Insight to Payment Card Industry Data Security Standards (PCI DSS)

ACC 626 Research Paper – University of Waterloo

Robert Yang Xia
6/30/2011
Background information

The current trend of technology is headed toward the “paperless” direction. Cash transactions are gradually being replaced by debit or credit cards, even for smaller purchases. This raises security concerns as the merchant’s computer can capture the information embedded within the magnetic strips on the back of credit cards. This magnetic strip contains cardholders’ information such as account numbers, names, expiration dates, and security codes used to authorize certain purchases. The card-industry ruled that storing card information on merchants’ computers is prohibited, yet it has been proven that small merchants are unprepared and uneducated over the safeguarding of credit card information. According to Visa USA Inc, small merchants occupied 80% of cases involving unauthorized access to card data. Since these merchants are relatively unsophisticated with data security, sensitive information can be exposed to unauthorized third parties who can steal the information for fraudulent purchases. Although the cardholders are not liable of credit card theft, it still creates other problems such as the creation of a fake identity. Additionally, this problem became more of a concern when an aggregate of $1.24 billion was lost amongst U.S. financial institutions due to credit card fraud in 2006. Issuing banks suffered from merchants and service providers who were unmotivated to improve their security systems. It became evident that a unified governing body was needed to provide guidance over the card-industry and to restore the balance between issuing banks and service providers, where service providers should be held accountable for the losses.

There are three primary reasons that require business to store cardholder data: handling chargeback, providing customer service, and processing recurring subscriptions. The data collected by businesses are usually in two states: stored in databases or traveling across merchant networks. Both states, stationary and moving, require different methods of security measures as set out by Payment Card Industry Data Security Standards, known more commonly as PCI DSS. Point-of-sale (POS) and payment processing applications are also areas that exhibit the most risk exposure. The increase in both breadth and depth of cardholder data risk is a warning for a new system to govern and protect cardholders and organizations that handle credit cards.

History

Credit card companies initially developed and managed their own data security policies independently, including VISA’s Accounting Information Security, MasterCard’s Site Data Protection, and credit card fraud. Later on, they realized the need for a unified governing body to provide guidance and ensure the balance between issuing banks and service providers. This led to the development of the Payment Card Industry Data Security Standards (PCI DSS).

---


American Express’s Data Security Standards, Discover Card’s Information and Compliance, and the JCB Data Security Program. These programs were aimed to bring a minimum level of standards for merchants who transmitted and processed cardholder data. Due to the similarities amongst these standards, PCI DSS was established on December 16, 2004 in order to bring a common set of security standards for entities that were involved with card transactions. Visa and MasterCard became the centre piece as they took on major duties. For instance, MasterCard is responsible for the certification of products and companies who are capable of fulfilling the scanning requirements and Visa is responsible for training and certifying companies and individuals capable of fulfilling the onsite audit requirements. All other PCI organizations are also involved as contributors to the standards, although each card brand still maintains its own programs that go more in depth beyond PCI DSS. However, there is no doubt that PCI DSS provides a solid foundation for cardholder data security as the PCI Council constantly amends the standards to continuously adapt to new discoveries and changes in technological trends.

**PCI DSS Overview**

The PCI DSS known today is a set of comprehensive information security standards that provide supporting materials for organizations that operate with debit, credit, prepaid, e-purse, ATM, and POS cards to enhance card data security. This standard operates on a global scale for merchants that transmit card data. Additionally, it provides software developers and device manufacturers with the required guidance under the specific requirements. Before discussing the technical mechanics of PCI DSS, a few terms need to be defined first. Refer to Appendix A for a pictorial illustration.

- Visa and MasterCard are made up of Member organisations that can be either Acquirers or Issuers (or both)
- Acquirers are the Members of the Visa or MasterCard organisations which handle Merchants
- Issuers are the Members of the Visa or MasterCard organisations that issue the cards to cardholders
- Merchants are those entities who “accept” card transactions
- Service Providers are the entities that provide any service requiring the processing, storing or transport of card information on behalf of any of the above

In addition to developing security prevention and detection processes, PCI is also responsible for validating each organization’s compliance. For merchants that do not require an on-site data security assessment as per PCI DSS Security Assessment Procedures, Self Assessment Questionnaires (SAQ) need to be performed in order to become PCI DSS-compliant. Companies that require SAQs are typically

---

merchants that handle small volumes of transactions. On the other hand, companies that handle large
volumes of transactions, such as service providers that “transmit cardholder data on behalf of card
company customers, merchants, or other service providers”, require an annual validation procedure done
by an external Qualified Security Assessor (QSA)\(^5\). All major credit card companies first define each
service provider into different levels based on criteria such as transaction volume. Each level then guides
the service providers to their respective validation requirements. Appendix B provides and explains both
the merchant and service provider levels and the respective requirements in detail\(^6\).

There are six basic goals adhering to PCI DSS and each goal is comprised of specific requirements.
Each goal is composed of additional procedures and requirements to be fulfilled outlined as follow:

- **Goal 1**: 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

- **Goal 2**: Protect cardholder data
  - Requirement 3: Protect stored data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks

- **Goal 3**: Maintain a vulnerability management program
  - Requirement 5: Use and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications

- **Goal 4**: 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

- **Goal 5**: 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

- **Goal 6**: Maintain an information security policy
  - Requirement 12: Maintain a policy that addresses information security for all personnel

In short, there are 6 principles, 12 requirements, 45 sub requirements, 75 detailed requirements and other
relevant testing procedures contained within PCI DSS 2.0 version which was released October 2010. To

---


4
efficiently design a compliant IT environment, six steps should be followed to avoid haphazard and unnecessary costs:

1. Identify business processes with card data
2. Focus on shrinking the scope
3. Identify where the data is stored
4. Determine what to do about data
5. Determine who needs access
6. Develop and document policy

It is crucial to understand that becoming compliant to PCI DSS is more than just a one-time project. In fact, it is a program that requires constant monitoring and maintenance involving more than just the IT department. Security is a process, not an event. This process should be initiated from the upper management team and established as an overall strategic initiative.

In general, the goal of PCI DSS is to prevent major security issues and reduce the risks of payment card transactions by raising security awareness amongst the merchants and service providers. PCI sets to enhance business processes by taking away the burden of data security from business owners and eliminating costly and risky data storage when possible. PCI operates on a global forum and monitors any business dealing with credit cards. Failure to conform will result in penalties issued by the PCI Security Standards Council.

**Awareness**

According to the same survey done by Ponemon Institute, 71 percent of the companies surveyed do not view PCI as a strategic initiative and more than half of them believed that their CEO does not embrace PCI DSS compliance as a value-added security vehicle. Chart 1 of Appendix C presents other attributions about the organization’s PCI data security posture and management’s belief regarding PCI compliance. Despite the negative attitude against PCI DSS, the survey showed that 75 percent of organizations achieved some level of compliance, while 22% achieved full compliance (see chart 2 of Appendix C). In addition, organizations are often unclear as who should be responsible for PCI DSS compliance (see chart 3 of Appendix C). Furthermore, 23 percent of organizations surveyed believed that Certified Information Security Officer (CISO) should be held accountable; while 21% believed that no one person should be responsible for PCI compliance. This means that the process of achieving PCI compliance will be inefficient and more time consuming. Additionally, staff members that are hired solely for the purpose of PCI compliance will prove to be costly.
Effectiveness and Cost

Since the inception of PCI DSS, many have questioned its effectiveness to protect sensitive cardholder data. Compliance with PCI DSS requirements demands changes to existing business systems. In the past, many of these changes proved to be costly and altered business infrastructures. Particularly for smaller business, the implementation of business data infrastructure, including access controls, secured network, and information security policy, can deteriorate the business’ cash flow and can possibly outweigh its potential benefits. Critics have challenged the effectiveness of PCI DSS with compelling facts and statistics. For instance, Hannaford Brothers, a PCI DSS compliant grocery chain, lost 4.2 million credit card numbers in 2008. Furthermore, Ponemon Institute conducted a study that collected information from officers representing 517 multinational IT and IT security practitioners who were involved with their companies' PCI compliance. The study shows the following findings:

- Cost of PCI is, on average, 1/3 of the overall security budget
- 79% have had a data breach
- 55% of companies focus only on protecting the credit card data but not other sensitive information
- There is uncertainty as to what personnel are the most accountable for PCI-DSS compliance
- Smaller companies are less compliant than larger companies

It is evident from the above statistics that PCI favours larger companies with more luxurious security budgets. Cost is an apparent obstacle for smaller companies to be PCI DSS compliant. Merchants are increasingly facing the dilemma between the risk of losing cash flow and penalties for being non-compliant to PCI DSS. Statistics have showed that on average, level 1 merchants, merchants dealing with more than 6 million transactions per year, spent $US 3.38 million to become PCI compliant in 2008 and an aggregate of $1 billion was spent since 2006 since the introduction of PCI DSS. Larger and well-budgeted companies are able to achieve better compliance with more cost effective solutions. On the contrary, smaller companies have fewer resources and often have difficulty in interpreting the standards and subsequently drafting a plan. In addition to the confusion caused by the administrative aspects of compliance, PCI standards appear to be an incomplete security measure. Businesses comply with PCI DSS for the mere reason to be operationally functional legally and PCI DSS becomes nothing more than a checklist of rules. This means that most businesses attain the minimum standard just to adhere to the PCI DSS but are not really thinking about security. Moreover, 55% of the companies surveyed showed interest only in protecting credit card data and neglected other confidential information such as social security numbers and addresses. In other words, PCI DSS did not attain its purpose of enforcing security.

---

and protecting systems against threats. It is not a complete cure to cardholder data breaches. Therefore, being PCI compliant does not imply security.

QSAs claimed that more than 50 percent of companies do not take a proactive approach in managing data security and 54 percent of the companies are overwhelmed by the cost of PCI DSS compliance. Another issue raised was the segregation between a department that handles the IT budget and the department that implements IT functions. Most business units allocate a budget for PCI compliance while the IT security group is responsible for the compliance procedures. This creates a mismatch of investment and expectation of outcome.

### Positives of PCI DSS

Despite unfavorable evidence, PCI DSS is not necessarily ineffective and can be examined from a contrary view by scrutinizing the purpose of the standard. The primary goal of PCI is aimed at reducing the risk of transaction and raising awareness of key aspects of data security. In this light, PCI fulfilled its objectives as businesses are spending more on system security and are forced to be compliant with PCI DSS. Although it still does not guarantee absolute security, the risks faced by card brands and cardholders have been significantly reduced. PCI DSS should be viewed as a valuable foundation that a good security system can be built upon. Surveys suggest that PCI was effective in persuading organizations to encrypt their data, and evidence also suggests that there has been a decline in theft of card data in the stationary state. In addition, complying with PCI DSS brings a competitive edge through building brand trust, limiting risk exposure, and therefore increasing revenue. Moreover, another advantage of becoming compliant to PCI DSS is that it grants the business the safe harbor status. This means that in the event of a security breach, PCI DSS compliant business will be pardoned from being fined, and courts will also be more lenient with PCI compliant businesses if they are sued by customers. Non-compliant businesses that handle credit cards are subject to audits, fines, lawsuits, and the penalty of losing the right to process credit cards.

A true security system requires personalization that addresses the specific needs of each individual company. PCI DSS should be the baseline for the overall security program and additional steps should be taken after assessing the business’ overall controls and risks. According to VeriSign Global Security Consulting Services who conducted many PCI assessments over the past years, 79 percent of the companies are overwhelmed by the cost of PCI DSS compliance.

---


percent of assessed business failed the audit due to lack of data protection. Interestingly, non-technical issues such as the lack of IT policies, controls, and governance were the primary issues that caused the failure. Proper governance should be structured in place to ensure the success of PCI compliance. Risk assessments should be done outside of PCI scope as a supplement to PCI standards.

**PCI in Canada**

Canadian businesses have a particular interest in these developments since Canadians are among the world’s most frequent users of payment cards. However, Canada has lagged behind Europe in adopting Chip & PIN technology on credit cards, making itself an alluring target for international data thefts. According to the Canadian Bankers Association, the total value of reported payment card fraud exceeded half a billion dollars in 2008.

Due to the lack of privacy laws and a large base of small and medium-sized enterprises (SME), Canada is a primary target for identity and data theft. These SMEs lack the awareness and resources to adequately secure their confidential data and their computers are often left unsecured. In addition, even government bodies such as the Royal Canadian Mounted Police (RCMP) and Passport Canada do not have sufficient control and governance over their data protection policies. IT security experts have surveyed and discovered that Canadian consumers did not exhibit confidence over the security of their personal data held by institutions and banks, but fortunately, Canadian legislators quickly grasped this concept and recognized the need to improve Canadian laws over the protection of consumers’ data. Consequently, the PCI DSS adopted by the United States became a favourite model to meet Canadian needs. Due to the frequency and magnitude of US-Canadian business involvement, the implementation of PCI DSS in the US reduced the number of cases of Canadian data theft. Thus, PCI DSS became a suitable candidate to protect Canadian consumers.

However, during the early stage, there has been much debate in Canada regarding the introduction of PCI DSS. Although Canada was looking for a way to protect cardholder data, many have opposed the act of legislating PCI DSS. Arguments have been made that the existence of Personal Information Protection and Electronic Documents Act (PIPEDA), which regulates and protects personal data and other sensitive information, was a sufficient system to guarantee security in Canada and that PCI DSS can be used merely as a framework to enhance data security.

Canada was evidently distant behind the U.S. in the implementation of IT security. The federal Personal Information Protection and Electronic Documents Act (PIPEDA) and the Privacy Act only imposed insubstantial penalties to violators such as a notice of offence. The U.S. privacy laws, on the other hand, enforced strict policies that encouraged organizations to have strong IT security. The weak governing body was coupled with consumer concerns where only 0.5% of the consumers surveyed were confident that retailers could protect their online personal information, 9% were confident that major
financial institutions could safeguard their online information and only 36% of Canadian IT security executives surveyed believed that their company could exercise sufficient control to safeguard customer data.\textsuperscript{11}

However, the forthcoming of PCI DSS also brought Canadian businesses trouble. Because of the delay in PCI implementation in Canada, many Canadian businesses became disoriented during the initial implementation stage due to lack of guidance and inconsistency in deadlines with their U.S. counterparts. The initial tight deadlines were dreadful for Canadian businesses, especially for SME, as they had a difficult time in interpreting the standard and little time to become compliant. In addition, SME in Canada complained that the cost of implementing PCI DSS greatly outweighed the potential penalty for being non-compliant. Consequently, many have resisted the implementation of PCI DSS.

**Technologies Involved**

There are a few technologies that enable cost effective compliance of PCI DSS. Among them, firewalls, anti-virus, anti-malware solutions, and encryption for data at rest and in motion ranked the highest. The survey also indicated that perimeter, location surveillance systems, website sniffer and crawlers appeared to be the least used out of the 18 technologies. QSAs believe that encryption is the most effective technology for data in motion and firewalls and encryption are amongst the most effective technologies for data at rest.

Another interesting observation noticed was that only 2 percent of organizations assessed by QSAs fail, but 41 percent of organizations that pass the audit do not rely on mechanisms prescribed by the PCI DSS. Rather, compensating controls are used because the organizations deem the technology prescribed by PCI DSS to be infeasible. However, compensating controls can only serve as a temporary solution. As the reduction in future cost in technology, organizations need to adapt PCI DSS’ prescription.

**PCI DSS - Accounting Firms & Job Creation**

Since the inception of PCI DSS, accounting firms have been actively seeking ways to extend the breadth of their services and expand their services in the IT control and security industry. Major accounting firms such as Grant Thornton International Ltd earned their certification to become a Qualified Security Assessor (QSA)\textsuperscript{12}. Accounting firms are trying to establish the highest integrity and exhibit the highest level of competency in delivering PCI assessments. Increasingly, accounting firms are also


delivering IT consulting services incorporating PCI DSS compliance combined with process, controls, and other advisory services. The public has generally recognized that accounting firms’ auditing experience is of a great asset to assist them with PCI DSS assessment related works. Additionally, services offered by accounting firms such as internal controls audit and information security correspond to the skills necessary to assess card transaction security. An assessor should have an assurance background and experience to confirm compliance.

Accounting firms will experience an increase in revenue due to the extended service line because they have a great reach to businesses and a solid client base. Compliance to PCI DSS is required by every business that handles credit card information, and thus, accounting firms can offer a more complete and one-stop-for-all services. Combined with their knowledge for existing clients and various industries, accounting firms will be able to add value to their service packages.

The complexity of PCI DSS also triggers an additional line of service for savvy solution providers that help businesses to implement the system, reduce costs, and educate their clients. As the new 2.0 version emerges, businesses are rushing to update their systems while still struggling to grasp the existing mandate. The win-win opportunity arrives as savvy solution providers can handle PCI compliance projects and keep businesses focused on their main line of services. These solution providers also specialize in ensuring project efficiency and avoid redundancies in process and technology, which greatly enhances cost-savings for many businesses. A recent study done by the Aberdeen Group claimed that half of the cost can be saved by hiring solution providers.

Conclusion

Although PCI DSS has apparent weaknesses and does not guarantee absolute security and safeguarding of cardholder data, it has enhanced the security over cardholders’ data to a great extent. PCI DSS should be kept in place and possibly implement minor changes to improve its efficiency and effectiveness. It has helped raise awareness of data security in the business world and encouraged many organizations to implement IT security systems. Additionally, PCI DSS has improved consumer confidence over the security of personal information to a great magnitude. Fraudsters are also forced to exploit more sophisticated data breach methods and overthrow traditional methods. This means that PCI DSS needs to remain alert to face emerging threats.

Despite all the positive aspects of PCI DSS, it is by no means the end of IT security development. Each organization should assess its needs for security and develop a more company-specific solution, using PCI DSS as the foundation. Companies should feel responsible for the safekeeping of consumer data and continually enhance their IT policy, governance and system. No standard can ever guarantee absolute security, and it is dependent on each company’s effort to develop a complete and secure data storage system. PCI should be the “floor” of security and should not be treated as a “ceiling”.
Recommendations

The surveys and studies used to construct this report have led to the identification of some deficiencies and concerns raised regarding PCI DSS. The following recommendations can help address some of the issues and concerns involving PCI DSS.

- Tailor the compliance requirements to the specific needs and business environment of each organization. Smaller companies do not need the same security measure as larger firms. Smaller companies also lack resources to comply with complex policies and requirements.

- Develop a more cost-effective framework to benefit small to medium sized companies. If the cost to comply with PCI DSS is greater than the penalty it imposes for non-compliance, businesses are discouraged to adopt PCI DSS. The above recommendation is a possible method to reduce costs where smaller companies should have less complex requirements and procedures.

- PCI Council should provide additional support and educate company executives on the role and importance of PCI DSS as part of a company's overall strategy. Company executives often only fulfill the minimum regulatory requirements and fail to realize the potential role that PCI DSS can take on as part of a firm's overall IT governance. This is especially true for small businesses where the owner lacks IT security knowledge and often do not use PCI DSS to its fullest extent.

- PCI Council should improve its overall brand image and raise awareness of its brand value amongst the general public. It should subsequently create a compliance logo for each compliance business to display in-store or online. The purpose of this recommendation is to inform consumers that companies have taken additional security measures and have the capability to safeguard consumer confidential data. This can in turn encourage more companies to invest in security or improve the existing security system in order to gain a competitive advantage. PCI DSS can thus become a value-added requirement and businesses will be more willing to pay for its fees.

- Designate the responsibility of PCI compliance to a defined personnel or a team within an organization to implement a company-wide security program. This team should initiate the implementation of PCI DSS and provide subsequent support upon implementation. Additionally, the team should be held accountable for the degree of utilization of PCI and integrate PCI as the foundation of the company's overall security governance. This recommendation is more practical for larger firms with bigger IT security budgets, resources, and personnel.
Appendix A – Related Parties within PCI DSS
## Appendix B - Merchant and Service Provider Levels and Validation Requirements

<table>
<thead>
<tr>
<th>MERCHANTS</th>
<th>ON-SITE AUDIT</th>
<th>SELF-ASSESSMENT</th>
<th>NETWORK SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any merchant - regardless of acceptance channel - processing over 6,000,000 transactions per year.</td>
<td>Required Annually</td>
<td></td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any merchant that has suffered a breach that resulted in an account data compromise.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>Any merchant that card network provider, “at its sole discretion,” determines should meet the Level 1 merchant requirements to minimize risk to their respective system.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any merchant - regardless of acceptance channel - processing 1,000,000 to 6,000,000 transactions per year.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any merchant processing 20,000 to 1,000,000 e-commerce transactions per year.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 4</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any merchant processing fewer than 20,000 e-commerce transactions per year, and all other merchants – regardless of acceptance channel – not in Levels 1, 2, or 3.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>SERVICE PROVIDERS</th>
<th>ON-SITE AUDIT</th>
<th>SELF-ASSESSMENT</th>
<th>NETWORK SCAN</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Level 1</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>All processors and all payment gateways.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 2</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any service provider that is not in Level 1 and stores, processes, or transmits more than 1,000,000 accounts or transactions annually.</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td><strong>Level 3</strong></td>
<td></td>
<td>Required Annually</td>
<td>Required Quarterly</td>
</tr>
<tr>
<td>Any service provider that is not in Level 1 and stores, processes, or transmits fewer than 1,000,000 accounts or transactions annually.</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Appendix C – Survey Results

Chart 1

Attributions about the organization’s PCI data security posture

- My organization does not view data security as a strategic initiative across the enterprise: 71%
- My organization does not have sufficient resources to achieve compliance with PCI DSS: 60%
- Compliance with PCI DSS does not improve our organization’s data security posture: 56%
- My organization’s CEO is not a strong supporter of PCI DSS compliance efforts: 55%
- My organization is not proactive in managing privacy and data protection risks: 52%

Chart 2

Organizations compliant with PCI DSS requirements today

- Yes, for all applications and databases across the enterprise: 22%
- Yes, for most applications and databases across the enterprise: 28%
- Yes, but only for some applications and databases across the enterprise: 25%
- No: 25%

---

**Chart 3**

- **IT security leader (CISO)**: 23%
- **No one person**: 21%
- **CIO**: 19%
- **Legal**: 15%
- **IT compliance**: 9%
- **CTO**: 8%
- **Internal audit**: 2%
- **Privacy officer or leader (CPO)**: 2%
Bibliography


## Appendix D – Annotated Bibliography

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
</table>

- Why PCI exists, its purpose and objectives
- Introduction to Cybercrime, ID theft and credit card fraud
- How PCI is designed to deal with the issues above and the book discusses the risks of non-compliance
- The book introduces compliance standards and introduction to the actual mechanism for compliance validation
- Common myths and misconceptions of PCI DSS are examined (page 115 for details)
- Managing a PCI DSS project to achieve compliance
  - Figure out needs of the business
  - The level of validation
  - Sponsorship
  - Staff training and education
- History of PCI
- Reputation, Financial, Compliance and Operational aspects of PCI DSS and how they can impact a business
- Definitions of professional terms
- Illustration of payment card transactions and problems involved in each sub-procedure.
- Merchant level Vs Service Provider Level
- Strategies and risks for businesses that are seeking to comply with PCI
- PCI breakdown – control objectives and associated standards
- Maintain a vulnerability management program
- Implement strong access control measures
- Regularly monitor and test networks
- Maintain an information security policy
- Assessment and remediation

**Overview:**

“The PCI Security Standards Council offers robust and comprehensive standards and supporting materials to enhance payment card data security. These materials include a framework of specifications, tools, measurements and support resources to help organizations ensure the safe handling of cardholder information at every step.”

- “The keystone is the PCI Data Security Standard (PCI DSS), which provides an actionable framework for developing a robust payment card data security process - including prevention, detection and appropriate reaction to security incidents.”
- Defined by the Payment Card Industry Security Standards Council, “the standard was created to increase controls around cardholder data to reduce credit card fraud via its exposure”. Validation of compliance is done annually - by an external Qualified Security Assessor (QSA) for organizations handling large volumes of transactions, or by Self-Assessment Questionnaire (SAQ) for companies handling smaller volumes.
• PCI DSS is enforced by transaction processor known as Aquirer
• PCI DSS’ compliance is managed by brand name cards (VISA, MasterCard and etc)
• Organizations are categorized by:
  o type of payment processing they perform
  o the volume of transactions or accounts processed and,
  o the payment channels used.
• Merchants that take payments as well as service providers that process credit card information are grouped in levels based on these secondary factors.
• Merchant levels & Validation Requirements
  o Each merchant follow different PCI Validation Requirements depending on its ‘merchant level’. Each brand name card also has different definition for each level. For illustration for Visa, MasterCard and Amex, please refer to the charts on the website for detail (too long to paste it in this document)
• Service Provider Level & Validation Requirements
  o Service Providers “process, store or transmit cardholder data on behalf of card company customers, merchants or other service providers”.
  o Service Provider Level requirements also vary by card company. Please refer to the charts on the website for detail (too long to paste it in this document)
PCI security standards
- Both technical and operational requirements
- Set by Payment Card Industry Security Standards Council to protect cardholder data
- It is governed globally for all merchants and organization.
- It provides specific guidelines and requirements for software developers that create applications used in transaction process
- PCI also provides requirements for manufacturers of devices.
- It is enforced by major card brands such as MasterCard Worldwide, Visa Inc, American Express, Discover Financial Services, and JCB International

Payment Application Data Security Standard (PA-DSS)
- It is a standard for software developers and integrators of applications that store, process or transmit cardholder data as part of authorization or settlement.
- It governs these applications that are sold, distributed or licensed to third parties.

PCI Data Security Standard for Merchants & Processors (see website for detail)
- Six Goals
- 12 corresponding PCI DSS requirements
- And many sub-requirements

The PCI DSS specifies and elaborates on six major objectives.
- Build and maintain a secure network
- Protect Cardholder data
- Maintain a vulnerability management program
The article stated all the necessary steps that should be taken to ensure all objectives can be reached.

**PCI Data Security Standard for Merchants & Processors**

The PCI DSS is the global data security standard that any business of any size must adhere to in order to accept payment cards. It presents common sense steps that mirror best security practices.

<table>
<thead>
<tr>
<th>Goals</th>
<th>PCI DSS Requirements</th>
</tr>
</thead>
<tbody>
<tr>
<td>Build and Maintain a Secure Network</td>
<td>1. Install and maintain a firewall configuration to protect cardholder data</td>
</tr>
<tr>
<td></td>
<td>2. Do not use vendor-supplied defaults for system passwords and other security parameters</td>
</tr>
<tr>
<td>Protect Cardholder Data</td>
<td>3. Protect stored data</td>
</tr>
<tr>
<td></td>
<td>4. Encrypt transmission of cardholder data across open, public networks</td>
</tr>
<tr>
<td>Maintain a Vulnerability Management Program</td>
<td>5. Use and regularly update anti-virus software or programs</td>
</tr>
<tr>
<td></td>
<td>6. Develop and maintain secure systems and applications</td>
</tr>
<tr>
<td>Implement Strong Access Control Measures</td>
<td>7. Restrict access to cardholder data by business need-to-know</td>
</tr>
<tr>
<td></td>
<td>8. Assign a unique ID to each person with computer access</td>
</tr>
<tr>
<td></td>
<td>9. Restrict physical access to cardholder data</td>
</tr>
<tr>
<td>Regularly Monitor and Test Networks</td>
<td>10. Track and monitor all access to network resources and cardholder data</td>
</tr>
<tr>
<td></td>
<td>11. Regularly test security systems and processes</td>
</tr>
<tr>
<td>Maintain an Information Security Policy</td>
<td>12. Maintain a policy that addresses information security for all personnel</td>
</tr>
<tr>
<td>Author</td>
<td>Title of Article</td>
</tr>
<tr>
<td>----------------</td>
<td>-----------------------------------------------------------------------------------</td>
</tr>
</tbody>
</table>

**Background information:**

- Increasing plastic card usage all over the globe
- Small merchants are unaware that security rules existed and some of them have been storing confidential data of their customers
- U.S. financial institutions that issue credit cards incurred a record $1.24 billion of losses from fraud last year, up 9.3% from 2005, according to Nilson Report, an industry newsletter based in Carpinteria, Calif. Most credit-card fraud, by dollar volume, tied to merchants occurs because hackers broke into the networks of big retailers.
- VISA and MasterCard Inc. joined forces to educate small merchants

The following is a list of specific issues to consider related to PCI-DSS. This should help ensure that organizations can not only meet the letter of PCI, but actually make their systems more secure:

- Implement a security program
- Know your assets
- Build and maintain a document library
- Awareness and training
- Your auditor is your friend
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
</table>

Payment Card Industry Digital Security Standards
- A collaborative effort to achieve a common set of security standards for use by entities that process, store or transport payment card data.
- Multiple Credit Card organisations participating in PCI efforts
- Members include Visa, MasterCard, American Express (Amex), Diner’s Club, Discover Card, and JCB
- Established on December 16, 2004
- MasterCard is responsible for certifying products and companies capable of fulfilling the scanning requirements
- Visa is responsible for training and certifying companies and individuals capable of fulfilling the onsite audit requirements.
- All other PCI organizations are also involved as contributors to the standards


- VISA Service Provider Levels Defined
- American Express, Discover, JCB, MasterCard Service Provider Levels Defined
- VISA Service Provider Validation Requirements Defined
- American Express, Discover, JCB, MasterCard Service Provider Validation Requirements Definitions are listed in the charts on the website.
Cost Vs Benefit

- The process of becoming compliant with PCI DSS may require system upgrade if the system of one’s business does not meet PCI DSS requirements. Such upgrade proved to be costly.
- The costly upgrade can provide the organization with safe harbor status in the event of security breach. When a business is being sued by customer, the safe harbor status will increase the chances that the court to side with the business.
- The business may also be fined and audited for not being compliant with PCI DSS. Additionally, the business may be banned from processing credit cards.

Credit Card Frauds & history of PCI DSS in Canada

- 25% of identity theft is due to credit card fraud in the U.S. in 2006, amount to a total of $50 billion loss.
- Other significant card data theft incidents were listed including TJX’s experience of losing 45 million customers’ credit/debit card numbers.
- Non-compliance to PCI DSS may lead to:
  - Lawsuits
  - Cancelled accounts
  - Payment card issuer fine (up to $500,000 per accident)
  - Government fines
  - Insurance claims
  - Loss of ability to process payment card transactions
- PCI DSS in Canada
  - Provide sufficient framework to enhance IT security
  - Organize different types of organizations such as companies, government, service providers and other merchants with a
unified system.

- IBM Canada security architect Gary McIntyre said “Canadian firms that failed to achieve PCI compliance would not likely get disconnected from the card networks, but they would face stringent financial penalties from Visa or MasterCard”.

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, data base, website, link</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>Initially, Canada wasn’t sure if it should implement PCI DSS</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>But Canada needed ways to protect cardholder data</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Canada already had PIPEDA which regulates and protects personal data and other sensitive information</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Canada needs a unified standard, rather than having a stand-alone standard in each province</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Distinguishes between Merchants and Service Providers</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Levels of each subset is defined and requirements are summarized in charts on the website</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consequences of not complying</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Merchants – lost trust, money and brand image</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Service Providers – card reissues in addition to merchants</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Consumers – putting personal confidential information at risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td></td>
<td>Other risks include Financial Risk, Reputation Risk, Operational Risk, and Compliance Risk</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

For illustration, refer to the following chart:
Malik, Javvad  
Is PCI DSS useless?  
Infosec Island  
n.a.  
2010  
1  
May 28, 2011  

- Cases where companies had PCI DSS certification but still suffered data breach
  - E.g. Heartland and RBS WorldPay
  - PCI DSS may be the beginning of a security model
- How effective is it?
  - Decline in card data theft while stored in company system since implementation of PCI DSS
  - However, in-transit data theft increased
    - This suggests insufficient data encryption with regard to requirement 4 set out by PCI DSS
  - PCI DSS increases companies’ awareness over security
  - PCI DSS is a mere minimal baseline for security
  - PCI DSS needs further improvement and enhancement.
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
</table>

“The fact is you can be PCI-compliant and still be insecure. Look at online application vulnerabilities. They're arguably the fastest growing area of security, and for good reason — exposures in customer-facing applications pose a real danger of a security breach.” – Greg Reber

<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
</table>

Miachel Jones, CIO of Michaels’ stores, testify that:
- PCI DSS is expensive to implement
- Confusing to comply and also very subjective in interpretation and enforcement
- Tremendous amount of work i.e. 12 requirements include 220 sub-requirements
- It places lots of burden on businesses.
Nicho, Matthew  
Effectiveness of the PCI DSS 2.0 on Preventing Security Breaches: A Holistic perspective  
Real World Security Practitioner (RWSP)  
n.a.  
2011  
1-10  
May 29, 2011  

Cost Vs Benefit
- Risk of fraud and theft if not compliant with PCI DSS
- Compliant with PCI DSS means substantial cost
- In 2009, an aggregate of $1 billion were spent on complying with PCI DSS by merchants. However, 79% of the implementation was cited for failure.
- PCI DSS 2.0 version was released on October 2010.
  - It comprises of 6 principles, 12 major requirements, 45 sub requirements, 75 detailed requirements with corresponding testing procedures for the requirements and sub requirements.
  - Statistics suggest that data breaches have decreased since the release of version 2.0
  - Specifically details of how version 2.0 enhanced data security was also discussed

Gemini Security Solutions  
How Effective is the PCI-DSS?  
Gemini Security Solutions  
n.a.  
2009  
1  
May 28, 2011  
http://securitymusings.com/article/1474/how-effective-is-the-pci-dss

- Does PCI DSS actually make credit card data safer?
  - In 2008, 4.2 million credit card numbers were stolen from the PCI-DSS compliant grocery chain Hannaford Brothers.
- Study has done to determine the effectiveness of PCI
  - The Ponemon Institute released a study, key findings include:
    - Cost of PCI is, on average, 1/3 of the overall security budget
    - 79% have had a data breach
    - 55% of companies focus only on protecting the credit card data and not other sensitive information
    - There is uncertainty as to what personnel are the most accountable for PCI-DSS compliance
    - Smaller companies are less compliant than larger companies (75k+ employees)
  - Conclusion: PCI favors larger companies

- Conclusion: PCI favors larger companies
<table>
<thead>
<tr>
<th>Author</th>
<th>Title of Article</th>
<th>Periodical/ website</th>
<th>Vol. / No. / Edition</th>
<th>Year published</th>
<th>Pages</th>
<th>Date accessed</th>
<th>Location, database, website, link</th>
</tr>
</thead>
</table>

Administrative aspect of PCI compliance is confusing for many merchants, especially businesses that are operating on a smaller scale. Problems have occurred in Canada:

- Lack of specificity in deadlines
- U.S’ deadlines did not apply to Canada
  - Non-unified organization approach
- Difficult for merchants to draft a plan
- Standards are difficult for merchants to interpret