The Payment Card Industry Compliance - Securing both Merchant and Customer data.

White paper – May 2007

This white paper introduces the Payment Card Industry Compliance standard, and the security threats which brought about the need to standardize the data protection of both merchants and customers. The internet is no longer just a source of information, but it is a trading universe where thousands of credit and debit card transactions are carried out every second. Private data is transmitted and stored online through systems which have been exploited numerous times, resulting in immense financial repercussions on both traders and buyers. PCI Compliance is a structured security checklist which aims at securing financial data, and helps to distinguish the secure and reliable businesses from the risky ones. This compliance structure is also used in the Acunetix WVS Reporting Application, and allows security alerts to be presented in a document which abides by the PCI specification.

Table of Contents

1. What is PCI Compliance?

Time and time again, security breaches and system exploits have resulted in the theft of millions of dollars worth of credit card details and personal document information. Over the years, large businesses including banks have suffered security breaches which caused the theft of customer private data. In 2004, the Payment Card Industry Data Security Standard was created in a joint effort by the major credit card companies American Express, Visa, MasterCard and Discover, with each one of the credit card companies having its separate standard detail. On the 30th June of 2005, the PCI DSS regulations were standardized and implemented.

Each credit card company created its own security policy as follows:

American Express:	Data Security Operating Policy (DSOP)
Visa:	Cardholder Information Security Program (CISP)
Discover:	Discover Information Security and Compliance (DISC)
MasterCard:	MasterCard Site Data Protection (SDP)

The PCI Compliance regulation is designed to be implemented by organizations which process transactions made through these credit or debit card types, and severe penalties may be imposed on businesses which suffer a security breech as a result of lack of compliance to the PCI standard. Also, businesses which do not enforce the compliance correctly, or choose not to comply, may be denied the right to process card transactions altogether. Since the compliance regulations are subject to constant development and improvement, participating businesses are required to closely observe the changes in any requirements of the card systems which they process.

In September of 2006, the five major card brands (American Express, Discover, JCB, MasterCard and Visa) joined to create the PCI Security Standards Council, which is an independent body established to monitor and develop the PCI standard. The announcement of the creation of this council also brought forward version 1.1 of the standard. While the council manages the detailing and implementation of the regulatory standard, it is the card companies which dictate their separate requirement specifications, and the way they are implemented according to the size of the organization.

PCI Security Standards Council duties: (http://www.pcicomplianceguide.org)

- Develop and maintain a global, industry-wide, technical data security standard for the protection of account holder account information.
- Reduce costs and lead times for Data Security Standard implementation and compliance by establishing common technical standards and audit procedures for use by all payment brands.
- Provide a list of globally available, qualified security solution providers via its Web site to help the industry achieve compliance.
- Lead training, education and a streamlined process for certifying Qualified Security Assessors (QSAs) and Approved Scanning Vendors (ASVs), providing a single source of approval recognized by all five founding members.
- Provide a transparent forum in which all stakeholders can provide input into the ongoing development, enhancement and dissemination of data security standards.

Each card brand is to administer its own requirements structure and impose its own penalties on businesses which fail to comply.

2. The Compliance Regulations

The PCI compliance specification describes a set of requirements which participating businesses must observe to ensure that correct measures are taken to secure all data, both internal and externally exposed.

Participating financial establishments must ensure the 6 following categories

1. Secure Network Design and Maintenance
- Installation and maintenance of firewall implementation to protect cardholder data
- Default hardware and software credentials and security configuration must be changed

2. Cardholder Data Protection
- Cardholder data must be diligently safeguarded and protected
- Cardholder data transmitted over publicly available networks must be encoded

3. Vulnerability Management Program Maintenance
- An updated anti-virus solution must be in use at all time
- Secure systems and applications must be developed and maintained

4. Strong Access Control Measures Implementation
- Access to cardholder data must be restricted to business need-to-know
- Each person who has computer access must have a unique ID
- Physical access to cardholder data must be restricted

5. Regular Network Testing and Monitoring
- All access to network resources and cardholder data must be tracked and monitored
- Security systems and processes must be tested regularly

6. Information Security Policy Maintenance
- A policy that addresses information security must be implemented and maintained

These 6 guidelines must be diligently carried out in the participating business system implementations and regular testing must be performed to ensure that these standard requirements are all in action at any given moment. The ease with which merchants can achieve PCI compliance depends on the annual transaction quantities processed by the company. For this reason, merchants who require PCI compliance are categorized into 4 separate groups as follows:

Level 1:
- Businesses which process over 6,000,000 annual transactions
- Businesses which have already suffered an attack resulting in compromised data
- Businesses which have already been classified as Level 1 by another card company

Level 2:
- Businesses which process between 150,000 to 6,000,000 annual transactions

Level 3:
- Businesses which process between 20,000 to 150,000 annual transactions

Level 4:
- Businesses which process less than 20,000 annual transactions

3. Protecting the Consumer

Consumers who use credit/debit cards online to purchase products or services risk suffering financial losses when businesses process their transactions through systems which are not secure. There have been an infinite number of cases involving the theft of credit card details from the databases of exploited web applications. Most often, these details get sold on the black market for illicit transactions. I. In these cases, both the organization and the consumer could suffer great losses.

However, another issue which gets less coverage than financial loss is the problem of identity theft. Identity theft is the act of using someone else's personal details like name, address, social security number, or purchase history, without authorization, for fraudulent reasons. It is studied that in the USA alone, over 9 million citizens are victims of identity theft, and experience repetitive abuse of their personal details for several illegal transactions done in their name. These victims usually have no idea about their details being maliciously used until debt collectors show up at their door, or until shocking bills are found in the mail.

A recent case which has shook security professionals around the world was the severe TJX exploit. The owner of clothing retailers T.J. Maxx, Marshall's Inc. suffered the largest known data theft to date. Hackers invaded the TJX systems resulting in at least 45.7 million credit and debit card numbers stolen over an 18-month period. As well as the stolen personal data, including drivers' license numbers of another 455,000 customers who returned merchandise without receipts. TJX first learned that there was suspicious software on its computer system on Dec. 18, 2006, however the stolen data covered transactions dating as far back as December 2002.

The PCI compliance standard aims to stop the cause of online financial and identity theft from its source by ensuring the systems which process and store customer details and transaction information are secure. Web attacks and technological flaws in network security will always keep businesses and security experts on their toes, and once vulnerabilities are secured new ones are being discovered. That is why the PCI compliance standard is an ongoing process which must be maintained at all stages of the online business operation - from designing a system to implementing and running it in the real world.

4. Compliance Certification

The PCI compliance is implemented in both the technological and administrative side of the business process. A solid guideline must be implemented when it comes to company employees handling customer data and processing transactions. Many exploits are actually performed from the inside, and on several occasions members of staff have been convicted of theft, or actions which led to data being illegally acquired. Businesses must also keep track of any changes made to the technical or business process, to ensure that each change is followed by the relevant security counter-measure designed to be successful in a security audit. Data protection and preservation must also be enforced upon elements which do not involve consequences brought about by human involvement. Technical failures must be considered, and timely backups of all precious data must be performed. These backups must be encrypted and stored in specific areas which can only be accessed by authorized administrators or management.

All businesses which apply the PCI compliance procedure must use the services of approved companies to perform compliance security scans. The results of these scans are issued in detailed compliance reports which are then used for approval by the specific card company requirements. The PCI Security Standards Council manages the process for security companies to become Approved Scanning Vendors (ASVs), and PCI compliance reports may only be issued by these approved entities.

5. Security Assessment Tools

The PCI Compliance specification is more than just a rule-set to which organizations must abide. It is also a guideline which provides a method to trace and secure all the potential security flaws which might be exploited. Detecting these potential exploits is made easier by using tools such as web vulnerability scanners and network scanners.

A web vulnerability scanner is a software product which performs an in-depth assessment of a web application or web service. It detects all the security flaws which may be exploited by a hacker whose intention is to gain access to web servers, internal networks, and back-end databases. The web application is often overlooked when organizations allocate funds to purchasing high-spec intrusion detection systems, and network security systems. However a common mistake is to forget that if a website is made publicly available then it also provides an entry point which is open 24 hours a day. Web vulnerability scanners assist developers in identifying these possible entry points and securing the web application to prevent this from happening.

Network scanners on the other hand are tools which scan network hosts for open ports, missing security patches on operating systems and server technologies, potential exploits discovered in applications installed on a network, network device weaknesses, and incorrectly configured user rights. These security risks are resolved by various configurations and application of security software patches and updates. Any changes in a network infrastructure may open potential security breaches, therefore regular scans must be on any system administrator's maintenance schedule.

6. Summary and Conclusions

The objective for a business which operates online is to be able to provide the customer with the purchased goods or services in a reduced time-frame, and with greater efficiency. The internet is slowly but surely turning the idea of physical money into an abstract concept, which in theory sounds extremely practical, however the digitalization of funds and payment systems also exposes greater threats. Many people see it as a way of eliminating the need to guard their physical cash, however it is this same digitalization which puts a greater risk on people's money and identity.

Information about the risks associated with exchanging and transferring funds online can be researched and found in various publications and websites, however this information is not designed to intimidate but it is intended to create awareness among consumers and businesses. PCI compliant merchants can benefit from a standardized approach to secure their online systems, and also to prove their reliability to the consumer public.

The Approved Scanning Vendors who provide PCI Compliance audits can benefit from Acunetix Web Vulnerability Scanner to identify vulnerabilities in merchant web applications, and also guide them to resolving any potential exploits. Full PCI Compliance extends the capabilities of Acunetix WVS to certification of secured web applications according to the specifications detailed by the Payment Card Industry security guideline.

Jacques Guillaumier, May 2007

About Acunetix

Acunetix was founded to combat the alarming rise in web attacks. Its flagship product, Acunetix Web Vulnerability Scanner, is the result of several years of development by a team of highly experienced security developers. Acunetix is a privately held company with headquarters based in Europe (Malta) with an office in London, UK. For more information about Acunetix, visit: http://www.acunetix.com; http://www.acunetix.de.