



TAKE CONTROL.

PCI Compliance:
Are UK Businesses Ready?

WHITE PAPER ○



Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS), one of the most prescriptive data protection standards ever developed, addresses the ever-increasing threats to customer cardholder data by requiring security controls for the cardholder data environment. As a pass/fail regulation, organizations must pass each and every one of the 214 requirements to be certified as PCI compliant. In 2010, almost three years after the United States market mandated that organizations comply with the (PCI DSS), the United Kingdom now faces its compliance deadline.

Following an initial, significant reluctance to MasterCard, Visa and American Express dictating compliance, the US market has recently experienced a rapid change of heart. The combination of high penalties and the threat of being unable to accept payments via each of these card brands certainly focused attention on PCI. But more importantly, those storing cardholder data have been rocked by the huge brand damage, loss of customers and financial costs incurred by organizations that have endured high profile data breaches.

But is this attitude reflected in the UK market today? According to research commissioned by Tripwire, only 11 percent of UK organizations processing credit and debit cardholder data are currently certified PCI compliant. Level 1 merchants—those processing over six million transactions annually—embraced the regulation first, with over half (58 percent) audited and certified compliant. For those merchants processing under six million transactions, the percentage of certified organizations falls to a surprising low of 4 percent to 8 percent.

The study revealed a particularly interesting finding: that senior management in organizations studied have a resounding commitment to PCI compliance. In fact, organizations easily raise funds for compliance projects. This second finding is extraordinary given recent restrictions in IT spending. Furthermore, senior management is represented on the PCI compliance team in the majority of organizations.

This top-level commitment reflects a key conclusion of the research: brand awareness and fear of reputation damage significantly drive PCI compliance activities in most organizations. It makes sense then, that organizations prefer to

KEY FINDINGS

- Only 12% of United Kingdom (UK) organizations processing credit and debit cardholder data are currently certified as being PCI compliant.
- While 58% of Level 1 merchants have been audited and certified as compliant, that falls to 6%, 8% and 4% for Level 2, 3 and 4 organizations.
- Over half (57%) of retail organizations admit to not fully understanding the requirements of the Payment Card Industry Data Security Standard (PCI DSS).
- Brand awareness and fear of reputation damage is a significant driver for achieving PCI compliance.
- Over three quarters (77%) of organizations have had no difficulty in securing funding and resource to ensure PCI DSS requirements are met.
- 88% of organizations have senior management on the PCI DSS team or working group—a figure that is 100% for Level 1 organizations.

invest time and resources in achieving compliance rather than pay penalties for non-compliance or endure a data breach that damages their reputation.

However, the study revealed a disturbing trend; many Level 3 and Level 4 merchants, (those most likely to be early in their PCI compliance efforts) perceive that their existing security procedures exceed the level of security required by PCI. In contrast, none of the Level 1 and 2 merchants surveyed—those more likely to be further along the compliance route—hold this opinion. Rather, these more experienced merchants feel the PCI DSS requirements are actually only on par now with their current security procedures.

This raises a worrying concern that organizations not yet certified may have a tendency to underplay the PCI requirements and risk complacency. Unfortunately, as the PCI compliance deadline approaches in which these organizations must experience a full PCI audit, they may realize too late that they face a steep climb to achieving PCI compliance and ensuring cardholder data protection.

Introduction

Effective September 30, 2010, the Payment Card Industry Data Security Standard (PCI DSS) will apply to organizations in the UK; specifically, Level 1 merchants must be validated as PCI DSS compliant. Recent research undertaken in the UK by Redshift Research of behalf of Tripwire reveals that with just months to go before the compliance validation deadline, only 12 percent of UK organizations that handle credit card data currently have been audited and certified PCI compliant.

Brand Value

These organizations also understand the direct relationship between attaining PCI compliance and safeguarding brand value. The impact on brand value of the highly publicized data breaches that have occurred in the US undoubtedly raised PCI awareness amongst senior management across every division of the surveyed organizations.

For example, they're well aware of the brand damage

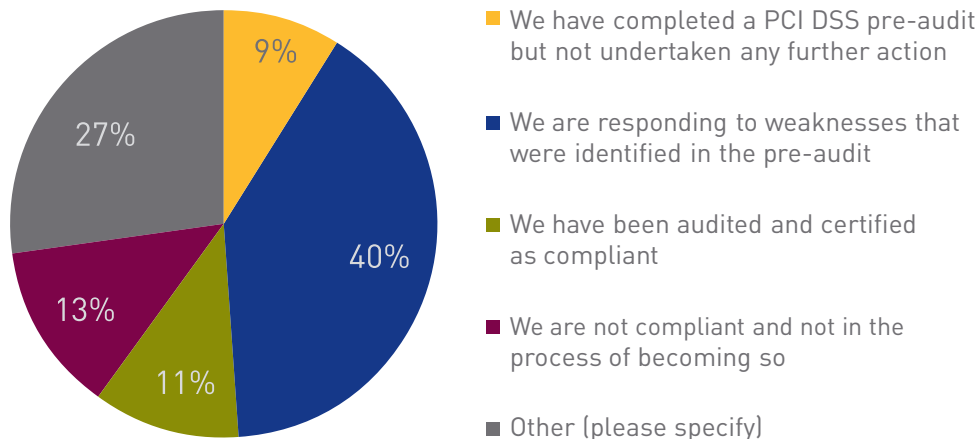
inflicted on organizations such as RBS Worldpay, which believes a breach of its payment system may have affected more than 1.5 million people; Hannaford Brothers, which disclosed that a breach of its payment systems, aided by malicious software, compromised at least 4.2 million credit and debit card accounts; and of course, TJX Companies Inc, the parent of retailers Marshalls and TJ Maxx, which confirmed that more than 45 million credit and

debit card numbers were exposed over a three year period.

As a result of this knowledge, many UK organizations view PCI as a positive move and a clear opportunity to demonstrate to customers a strong commitment to data protection. Over one third (40 percent) of respondents believe that PCI compliance will enhance brand reputation by giving consumers greater confidence.

The survey also revealed that merchants recognise that proactively and wisely investing in IT security is far preferable to incurring unexpected costs for repeat audits, fines, law suits and brand damage. When it comes to making this simple and smart business decision, 89 percent of organizations prefer to take the time and invest in becoming PCI compliant rather than receive a penalty. [Q11]

Q6 Current status of PCI DSS compliance in the organization



The research, conducted during December 2009 and January 2010, based its findings on interviews with organizations across the finance, leisure and retail sectors and across a wide range of company sizes. This broad sample of organizations ensured the research captured the wide variety of different attitudes and experiences associated with organizations subject to PCI compliance.

The survey showed that without question, organizations take PCI compliance seriously, with only 8 percent of respondents ignoring the compliance requirement (although this rises to 10 percent for retail organizations). [Q10] The findings also indicated that organizations buy into the reasoning behind the standards: the majority (62 percent) agree that PCI improves the security of cardholder information, and well over a third (44 percent) also believe PCI compliance improves the company's overall security. [Q11]

Uncertain Future

Yet despite this clear commitment to the PCI standard, 25 percent of organizations surveyed either will not be compliant or are unsure if they will be compliant by the 2010 deadlines. And these organizations appear far from confident about their understanding of the requirements of PCI; 36 percent are not confident, with an astonishing 57 percent of retailers lacking confidence in their understanding. [Q1]

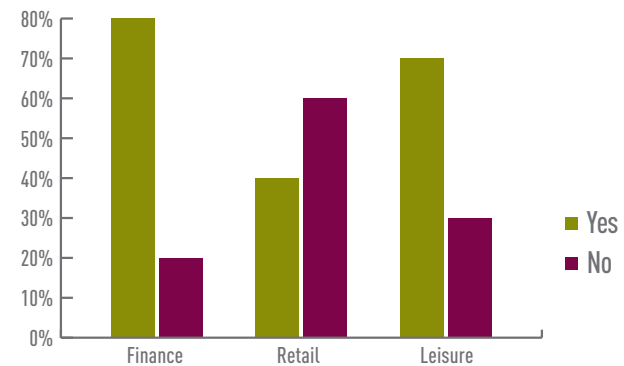
But there is also a clear divergence in expectations and understanding of the PCI requirements between the Level 1 and 2 merchants compared to Level 3 and 4 merchants. One hundred percent of Level 1 organizations believe they fully understand the requirements of PCI compliance, as do 86 percent of Level 2 organizations. In comparison, only 64 percent of Level 3 and 44 percent of Level 4 organizations believe they fully understand the requirements. [Q1]

This lack of understanding of the PCI requirements raises a real concern that these organizations will fail to address each aspect of the PCI standard, thereby increasing the danger of data compromise. Other implications may include organizations not implementing the requirements until or unless required; implementing them incorrectly; and not ensuring the requirements are adhered to continuously. Failure in each or all of these areas will result in a heightened risk of data compromise, potentially leading to loss of customer data, fines from the card brands for non-compliance with PCI, customer law suits, and of course, brand damage.

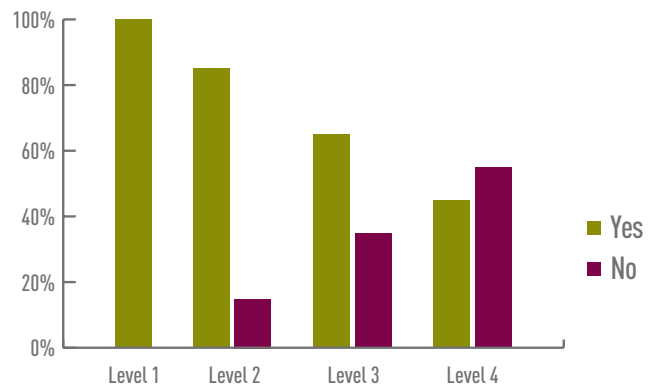
So why are these organizations not better educated about the demands of PCI? According to the survey, only 45 percent had received a letter from their acquiring bank regarding PCI compliance. [Q4] Although 79 percent of Level 1 and 75 percent of Level 2 merchants had received letters, only 36 percent of Level 3 and 14 percent of Level 4 merchants had been contacted. The study also revealed an interesting industry-specific difference: that 73 percent of leisure companies had received a letter, while only 23 percent of retail companies had.

This lack of communication raises a number of issues: first of all, a process by which merchants are educated about the PCI standard is apparently lacking. But it is not just the merchants that need to understand PCI compliance and take it seriously; the acquiring banks, auditors, and all other organizations in the PCI loop need to get on board with the

Q1 Do you feel you fully understand the requirements of the PCI DSS?



Q1 Do you feel you fully understand the requirements of the PCI DSS?



demands and implications of PCI compliance. Involvement of each of these groups in developing these educational strategies ensures the strategies will address all four merchant levels of organizations processing cardholder data.

The other issue relates to internal communication. Specifically, are acquiring banks sharing information about PCI compliance in a timely manner with the team responsible for PCI compliance—primarily IT security personnel at merchant organizations? In the US, only after highly publicized security breaches occurred did organizations begin to focus attention on PCI and significantly change their opinions and attitudes on the value of adhering to the PCI requirements. Will the UK market shift its mindset and begin internal and external PCI communication and collaboration only after further exploitation of cardholder data?

Right Approach

Attitude is key to both achieving and sustaining PCI compliance. Despite appearing to take PCI compliance seriously, over a quarter of respondents (27 percent) feel PCI DSS is unnecessary, and 27 percent will put off becoming compliant for as long as possible. [Q11]

Q11 Attitudes of Merchants towards PCI DSS

- 27%** of respondents feel that PCI DSS is unnecessary
- 27%** plan to put off compliance for as long as possible
- 30%** don't believe that PCI DSS will improve IT Security
- 29%** think security should be the problem of credit card companies
- 19%** don't believe that PCI is necessary to improve the security of cardholder information

This latter finding demonstrates perhaps the clear conflict between internal security personnel and senior management. Internal security owns the difficult process of implementing the technologies and processes to achieve and maintain compliance. In contrast, senior management prioritizes compliance over other activities to minimise exposure to events that could affect brand or reputation, regardless of the work involved. Most likely, the 27 percent of respondents who will put off becoming compliant or feel compliance is unnecessary are IT security personnel, not senior management.

So how are these organizations weighing the cost of achieving PCI compliance against the value compliance delivers? As highlighted above, 46 percent of respondents perceive PCI compliance to aid brand reputation. For 50 percent of the respondents, this perception appears to justify investment in the existing security infrastructure to support compliance, improve attention to information and security, and help protect data privacy. [Q12]

As a result of this perceived value, organizations across every level appear strongly committed to achieving PCI compliance. Money has been made available when required, with 77 percent of organizations finding no difficulty in securing funding and resources to ensure they meet PCI DSS requirements. [Q20] Furthermore, 88 percent of organizations have senior management on the PCI DSS team or working group—a figure that reaches 100 percent for Level 1 organizations. [Q19]

Q12 The Wider Benefits of PCI Compliance

- 44%** believe that PCI compliance will aid Brand reputation
- 46%** think that PCI compliance helps to justify investment in existing security infrastructure
- 50%** believe PCI compliance improves attention to information, security and protect data privacy

PCI LEVELS

The acquiring banks must ensure that all merchants and service providers are compliant with the PCI DSS requirements. However, compliance validation has been prioritized based on the volume of transactions, the potential risk and exposure introduced into the payment system. Merchant levels are defined based on the volume of annual transactions.

- **Level 1** Processing over 6 million transactions annually
- **Level 2** Processing 1 to 6 million transactions annually
- **Level 3** Processing 20,000 to 1 million e-commerce transactions annually
- **Level 4** Processing less than 20,000 eCommerce transactions annually and other merchants processing up to 1 million transactions annually.

In addition to the annual audit by a Qualified Security Assessor or Self Assessment Questionnaire, organizations must also have a quarterly network scan by an Approved Scan Vendor and an attestation of Compliance Form.

Source: Visa

Achieving Compliance

So how far along the route to compliance are UK businesses? Of the 12 percent that have been audited and found compliant, the vast majority are Level 1 organizations. Over half (58 percent) of Level 1 merchants are compliant, compared with just 4 percent of Level 2, 8 percent of Level 3, and 6 percent of Level 4 merchants.

For the vast majority of these businesses

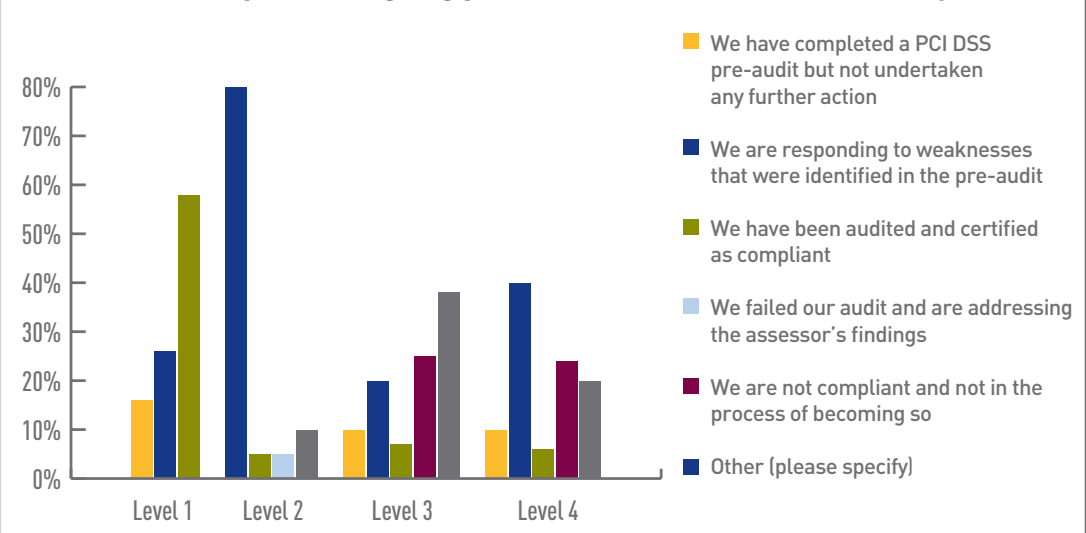
PCI compliance remains a work in progress. Slightly less than half (40 percent) are responding to weaknesses identified in the PCI DSS pre-audit, while 9 percent have completed a PCI DSS pre-audit but have yet to take further action. Just 1 percent of organizations that failed an audit are addressing the assessor's findings. However, 24 percent of both Level 3 and Level 4 merchants are not compliant and are not in the process of becoming so. [Q6]

The survey also revealed that for the vast majority of organizations (68 percent), achieving PCI compliance requires, or will require, corrective action. This rises to 84 percent for Level 1 companies—a key finding considering how many more of these organizations are now certified as compliant. A worrying 32 percent of Level 4 organizations do not know if corrective actions are or will be necessary and 20 percent believe no corrective action is required.

At the same time, no Level 1 or 2 merchants believe their security requirements go above and beyond the requirements of PCI; yet 12 percent of Level 3 and 16 percent of Level 4 merchants do have that belief. Given the fact that most Level 1 companies are now compliant, and as large organizations already had significant security procedures in place, this can only mean that Level 3 and 4 merchants are fundamentally underplaying the requirements of PCI.

Because only 8 percent believe they will not be compliant in time, these figures would suggest a degree of

Q17 PCI DSS compliance ongoing process or an annual assessment by Level



complacency, especially amongst Level 3 and 4 organizations. This raises the real risk that many will have trouble passing the audit because these organizations simply do not have the security best practice processes and procedures in place to allow them to pass. As the experiences of the Level 1 merchants show, PCI compliance should not be treated as a rubber stamp, whether the audit is performed by a Qualified Security Assessor (QSA) or as a self-assessment.

While there may be misunderstandings in the requirements for PCI compliance, experience shows that most failures occur because PCI compliance is too often treated as a one-time project rather than a continuous process of security best practices. This message certainly seems to have hit home with UK organizations, with 89 percent now regarding compliance as a continuous process. However this figure falls to 72 percent in retail companies. And surprisingly, 5 percent of Level 1 and 7 percent of Level 2 merchants still view compliance as an annual assessment. [Q17]

Getting a tick mark from a PCI assessor differs tremendously from being PCI compliant. As the CEO of Heartland Payment Systems admitted, the company received the Report of Compliance one day and was breached the next—a breach that may have compromised tens of millions of credit and debit card transactions. The company, which processes payments for more than 250,000 businesses across the US, representing some 100 million transactions a month,

fell foul to a piece of malicious software planted on the company's payment processing network.

This example illustrates a key principle about the PCI standard: the spirit of the standard means that organizations must protect cardholder data not just for the day the auditor is in town, but every day.

Imposing Controls

So what controls are in place to ensure that organizations do not run the risk of a post-certification breach and all the negative publicity that goes with it? The standard demands that an organization deploys file integrity monitoring software and alerts on unauthorized modifications of critical system content and configuration files (Specification 11.5). As a result, organizations have invested in monitoring and management tools that identify change.

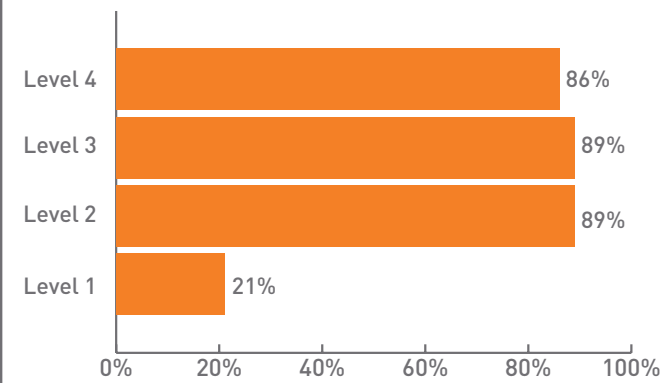
The survey revealed that 86 percent of Level 3 and 71 percent of Level 4 merchants are completely or reasonably satisfied with the organization's ability to alert personnel to unauthorized modification of critical files and maintain file integrity on systems within the scope of PCI. For Level 1 merchants, this figure drops to 16 percent.

The key problem the experience of US merchants highlights is that although organizations have invested heavily in monitoring and management tools to highlight changes, these tools identify all changes—not just the small fraction that represent a potential breach or security exposure. The result if this ability to capture all change is a huge amount of noise, and no way to identify the critical changes of interest.

The result? Auditors cannot enforce the standard requirement to uncover unauthorized modification of files. But in addition, the average time between a security breach occurring and it actually being discovered—the breach-to-detection gap—is between 4 and 24 months. This gap leaves organizations and their customers exposed to huge risks. (Verizon 2009 Data Breach Investigations Report)

Without the facility to rapidly identify suspicious changes, organizations will struggle to remain continuously compliant. By implementing an automated solution that continuously and immediately identifies these changes as well as other security events, organizations gain confidence that they can immediately take action to avert a breach or address a security situation before real damage occurs.

Q14 Proportion of Merchants who are satisfied with their organization's ability to alert personnel to unauthorized modification of critical files and maintain file integrity on systems within the scope of PCI



Escalating Challenge

So are organizations in the UK taking PCI compliance lightly? Certainly in the US, organizations were complacent about the first audit. But that thinking changed rapidly when US merchants experienced a second audit. At that point, requirements had become stricter, but more importantly, the implication of failing to meet compliance had begun to hit home as these organizations heard repeatedly about the brand and reputation damage suffered by organizations that had experienced a breach.

However, even if an organization passes one audit that does not mean it will pass the next. Audits get tougher year on year, reinforcing the need for continuous activity at every level. Preparing for these tougher audits requires the right staff supported by the appropriate level of resource. Unfortunately, few of the organizations surveyed had dedicated PCI project managers (27 percent), leaving responsibility for the task largely to IT security/senior management and IT operations.

In addition, because PCI amounts to basic security best practices, if an IT organization lacks staff who understand security issues and know how to implement security technologies and follow security processes, the organization has larger problems than just PCI compliance. [Q19] For these organizations this lack of security expertise represents a fundamental business issue they must address.

Conclusion: Protecting the Brand

At a time when IT budgets are under tight scrutiny, senior managers are more willing than ever to release funds for PCI compliance. Because of the experiences of US organizations in the US related to PCI and data security, these organizations now understand that good data security and PCI compliance are key to protecting the organization's reputation. Compliance deters would-be attackers and presents an opportunity for organizations to reinforce public and customer confidence in their brand. Simply enough, in this market no organization can risk the massively damaging effects of a publicized breach of cardholder data.

But given the budgets and resources available, are these organizations prepared for the pending deadline? The fact that only 58 percent of Level 1 merchants have been audited and found compliant, with the remainder of merchants at Levels 1, 2, and 3 only in single digits should raise concern. As the deadline approaches the only option for many is to take the unfortunate "checklist approach" to PCI compliance, rather than relying on ongoing good security practices to protect cardholder data.

Adding to these concerns, smaller organizations have clearly underestimated the serious implications of PCI. While most organizations hear loud and clear that continuous compliance activity is essential, the majority of these organizations are not implementing the processes or tools required to achieve that objective.

Combining the experience of the US market with that of those Level 1 merchants that have achieved PCI compliance in the UK provides some valuable lessons; organizations must have the right attitude underpinned by appropriate technology and processes to achieve a more secure organization and protect cardholder data. With greater security and data protection, these organizations ensure they protect their brand and reputation.

For UK merchants—as well as all merchants subject to PCI—the objective should not be to just pass a PCI audit. Achieving continuous PCI compliance should be viewed as just one way of demonstrating that good security practices are in place. If compliance itself is the driving factor, organizations will struggle to achieve the goal. Instead, if organizations focus on putting in place security best practices, they often achieve continuous PCI compliance as a natural by-product and benefit.

ABOUT TRIPWIRE

Tripwire is the leading global provider of IT security and compliance automation solutions that help businesses and government agencies take control of their entire IT infrastructure. Over 7,000 customers in more than 86 countries rely on Tripwire's integrated solutions. Tripwire VIA™, the comprehensive suite of industry-leading file integrity, policy compliance and log and event management solutions, is the way organizations proactively prove continuous compliance, mitigate risk, and achieve operational control through Visibility, Intelligence and Automation. Learn more at tripwire.com.

