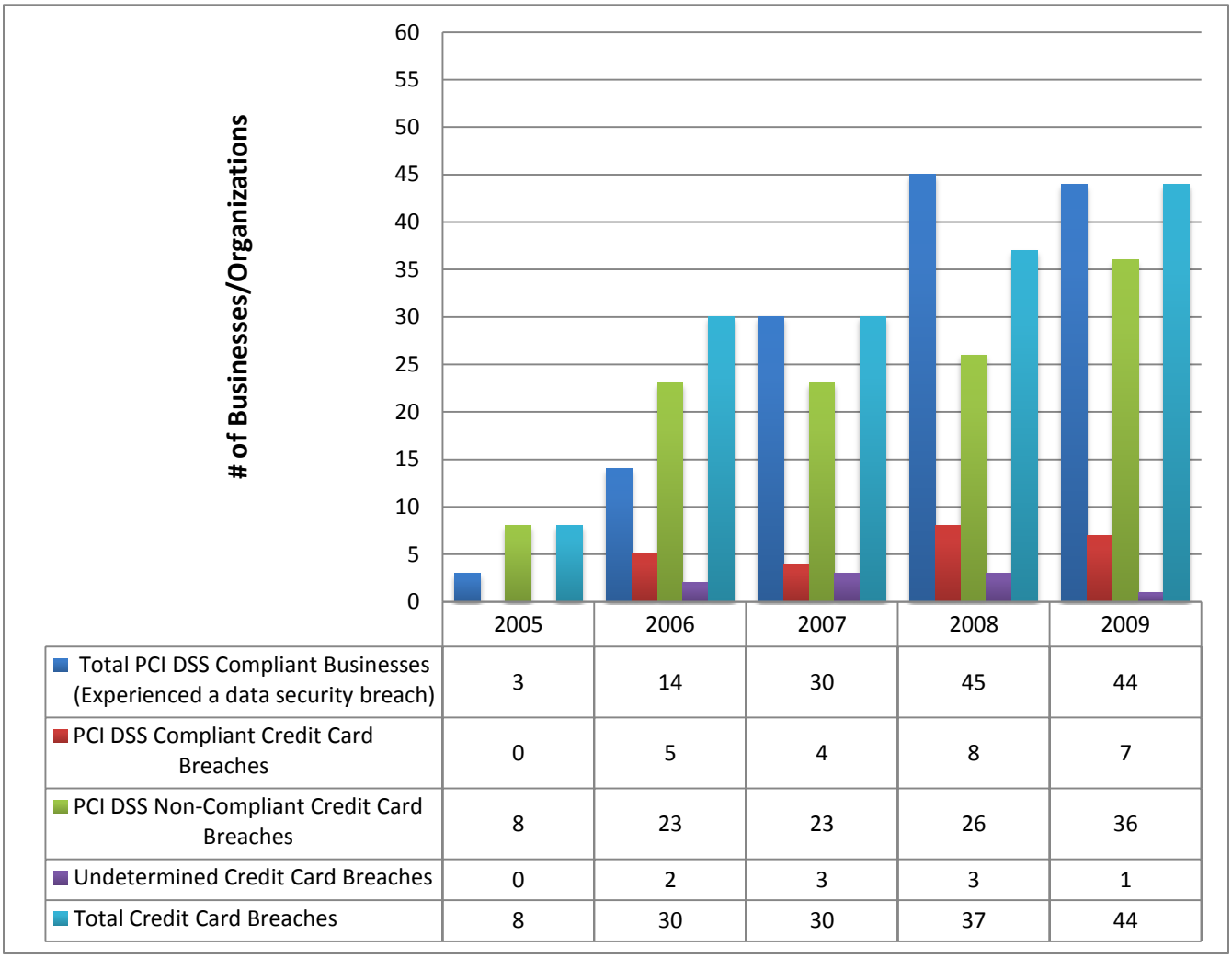
PCI DSS is not government regulation or law but agencies on all levels city/local, state, national, and international do experience some sort of security breach from privacy to credit card fraud. Government agencies are usually involved with e-commerce and use credit cards in instances of paying taxes online, renewing licenses or permits, and for recreational purposes. Governments are accustomed to using a third party to processes their payments and therefore need to not only have their own PCI DSS policy but ensure that their processor is also compliant.

5. Project Findings

Throughout the course of this project, security breach matrices provided by eFortresses were to be updated from the past five years (2005-2009). Unfortunately the PCI Council does not publish a list of compliant merchants. This is believed to be because the merchants use service providers or payment gateways to processes their credit card payments. However, both Visa and MasterCard publish lists of PCI DSS compliant service providers and payment gateways. This information was used as an advantage for the project because with some research it is possible to determine which service provider a merchant used. A vast majority of service providers require that their merchant be compliant to the payment card standard or they will not process credit cards for them; this did help with determining whether or not the listed companies were compliant. Other than using the Visa and MasterCard lists, the ways that this data was concluded are if the merchant/service specifically were stated they were compliant or not, press releases that covered this topic, and supporting documents that were found through the company.

The results

The following are the results found from doing research based only on the companies listed on the matrices given. The data states if the company was found to be compliant (yes), non-compliant (no), not able to be determined for lack of information, or do not process credit cards at all (N/A). All of these companies made this list because they had experienced a security breach of some type. Many companies are repeat offenders and others have become compliant through the years.



	2005	2006	2007	2008	2009
Total PCI DSS Compliant Businesses (Experienced a data security breach)	3	14	30	45	44
PCI DSS Compliant Credit Card Breaches	0	5	4	8	7
PCI DSS Non-Compliant Credit Card Breaches	8	23	23	26	36
Undetermined Credit Card Breaches	0	2	3	3	1
Total Credit Card Breaches	8	30	30	37	44

Chart 1 PCI DSS Compliant/Non Compliant Credit Card Breach Results

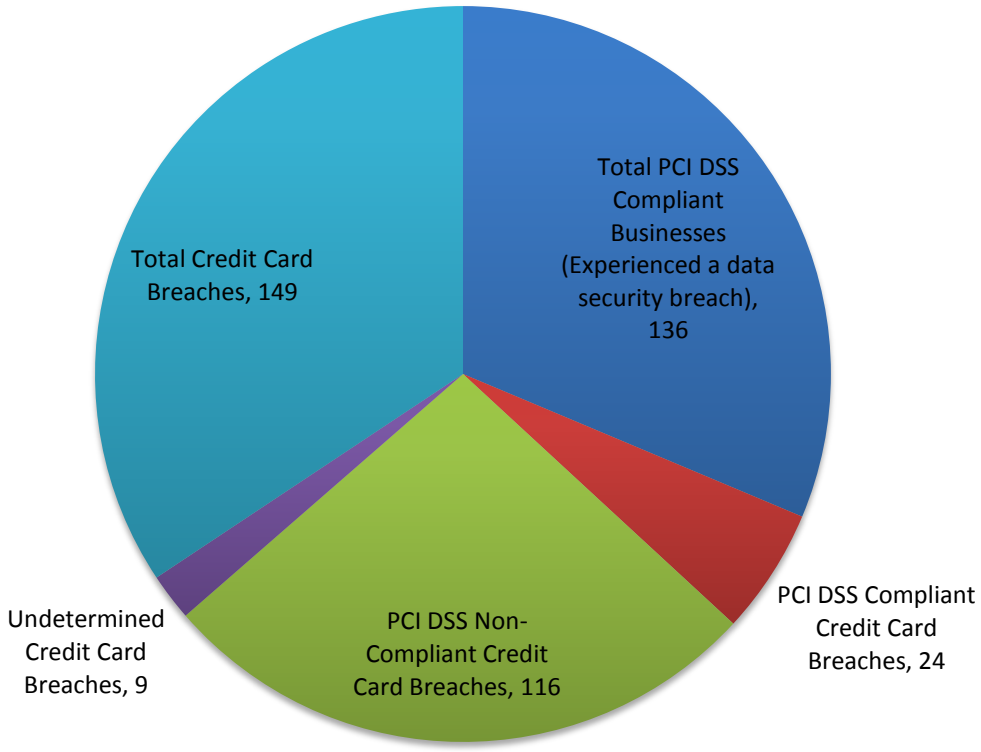


Chart 2 PCI DSS Compliant/Non Compliant Credit Card Breach Results 2005-2009 (As of March 2010)

Conclusions

From the resulting data it can be concluded that each industry does have its share of security breaches, however when it comes to compromises involving credit card information the business sector seems to have the greatest number of incidents that had occurred and the greatest number of compliant companies. In later years, beginning approximately in 2007 Education began to follow close behind business in number of incidents and compliant companies. The majority of the credit card compromises have been by companies that did not meet the PCI DSS standard, but in a few special cases there were a few organizations that had been complaint but still experienced breaches involving credit cards. Major breaches occurred in the business sector with companies such as CardSystems, TJX companies, RBS Worldpay, FirstData, and Heartland Payment Systems. As higher education institutions become compliant they were experiencing a reduction in credit card breaches and therefore are benefiting from the PCI DSS industry standard. The Healthcare and Government industries has had a

very minimal amount of reported breaches involving credit card data but has had significant amount of breaches involving other privacy and security regulations which are not the scope of this paper, but can be found in the eFortresses security breach matrices.

It can be difficult to pinpoint what exactly caused the successful penetration of seemingly secure systems; have different security challenges. A few reasons may be that the merchant may have contracted a non compliant service provider or payment gateway, the merchant itself was not fully compliant but claimed they were, there may be a intentional violation from inside by an employee, poor security practices by employees could cause an accidental breach, or the merchant had achieved compliance and did not maintain their compliance. Non compliant establishments usually do not have as strong security measures as compliant ones but those that do reach compliance must maintain and continually improve to remain secure and compliant.

It can be seen that the Payment Card Security Standard is not yet perfect. As technology advances, criminals will almost always find ways to try to get around security systems and gain unauthorized access to the sensitive information they seek, nevertheless, PCI DSS does make it difficult for this to occur and helps to reduce risk to the companies. As the standard evolves, organizations will also have to evolve and adjust to ensure that their systems are current and secure enough to process credit cards while keeping customer data safe.

6. ISO/IEC27001 and PCI DSS

What is ISO/IEC 27001?

The ISO/IEC27001 was published by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC) in 2005, it is a set of specifications intendedto maintain and establish an Information Security Management System or ISMS (ISO/IEC 27001). It involves a set of control objectives and controls that must be followed for certification.

- Establish an ISMS
- Manage the ISMS
- Monitor (Audit) the ISMS
- Review the ISMS
- Maintain and Improve the ISMS

Achieving ISO/IEC27001 certification standard can benefit an organization in that it provides a unified set of controls and simplified production of audit evidence attains legal compliance, improves risk management, business continuity, verifiable business credentials, and customer satisfaction. The

standard applies to several types organizations (i.e. government agencies, non-profit organizations, commercial enterprises) of all sizes where the misuse, loss, or corruption of its business or customer information could result in major impact for the organization.

Why Integrate ISO/IEC 27001 and PCI DSS

The PCI DSS and the ISO/IEC 27001 are not significantly different in their requirements for data security (Wright).Both are sets of standards concerning information security management for organizations; however both lack elements that would help to make them more secure, the good news is that both standards contain details that would supplement the other to make an organization have the best of both worlds. Even though they have the same goal of protecting and controlling consumer data, they differ in several ways. Similarities between the two are that they require regular audits and scans of systems to show compliance and perform industry best practices. On the other hand there are many differences. For example, the PCI DSS standard is mainly recognized in North America and Europe, compliance is mandatory, has functioning levels (Merchants and Service Providers), all standards are required and must be met, the separation of systems is high, flexibility is low, there is no mention of any prerequisite requirements for the management framework, and the PCI DSS applies to credit card holder information. Comparatively, ISO/IEC 27001 is internationally recognized, voluntary in compliance, the separation of systems is low, the degree of flexibility is high and there is little detail on how controls are actually implemented. However the corresponding code of practice - ISO/IEC 27002 provides more detailed guidance on how ISO/IEC 27001 controls are implemented.

The ISO/IEC 27001 standard is more flexible in terms of scope, controls, compliance, and enforcement (Wright) and designed to be applicable to a variety of organizations across industries around the world and to work with other standards and regulations. Because the standard is voluntary, the controls are more of a suggestion and the company may decide which controls are applicable to their particular scope. The controls in PCI DSS are much more strict and specific; companies must comply with each of the requirements listed in the standard. The strictness of the PCI DSS make it difficult for organizations to become compliant because of the variety of organizations and their functions, the lack of flexibility of the standard can be considered a hindrance on establishments like small businesses who happen to have a hard time achieving PCI DSS compliance. A comprehensive solution to fill the gaps between the two standards would be to integrate ISO/IEC 27001 and PCI DSS. Some of the requirements in PCI DSS are covered in ISO/IEC 27001 so while an organization meeting the requirements for one standard; parts of the other are being met also. While ISO/IEC 27001 is essentially focused on control objectives, PCI DSS has a combination of control objectives and its own specific

controls, and can compensate for ISO/IEC 27001's omission of the specific implementation of controls in ISO/IEC 27001. The two standards should also be integrated because PCI DSS is meant to deal with data security for credit card information therefore lacks objectives, scope, and management for other data and control measures. Using ISO/IEC 27001 covers all entities of information security that an organization may need including controls that embrace the PCI DSS standard. The ISO/IEC 27001 covers a broad spectrum of security for this reason the control objectives in the PCI DSS framework can be mapped (Appendix B: PCI and ISO/IEC 27001 Relationship Matrix with sections of the ISO/IEC 27001 primarily dealing with access control, communication, development and maintenance (ISO 27001 Implementer's Forum).

It can be concluded that a standard with such a specific design such as PCI DSS should be used in conjunction with a security standard such as ISO/IEC 27001 to successfully achieve a strong Information Security Management System (ISMS) that gives more understand to what controls are in place and being managed. Implementing the management systems aspect of ISO/IEC 27001 also ensures continuous improvement of an organization's information security program by embracing the proven Plan-Do-Check-Act continuous improvement cycle.

7. Summary

In any business or organization in every industry, protecting sensitive, confidential data is a top priority when it comes to information security. There are a number of laws, regulations, and standards that addresses concerns of this matter. But is complying with one law, regulation, or standard mean that an organization is fully secure against all security attacks against the organization? The logical answer would be…not necessarily. Many of the regulations pertain to particular industries or types of data security so there is almost always a chance that other parts of an information system are left vulnerable. The Payment Card Industry is a good example of this, although mandated their own strict standards for those establishments that deal with cardholder information, being compliant with only this standard may not be enough to keep an entire system secure. As shown earlier in the paper some, organizations that were found to be PCI DSS compliant were still compromised; of those, some breaches involved credit card information. Companies, especially those that manage cardholder information, can strengthen their information security program by combining ISO/IEC 27001 with PCI DSS to balance the elements in an information system that PCI DSS does not cover or vice versa.

In today's technological society, organizations are becoming more and more dependent on their information systems. Information is by and large the life line of the modern enterprise. Information

security has become a crucial initiative of all businesses. With new challenges and threats emerging almost daily, any breach to security can have a severe effect on the function, reputation, or survival of the organization. Appropriate steps should be taken to secure and protect information assets, it is no longer acceptable to just be compliant; organizations need to prove they are secure. If the proper steps are taken and security can be proven, the extra reporting and inspections can facilitate the combination of security and compliance programs to help control costs, keep systems and networks secure, and sustain compliance.

References

Bailey, Dave. "Survey Says 89 Per Cent of Firms Not Compliant with PCI-DSS." 4 March 2010. Computing.co.uk. 31 March 2010 <http://www.computing.co.uk/computing/news/2258889/survey-per-cent-firms-compliant>.

CISSP. "UK Firms Criticised for Non-Compliance with PCI DSS." 16 March 2010. CISSP.Com. 31 March 2010 <http://www.cissp.com/uk-firms-criticised-for-non-compliance-with-pci-dss-186>.

ControlScan, National Retail Federation, PCI Knowledge Base. "What Small Merchants Know (and Don't Know) about PCI Compliance." Research Report. 2009.

eFortresses.com. "Security Breaches Matrix." 2005-2010. <http://www.eFortresses.com>.

GFI Software. "PCI DSS Made Easy." White Paper. 2009.

Humphrey, Robert B. "Payment Card Industry Data Security Standard Compliance Implementation in Higher Education Network Environments." White Paper. n.d.

InfoSecurityAnalysis.com. Data Security Breach bu Industry/Vertical. 2008. 31 March 2010 <http://www.infosecurityanalysis.com/AllIndustries.html>.

ISO 27001 Implementer's Forum. "Mapping ISO 27001 Control to PCI-DSS V1.2 Requirements." 2009. ISO27001 Security. 3 April 2010 <http://www.iso27001security.com/ISO27k_Mapping_ISO_27001_to_PCI-DSS_V1.2.pdf>.

ISO/IEC 27001. 3 April 2010 <http://www.iso27001security.com/html/27001.html>.

Joseph E. Campana Ph.D, Cipp/G, CITRMS. How Safe Are We in Our Schools. Report. Madison, WI: J. Campana & Associates LLC, 2008.

Lacy, Jim. "PCI-DSS: Not on heath care provider's radar." 19 June 2009. SCMagazine. March 2010 <http://www.scmagazineus.com/pci-dss-not-on-health-care-providers-radar/article/138783/>.

PCI Security Standards Council. 2006-2010. January 2010 <https://www.pcisecuritystandards.org/index.shtml>.

Reddy, Dennis W. and Walter Conway. "Card at School: Why Banks View Campuses as High Risk Customers." AFP Exchange March 2007: 26-31.

Symantec. "PCI and Data Security." White Paper. 2009.

Verisign. "Enterprise Compliance Solutions for the Payment Card Industry." White Paper. 2006.

Visa Inc. Cardholder Information Security Program. 1996-2010. January 2010 <http://usa.visa.com/merchants/risk_management/cisp_merchants.html>.

Wright, Steve. Using ISO 27001 for PCI DSS Compliance. White Paper. UK: Siemens, 2008.

8. Appendix A: Merchant Levels and Requirements

Table 1: Credit Card Companies Merchant Levels

Level	Visa	MasterCard	JCB	American Express	Discover
1	Any merchant processing over 6,000,000 Visa transactions per year OR any merchant that Visa determines should meet the Level 1 merchant requirements to minimize risk to the Visa system.	Merchants processing over 6 million MasterCard transactions annually, identified b another payment card brand as Level 1	Merchants processing over 1 million JCB transactions annually, or compromised merchants	Merchants processing over 2.5 million American Express Card transactions annually or any merchant that American Express deems a Level 1	Merchants are currently not categorized into levels based on transaction volume. Discover takes a "risk based approach" for validating compliance
2	Any merchant processing 1,000,000 to 6,000,000 Visa transactions per year	Merchants processing 1 million to 6 million MasterCard transactions annually	Merchants processing less than 1 million JCB transactions annually	Merchants providing 50,000 to 2.5 million American Express transactions annually or any merchant that American Express deems Level 2	
3	Any merchant processing 20,000 to 1,000,000 Visa e-commerce transactions per year	Merchants processing 20,000 to 1 million MasterCard e-commerce transactions annually	N/A	Merchants processing less than 50,000 American Express transactions annually	
4	Any merchant processing fewer than 20,000 Visa e-commerce transactions per year, and all other merchants- regardless of acceptance channel-	All other MasterCard Merchants	N/A	N/A	

Table 2: Merchant Validation Requirements

<table>
<tr><th>Level</th><th>Visa</th><th>MasterCard</th><th>JCB</th><th>American Express</th><th>Discover</th></tr>
<tr><td>1</td><td colspan="3">Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV</td><td>Annual onsite review by QSA (PCI DSS Assessment) and Quarterly Network Scan by ASV</td><td rowspan="2">Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS Assessment and Annual Self Assessment Questionnaire</td></tr>
<tr><td>2</td><td colspan="3">Annual Self Assessment Questionnaire and Quarterly Network Scan by ASV</td><td>Quarterly Network Scan by ASV</td></tr>
<tr><td>3</td><td colspan="2">Annual Self Assessment Questionnaire and Quarterly Network Scan by ASV</td><td>N/A</td><td>Quarterly Network Scan by ASV</td><td rowspan="2">Quarterly Network Scan by ASV AND one of the following: Annual onsite review by QSA-PCI DSS Assessment and Annual Self Assessment</td></tr>
<tr><td>4</td><td>Annual SAQ recommended

Quarterly network scan by ASV if applicable

Compliance validation requirements set by acquirer</td><td>Annual Self Assessment Questionnaire

Quarterly Network Scan by ASV</td><td>N/A</td><td>Quarterly Network Scan by ASV</td></tr>
</table>

9. Appendix B: PCI and ISO/IEC 27001 Relationship Matrix

Figure 1: PCI and ISO/IEC 27001 Mapping

PCI DSS	ISO/IEC 27001 CONTROLS										
Requirement	A.5	A.6	A.7	A.8	A.9	A.10	A.11	A.12	A.13	A.14	A.15
1. Install & Maintain Firewall Configuration to maintain data							x				
2. Do not use vendor supplied defaults for systems, passwords and other security parameters						x	x	x			
3. Protect stored cardholder data						x		x			x
4. Encrypt transmission of cardholder data access open, public networks						x	x				
5. Use and regularly update anti-virus software						x					
6. Develop and maintain secure systems and applications		x				x	x	x			
7. Restrict access to cardholder data by business need-to-know						x					
8. Assign a unique ID to each person with computer access				x		x	x				
9. Restrict physical access to cardholder data			x	x	x	x					
10. Track and monitor all access to network resources and cardholder data						x	x				
11. Regularly test security systems and processes						x		x			
12. Maintain a policy that addresses information security	x	x	x	x		x	x		x	x	x

The following elements from the PCI DSS Requirements are addressed in the ISO/IEC 27001:

A.5: Security Policy

- Information Security Policy Document
- Review of the Information Security Policy

A.6: Organization of Information Security

- Addressing security in third party agreements
- Allocation of information security responsibilities
- Confidentiality agreement
- Contact with special interest groups
- Information Security coordination

A.7: Asset Management

- Acceptable use of assets
- Information of removable media
- Inventory of Assets
- Ownership of Assets

A.8: Human Resources Security

- Information security awareness, education, and training
- Removal of access rights
- Roles and responsibilities
- Screening
- Terms and conditions of employment

A.9: Physical and Environmental Security

- Cabling Security
- Equipment protection
- Physical entry controls
- Physical security perimeter
- Protecting against external and environmental threats
- Securing offices, rooms, and facilities

A.10: Communications and Operations Management

- Audit Logging
- Change control procedure
- Change Management
- Clock Synchronization
- Disposal of media
- Documented Operating Procedures
- Electronic messaging
- Fault Logging
- Information Backup
- Information exchange policies and procedure
- Management of removable media
- Managing changes to third party services
- Monitoring system use
- Monitoring
- Network Controls
- Network Security Management
- Physical media in transit
- Protection against malicious and mobile code
- Protection of log information
- Segregation of duties
- Separation of development, test and operational facilities
- Third Party Service Management

A.11: Access Control

- Access Control Policy
- Access Management
- Application and information access control
- Business Requirement for access control
- Clear desk and clear screen policy
- Equipment identification in networks
- Network Access Control
- Network Connection Control
- Network routing control
- Password Management System
- Password use
- Policy on the use of Network Services
- Privilege Management
- Remote diagnostic and configuration port protection
- Secure log-on procedures
- Segregation in Networks
- Sensitive system isolation
- Session Time out
- Teleworking
- Use of system utilities
- User Access Management
- User authentication for external connections
- User identification and authentication
- User password Management
- User Registration

A.12: Information Systems Acquisition, Development and Maintenance

- Change control procedure
- Control of internal processing
- Control of operational software
- Control of technical vulnerabilities
- Information Leakage
- Input data validation
- Key management
- Policy on the use of cryptographic controls
- Restrictions on changes to software packages
- Security requirements analysis and specification
- Technical review of applications after operating system changes

A.13: Information Security Incident Management

- Information Security Incident Management

A.14: Business Continuity Management

- Business Continuity and Risk Assessment
- Business Continuity Management

A.15: Compliance

- Compliance with security policies and standards
- Protection of organizational records