



PCI COMPLIANCE COST ANALYSIS

A Justified Expense

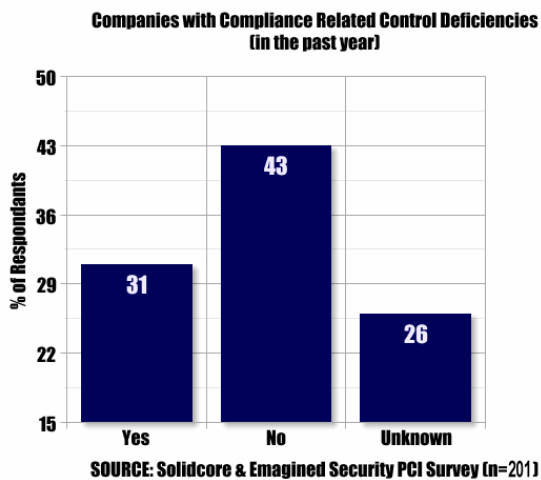
A joint analysis conducted by Solidcore Systems, Emagined Security and Fortrex

solidcore[®]


EMAGINED SECURITY

FORTREX[®]
TECHNOLOGIES
WORLD CLASS INFORMATION SECURITY

The Payment Card Industry Data Security Standard (PCI-DSS) was created by the credit card companies and is intended to protect cardholder data wherever it resides, ensuring that merchants and service providers maintain the highest degree of information security for their customers. While the standard is meant to have a positive impact on merchants, consumers and the retail industry, many retailers are still questioning its effectiveness and necessity in light of the high-cost to comply. A recent poll of 201 information technology (IT) and PCI compliance professionals reinforces this point. The study found that 57% of respondents either experienced a compliance control deficiency in the past year or did not know if they had a PCI compliance deficiency in the IT environment.



Despite the costs of compliance, recent research conducted by Solidcore Systems, Emagined Security, and Fortrex reaffirms the importance of complying with the PCI-DSS. The research finds that the cost of compliance is only a small fraction of the potential cost of non-compliance for Level 1 and Level 2 merchants.

Merchants and service providers must begin to look at the PCI compliance requirements as an opportunity to improve IT operations and gain broader IT benefits from an investment around PCI compliance. This means looking beyond meeting the requirements for PCI and evaluating technologies that can help ensure continuous PCI-DSS compliance as part of an IT organization's operations framework.

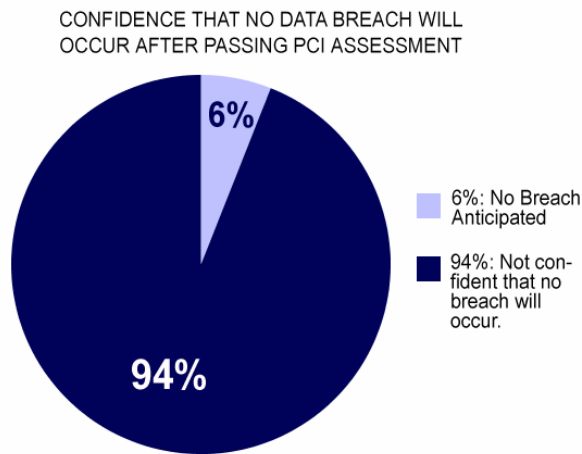
The credit card companies divide merchants into various levels based on the number of transactions processed every year. For example, Visa categorizes Level 1 merchants as those processing more than six million transactions.

LEVEL	# TRANSACTIONS
Level 1	> 6 million
Level 2	1 – 6 million

While each level is subject to a different set of compliance activities, the strictest rules and highest costs apply to Level 1 merchants. In 2006, Visa redefined how transaction counts are derived to include ALL credit card transactions, not just ecommerce. This change forced many merchants up a tier or two when they factored in their traditional brick-and-mortar sales. In addition to transaction volume, any merchant that has suffered a hack or an attack resulting in account data being compromised is automatically required to meet Level 1 compliance requirements. Further, the acquirer (usually a bank who services the merchant's credit card receipts) may, at their discretion, require any merchant in its network to meet Level 1 requirements. As a best-practice, many Level 2 merchants are advised to follow the Level 1 requirements, regardless of activity level.

Achieving PCI compliance, avoiding fines and retaining the privilege to accept credit cards requires merchants and service providers to address approximately 180 individual PCI requirements in 12 categories. The IT organization of a Level 1 or Level 2 merchant running hard toward PCI compliance can easily feel overwhelmed by the cost of upgrading the infrastructure and paying for ongoing infrastructure maintenance, as well as the assessment(s) needed to verify compliance. And because participating merchants must pay for their own PCI compliance assessments, the incremental cost of compliance depends upon the extent to which the infrastructure is already in a compliant or near-compliant state. Multiple assessments may also be needed to assure compliance, which is why it is essential for merchants to work with an experienced qualified security assessor (QSA) that has been approved by the PCI security standards council.

Another recent poll conducted by Solidcore Systems and Emagined Security surveyed a group of 173 IT professionals responsible for PCI compliance, and found that only 6% were completely confident they would not experience a data breach following a successful PCI compliance assessment. This reinforces the importance of working with an experienced QSA that can help the IT organization properly understand and set expectations around PCI compliance.



SOURCE: Solidcore & Emagined PCI Survey (n=173)

The Three Cost Categories of PCI-DSS

For the purposes of conducting this analysis, Solidcore, Emagined and Fortrex divided the costs tied to PCI-DSS compliance into three categories: Upgrading systems, assessments, and sustaining compliance.

Cost 1: Upgrading Infrastructure – Merchants and service providers must ensure that computer systems processing payment and cardholder information are upgraded in accordance with the PCI-DSS requirements. For many Level 1 and Level 2 merchants, much of the security infrastructure may already be in place. However, some may find the need to purchase and install new infrastructure components including and not limited to additional firewalls, upgraded anti-virus, anti-spyware and full-spectrum messaging security software, secure wireless systems, data encryption technologies, and file-integrity monitoring software. The costs involved for upgrading the

infrastructure not only include product costs, but also include the costs required for IT personnel to install and maintain the systems. For more information about the specific requirements, visit the PCI Security Standards Council Web site: <https://www.pcisecuritystandards.org>.

Cost 2: Verifying Compliance (Assessments) – While the PCI-DSS mandates that all merchants follow the 12 requirements, there is also an implicit 13th requirement to verify compliance with the PCI-DSS. This is often an overlooked yet integral part of any PCI compliance program. Level 1 Merchants must pay for their own PCI compliance assessment performed by an approved QSA or qualified security assessor. A Level 1 merchant or service provider must submit an annual “Report on Compliance,” which is validated by the approved QSA, and multiple assessments can be required during the year to ensure compliance is being maintained. The scope of the assessment and verification is focused on systems or system components related to the authorization and settlement where cardholder data is processed, stored, or transmitted.

Cost 3: Sustaining Compliance – It is insufficient for merchants and service providers to merely “meet” the PCI-DSS requirements. Merchants and service providers must sustain continuous compliance as part of the overall IT operations strategy and framework. Key to this is assuring that once systems are compliant, and policies and process are established, the IT organization must ensure systems remain in that compliant state. This includes monitoring changes in PCI requirements, such as the recently added requirement – mandatory June 30, 2008 – for implementing an application layer firewall. Future versions of the PCI-DSS requirements, which will evolve and become stronger over time, will require the regular attention of all merchants and their IT departments. If done manually, sustaining continuous PCI compliance can prove to be an arduous and costly endeavor. However, “change control” technology is paving the way for automating the ability to sustain continuous compliance by automatically producing compliance reports and locking-down the merchant infrastructure once placed in a compliant state.

Cost Analysis of PCI-DSS

The following cost analysis is based on a Level 1 merchant with 2,000 – 2,500 retail locations. This cost analysis is designed to simulate that the cost of complying with the PCI data security standard is only a fraction of the cost of not complying with the standard. These costs assume that a basic information security program is already in place before the need to add PCI upgrades is factored in.

Cost Category	Incremental Compliance Costs	Cost of Non-Compliance
<p>Cost 1: Upgrading Payment Systems and Security Infrastructure These costs include investments in technology and personnel that is required to meet the 12 PCI compliance categories. This includes and is not limited to installing and maintaining firewalls, security policies, anti-virus, WPA-based wireless security, and file-integrity monitoring software. The costs for upgrading the infrastructure can depend on how compliant an organization's existing infrastructure is.</p> <p>Note: The data for costs in this category was calculated by surveying IT and PCI compliance professionals at Level 1 and 2 merchants, analyzing public information about the costs incurred by a merchant with 210 stores, and analyzing cost data publicly disclosed by the TJX companies.</p>	<p>\$2 - \$10 million</p> <p>Upfront costs over one to two years</p>	<p>By not following the best-practices outlined by the PCI Security Standards Council, merchants run a high risk of incurring costs of a data breach. These costs include and are not limited to, the costs of a "crisis" project to upgrade payment systems and infrastructure to a higher compliance level, done as a condition of continuing to accept credit cards. This can include repeat assessments and internal audits to verify compliance, extensive notification costs and credit monitoring subscriptions for cardholders affected, and legal expenses to defend against shareholder and consumer lawsuits tied to a data breach. These costs could be dwarfed by the publicity driven decline in customer willingness to shop for fear of further security issues.</p> <p>Note: The data for costs of non-compliance collected from TJX public filings in accordance with the company's computer security breach, merchants surveyed by Solidcore Systems, Emagined Security and Fortrex; and independent research that cites the cost-per-record following a data breach can be as high as \$200.</p>
<p>Cost 2: Verifying Compliance (Assessments) These costs are for single or multiple security assessments conducted by a Qualified Security Assessor (QSA) that has been approved by the PCI Security Standards Council. Sometimes known as the implicit "13th category" of PCI compliance, costs in this area can vary based on size of the IT infrastructure and need to re-assess a merchant's security posture.</p> <p>Note: The data for costs in this category collected by surveying IT and PCI compliance professionals, and includes data provided by Fortrex, an approved QSA.</p>	<p>\$250k - \$3 million Annually</p> <p>(This is highly dependent on the previous compliance level and ongoing "auditability" of PCI required controls)</p>	<p>Note: The data for costs of non-compliance collected from TJX public filings in accordance with the company's computer security breach, merchants surveyed by Solidcore Systems, Emagined Security and Fortrex; and independent research that cites the cost-per-record following a data breach can be as high as \$200.</p>
<p>Cost 3: Sustaining Compliance These costs are for maintaining the compliant state of the IT infrastructure after initial compliance has been achieved. This includes auditing and maintaining physical and IT infrastructure security. Cost in this category can vary depending on the use of manual methods, automated technologies and the pace of change in the underlying infrastructure supporting your PCI related systems.</p> <p>Note: The data for costs in this category collected from IT and PCI compliance professionals, and customer data collected by Solidcore Systems.</p>	<p>\$1 - \$5 million Annually</p> <p>(Note that most of these costs will over time become indistinguishable from those currently budgeted for your ongoing information security program)</p>	<p>Note: The data for costs of non-compliance collected from TJX public filings in accordance with the company's computer security breach, merchants surveyed by Solidcore Systems, Emagined Security and Fortrex; and independent research that cites the cost-per-record following a data breach can be as high as \$200.</p>
Total:	\$3.5 - \$18 million	\$100 - \$250 million
The cost of a breach can easily be 20 times the cost of PCI Compliance		

Merchants should not view the need to address PCI compliance as a costly inconvenience, but rather an opportunity to improve and verify the secure state of the IT infrastructure. Viewed another way, the card issuing companies are giving merchants an opportunity to continue to do business. The cost of compliance is only a fraction of what a company might pay for not complying with the PCI data security standard, and certainly is overshadowed by the potential cost of a breach. By leveraging good security planning and architecture, experienced security consultants, approved QSAs, and proven technology vendors, the overall incremental costs of PCI compliance can be minimized.



About Emagined Security

Emagined Security is the leading professional services provider for Information Security & Compliance solutions. Emagined Security empowers its clients to help them effectively manage IT risk in today's dynamic business environment. With deep industry and domain expertise, a proven track record, and by employing well known and respected individuals from the Information Security community, Emagined Security can scale quickly and efficiently to provide clients with the rapid response required by best-in-class organizations. Emagined Security's commercial clients cover a wide range of U.S. and global Fortune 500 organizations, including the financial services, energy, healthcare, high tech, manufacturing, & insurance industries. Anticipate, protect, react, and deliver. Emagined Security is your partner in information security & compliance. For more information, visit www.emagined.com.

About Fortrex

Founded in 1997 Fortrex Technologies, Inc. has been a market leader in providing IT Security, Operational Risk and Compliance solutions for over 500 customers in various industry sectors. The Fortrex mission is to be our clients' long-term, trusted security advisor by ensuring the confidentiality, integrity, and availability of their data and systems through the provision of world-class, enterprise-wide information security services and solutions. At Fortrex, we believe that our unique differentiator is the team of individuals who are committed to a set of corporate values. These values, Integrity, Excellence, Empowerment, Teamwork and Thankfulness, are the foundation of all Fortrex relationships, including those with our employees, customers and vendors. For more information, visit www.fortrex.com.

About Solidcore Systems

Solidcore is a leading provider of real-time change and configuration control software. Organizations worldwide trust Solidcore to assure compliance with the Payment Card Industry (PCI) and Sarbanes-Oxley (SOX) standards, to improve service availability, and achieve faster returns on ITIL and IT service management initiatives. Solidcore's S3 Control software helps organizations by tracking changes to their critical infrastructure in real-time, determining if the changes are authorized and blocking unauthorized change. Solidcore is headquartered in Cupertino, California. For more information, visit www.solidcore.com.