Research by

Ponemon INSTITUTE

Commissioned by

THALES

PCI DSS Trends 2010: QSA Insights Report

Recommendations and guidance for achieving compliance from Qualified Security Assessors

March 2010

Executive Summary

The Payment Card Industry Data Security Standard (PCI DSS) is now part of everyday business for organizations that accept and process card payments. Since 2006, businesses have had to comply with PCI DSS requirements established by the PCI Security Standards Council (PCI SSC) and backed by all the major card brands. Certified auditors known as Qualified Security Assessors (QSAs) are critical to the success of the program and to the prevention of credit card theft and data breaches. Commissioned by Thales, Ponemon Institute surveyed 155 QSAs worldwide to develop an accurate picture of PCI compliance today.

Key findings of the survey include:

- **Few organizations fail compliance, but many are relying on mechanisms not prescribed by the PCI DSS.** Only 2 percent of merchants assessed by QSAs fail, but 41 percent are relying on compensating controls. While these controls are allowed in order to achieve compliance when an organization can't live up to the PCI DSS, they may be only temporary fixes and might be eliminated by future changes to the PCI DSS.
- **Cost of annual audits averages $225,000 for the largest merchants.** Excluding technology, operating, and staff costs, the world's largest acceptors of credit cards (also known as Tier 1 merchants) are spending an average of $225,000 on auditor expenses. 10 percent of these businesses are spending $500,000 or more annually on PCI auditors.
- **Restricting access to card data is the most important PCI DSS requirement, but also the most difficult to achieve.** QSAs believe controlling access to credit card data on a need-to-know basis (PCI DSS Requirement #7) is the most difficult requirement for merchants to achieve compliance with, as well as the most important.
- **Encryption is the favored technology for achieving end-to-end cardholder data protection**. 60 percent of QSAs believe encryption is the best means to protect card data end-to-end, compared to 35 percent for tokenization. 81 percent of QSAs require or recommend hardware security modules (HSMs) to manage data protection, while 63 percent say HSMs also reduce the time spent on demonstrating compliance.

These findings and others represent the first part of research into auditors' recommendations for achieving compliance, improving the PCI DSS program, and preparing for expected changes. The remaining findings will be published in a subsequent companion report.

Contents

Introduction

Since its introduction in 2006, the Payment Card Industry Data Security Standard (PCI DSS) has challenged businesses that accept and process credit cards.[1] Instead of introducing new technology standards, the PCI DSS brought a consistent set of baseline security requirements to the business of accepting and processing credit cards. The standard pushed responsibility for protecting the privacy of customer data onto the organizations accepting and processing transactions and away from the major card brands and banks.

Much of the responsibility for the program's success is in the hands of Qualified Security Assessors (QSAs). These certified auditors are tasked with validating the state of compliance at the largest merchants and service providers. Today, over 2,000 QSAs are working for more than 200 firms worldwide. The role of QSAs in the operation of the largest merchants can't be overestimated. Their evaluations and recommendations impact not just how businesses operate but also how their brands – and potentially their profits – can remain untarnished by credit card fraud and data breaches.

To develop an accurate picture of PCI compliance today, Ponemon Institute, commissioned by Thales, surveyed QSAs worldwide. 155 QSAs participated in the web-based survey. The first part of this research is presented in this report. The remaining findings will be published in a subsequent companion report.

Key Findings

The survey results form a clear picture of how PCI DSS compliance is being practiced and enforced today, providing answers to three key questions:

- State of compliance: How is the PCI DSS perceived and prioritized in business?
- Achieving compliance: How are businesses living up to PCI DSS requirements?
- Protecting cardholder data: Where is data at risk and how is it being protected?

State of compliance

Businesses are still not taking data security seriously and are struggling with compliance costs. More than half (51 percent) of QSAs say merchants are not proactively managing data privacy and security, while less than a quarter (24 percent) report that they are. Businesses continue to feel overwhelmed by the cost of PCI DSS compliance. 54 percent of QSAs report that their clients find PCI DSS compliance too costly; only 20 percent say clients are satisfied with compliance costs.

Business units own compliance assessment budgets, but IT security must ensure compliance. According to QSAs, the IT security organization is the group most often responsible for ensuring compliance, at 30 percent. However, business units are most likely to own the budget for assessing PCI compliance, at 40 percent.

Few organizations fail compliance, but many rely on mechanisms not prescribed by the PCI DSS. Only 2 percent of merchants assessed by QSAs fail, but 41 percent are relying on compensating controls. While compensating controls are allowed in order to achieve compliance when an

[1] The full PCI DSS is available for download at https://www.pcisecuritystandards.org/security_standards/pci_dss_download.html

organization can't live up to the PCI DSS, these may be temporary fixes that might be eliminated by future changes to the PCI DSS.

Achieving compliance

Restricting access to card data is the most important PCI DSS requirement, but also the most difficult to achieve. QSAs believe controlling access to credit card data on a need-to-know basis (PCI DSS Requirement #7) is the most difficult requirement for merchants to achieve compliance with, as well as the most important.

Firewalls and encryption are the most effective technologies for achieving compliance. QSAs find that firewalls, encryption for data at rest, and encryption for data in motion are the top three most effective technologies for achieving compliance. Out of 18 technologies, the least favored technologies are website sniffers, credentialing systems, and intrusion detection/prevention systems.

Cost of annual audits averages $225,000 per year for the largest merchants. Excluding technology, operating, and staff costs, the world's largest acceptors of credit cards (also known as Tier 1 merchants) are spending an average of $225,000 on auditor expenses. 10 percent of these businesses are spending $500,000 or more annually on PCI auditors.

Protecting cardholder data

Handling chargebacks still requires storage of cardholder data. QSAs report the three most common business reasons for storing cardholder data are handling chargebacks, providing customer service, and processing recurring subscriptions. These longstanding processes are requiring merchants to introduce new methods of protecting cardholders.

Cardholder data is most at risk traveling across merchant networks and stored in databases. QSAs find the most significant threats to cardholder data are in merchant networks and databases. Other risk areas include point-of-sale (POS) and payment processing applications.

Encryption is the favored technology for achieving end-to-end cardholder data protection. 60 percent of QSAs believe encryption is the best means to protect card data end-to-end, compared to 35 percent for tokenization. For storing data in databases, QSAs recommend encryption (51 percent) more often than tokenization (22 percent). However, recommendations change when cardholder data is moved beyond databases, with 39 percent of QSAs preferring encryption and 33 percent preferring tokenization.

Controlling access to encryption keys is the most difficult key management task. For 41 percent of QSAs, controlling access to encryption keys is the most difficult key management task clients face, followed by key rollover (30 percent). 81 percent of QSAs recommend the use of a hardware security module (HSM) for encryption and key management, while 63 percent find that the use of HSMs reduces the time spent on compliance.

Methodology & Demographics

The purpose of this study by Ponemon Institute is to identify trends, recommendations, and preferences of QSAs involved in PCI DSS compliance. The survey questions focused on the background, experience, client observations, expected changes in the PCI DSS, preferences on how to achieve compliance, and typical client recommendations.

The selected sample was built from lists of information security and compliance professionals likely to be QSAs. In January 2010, 3,005 subjects were invited to participate in the survey, resulting in 155 usable responses. Only participants currently certified or working towards certification were accepted. All participants had been involved in at least one PCI DSS audit project over the last 12 months. All accepted surveys passed statistical reliability tests before being used in analysis. The final sample represents a 5 percent net response rate.

Data was captured through a web-based survey. No compensation was offered for participation. The margin of error on all adjective or ordinal responses is ≤3 percent for all completed items.

On average, the QSAs surveyed had participated in eight PCI DSS assessments over the last 12 months. 59 percent of these assessments involved Tier 1 merchants, and another 28 percent involved Tier 1 service providers. Designation of merchant and service provider levels is established by card brands and identifies the largest acceptors and processors of card transactions.

Figures 1 to 3 show the organizational characteristics of the QSAs participating in this survey. As shown in **Figures 1 and 2**, the largest segment of QSAs surveyed (46 percent) work in IT security services firms and work in organizations with fewer than 50 employees (38 percent). All QSAs' organizations performed audits in the United States.

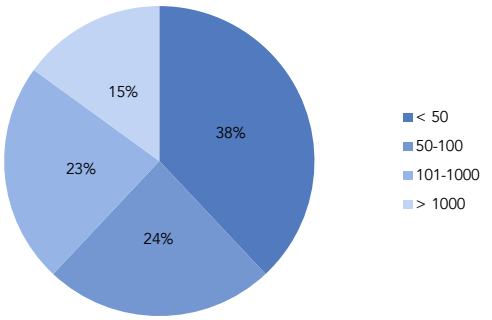


Figure 1: Number of employees in QSA organizations

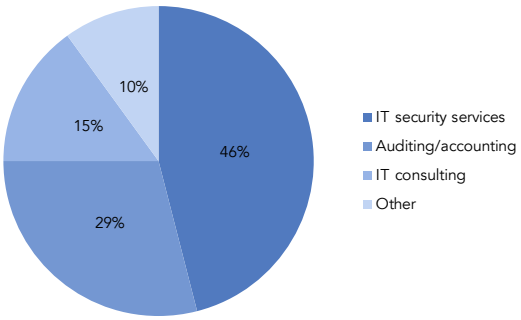


Figure 2: Type of organizations QSAs work for

Figure 3 shows 36 percent, 31 percent, and 5 percent of QSAs' organizations performed audits in Canada, Europe, and Asia Pacific, respectively.

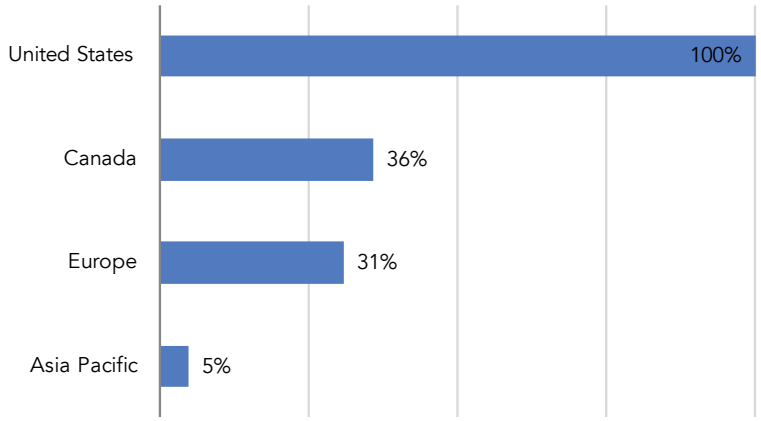


Figure 3: Regional auditing performed by QSAs' organizations

State of Compliance

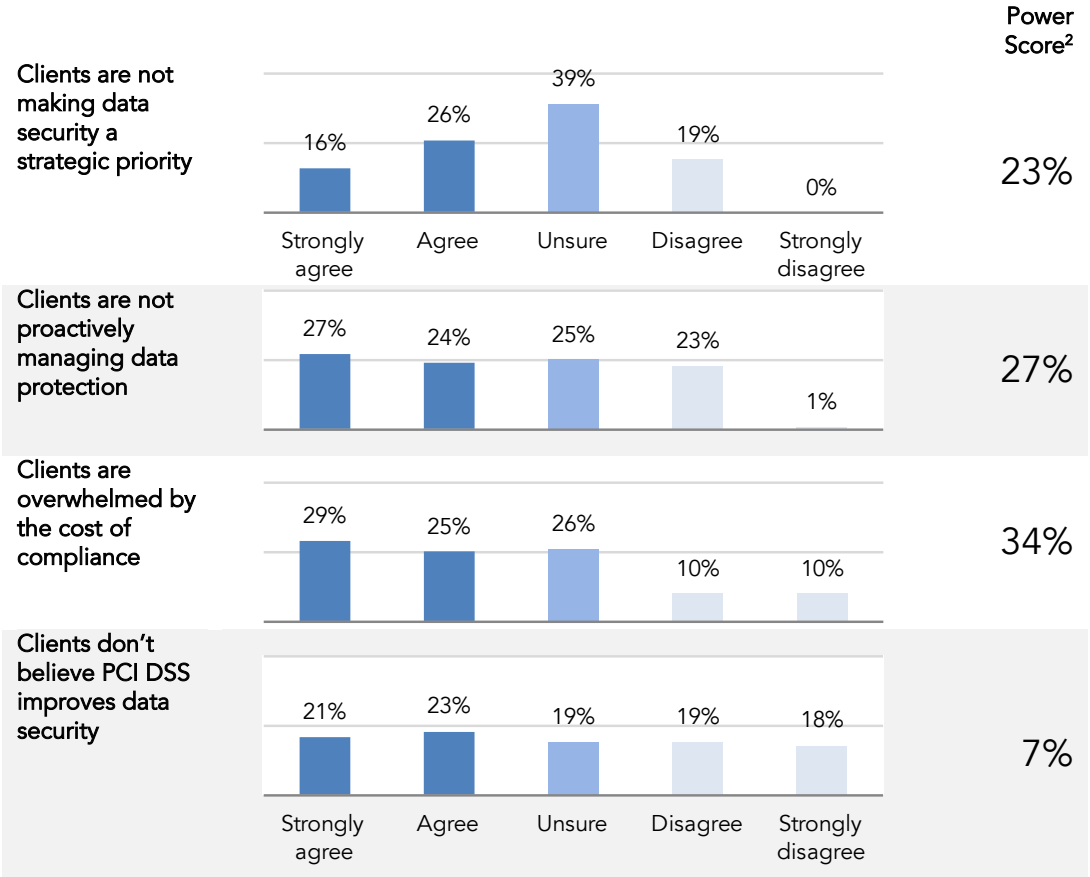
While QSAs are finding clients in compliance with the PCI DSS, they are also finding clients still not taking data privacy and protection as seriously as they should.

Managing risk, or compliance managing business?

After four years of merchants and service providers living with the PCI DSS, QSAs say their clients are overwhelmed by the PCI DSS and playing catch-up. **Figures 4 to 7** show that many QSAs are finding that their clients are:

- Not making data security a strategic priority (42 percent)
- Not proactively managing data privacy and protection (51 percent)
- Overwhelmed by the cost of compliance (54 percent)
- Uncertain if the PCI DSS helps improve data security

Merchants and service providers appear to treat the PCI DSS as just another compliance requirement instead of a core business initiative to reduce risk of data breaches.



Figures 4 to 7: QSA perception of clients' approach to the PCI DSS

[2] Power Score demonstrates the strength of agreement/disagreement on a subject. The further away from 0%, the more strongly views are held.

Business units hold assessment purse strings, but IT security is on the hook

QSAs report that business units most often own the budget for annual compliance assessments while IT security is responsible for ensuring compliance. Surprisingly, QSAs also find that legal teams are frequently responsible for assessment budgets. With different parts of the organization owning assessment budgets and being responsible for compliance, disagreements and varying priorities are certain to emerge. This is a likely contributor to the disappointing perceptions of the PCI DSS that QSAs are finding among clients (**Figures 4 to 7**).

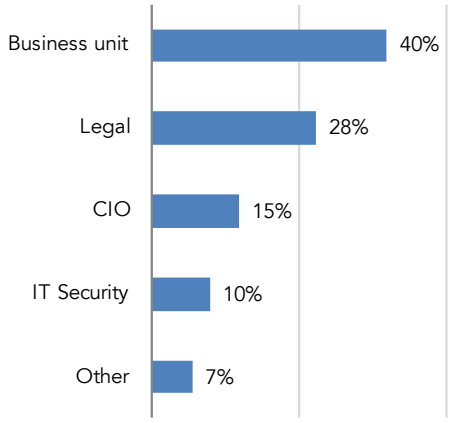


Figure 8: Budget ownership for annual compliance assesment

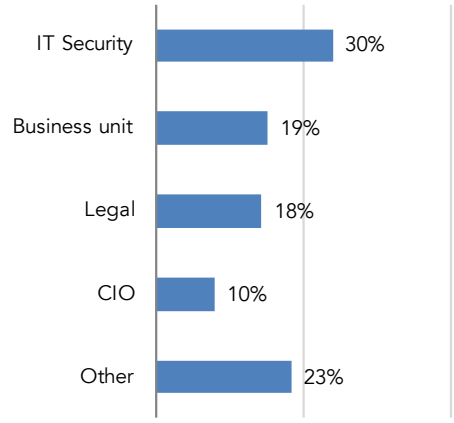


Figure 9: Responsibility for delivering compliance

Masking a compliance bubble?

From card brands to acquiring banks, the PCI DSS is being pushed in an effort to stop the embarrassing and costly data breaches that have become all too familiar. This push has put businesses under pressure to successfully pass annual audits and achieve compliance.

Few businesses are failing to do so. QSAs report that on average only 2 percent of their clients actually fail compliance outright, as shown in **Figure 10**. But 41 percent of clients would fail if compensating controls were not allowed (see **Figure 11**).

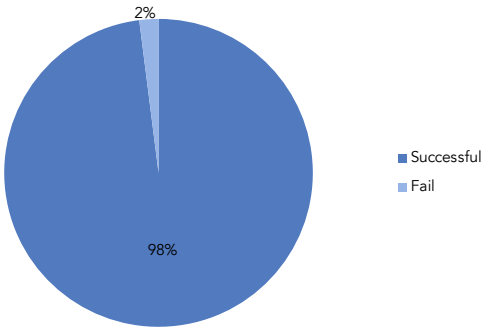


Figure 10: Businesses failing annual PCI DSS audits

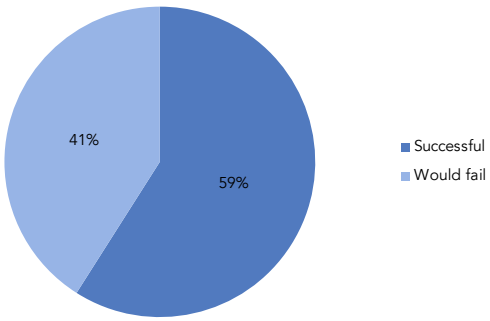


Figure 11: Businesses that would fail annual PCI DSS audits if compensating controls not allowed

According to PCI DSS Appendix B, compensating controls must:

1) Meet the intent and rigor of the PCI DSS
2) Provide similar level of defense as the PCI DSS
3) Be "above and beyond" other PCI DSS requirements
4) Balance the risk of not adhering to the PCI DSS

As defined by the PCI DSS, compensating controls are not shortcuts to or ways around compliance. Compensating controls are especially common for legacy systems (for example, an older system may not support encryption). While allowed, compensating controls may not address evolving threats. And an update to PCI DSS could eliminate a control completely.

It's unlikely that a compliance bubble is looming that would find large numbers of businesses failing audits after a change in the PCI DSS. However, QSAs and their clients need to be extremely diligent in specifying and assessing compensating controls.

Achieving Compliance

QSAs consistently agree that certain parts of the PCI DSS are more important and more difficult for clients to achieve compliance with than others. And while most of the largest merchants are paying less than $300,000 annually for QSA assessments, some are paying much more.

Controlling access to data: most important, most difficult

While 12 mandatory requirements make up the PCI DSS, it's clear that they are not equal in importance or difficulty. QSAs find that two requirements stand out:

- Most important and most difficult: *Requirement #7 – Restrict access to cardholder data by business need-to-know*
- Cannot be met with another control: *Requirement #2 – Do not use password defaults*

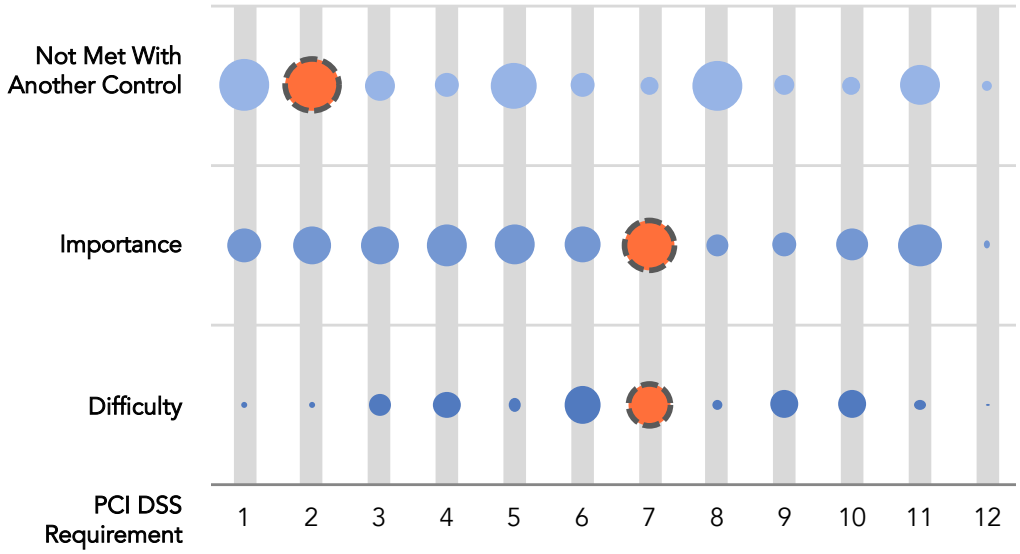


Figure 12: PCI DSS requirements in terms of their inability to be met with another control, their importance, and their difficulty. Circle size represents level of QSA agreement; orange circles with dashed outline indicate QSAs' top choice in each category.

As shown in **Figure 12**, QSAs consider the three most important requirements in the PCI DSS to be: #7 - *Restrict access to cardholder data by business need-to-know*, #11 - *Regularly test security systems and processes*, and #4 - *Encrypt transmission of cardholder data across open, public networks*. Requirement #7 is the most important for 80 percent of QSAs, making it the top choice by a margin of 11 percent. It was also cited as the most difficult requirement to achieve, by a margin of 9 percent. Chosen by 68 percent of QSAs, it is followed by #6 - *Develop and maintain secure systems and applications* and #10 - *Track and monitor all access to network resources and cardholder data*.

Possibly the most specific requirement, #2 - *Do not use vendor-supplied defaults for system passwords,* is the requirement QSAs were most likely to say cannot be met with another control, at 84 percent. However, it was closely followed by #1 - *Install and maintain a firewall configuration to protect cardholder data* (82 percent) and #8 - *Assign a unique ID to each person with computer access* (81 percent).

Firewalls and encryption: most effective technologies

When it comes to the technology used for achieving compliance, QSAs find that firewalls, encryption for data at rest, and encryption for data in motion are the three most effective technologies (see **Table 1**). The three least effective technologies were website sniffers, credentialing, and intrusion detection/prevention systems.

Technology	Effectiveness Ranking
Firewalls	1
Encryption for data at rest	2
Encryption for data in motion	3
Endpoint encryption solution	4
Identity & access management systems	5
Access governance systems	6
Anti-virus & anti-malware solution	7
Web application firewalls (WAF)	8
Correlation or event management systems	9
Data loss prevention systems	9
Code review	11
Virtual privacy network (VPN)	12
Perimeter or location surveillance systems	13
Database scanning and monitoring	14
Traffic intelligence systems	15
Intrusion detection or prevention systems	16
ID & credentialing system	17
Website sniffer or crawlers	18

Table 1: Most effective technologies for achieving compliance

Annual audits cost Tier 1 merchants $225,000

In most cases, the largest merchants and service providers, identified as Tier 1, are required to be assessed by an annual onsite QSA audit.[3] Audits last weeks and involve multiple QSAs. Those being audited not only incur the assessment fees charged by QSAs but also lose time and opportunity costs as staff refocus to assist with the audit. QSAs report that their assessment fees cost Tier 1 merchants an average of $225,000 annually. For 10 percent of Tier 1 merchants, assessment fees were more than double the average, exceeding $500,000 annually (see **Figure 13**).

[3] For MasterCard and Visa, Tier 1 merchants are those accepting 6 million or more card transactions annually. Tier 1 service providers are those processing more than 300,000 transactions annually.

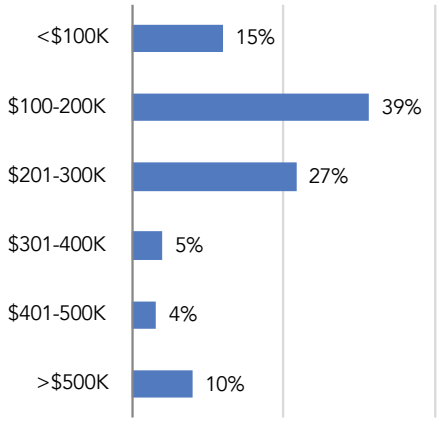


Figure 13: Annual onsite QSA assessment fees for Tier 1 merchants (USD)

In 2009, when MasterCard announced that onsite QSA audits would be required for Tier 2 merchants, it appeared that the number of mandatory QSA audits would increase significantly. However, MasterCard reversed this decision and, like Visa, will allow internal audit teams to perform annual assessments. MasterCard also announced Tier 1 merchants could use qualified internal audit teams instead of QSAs to perform annual assessments. This extends a similar provision already in place by American Express. In the future, this trend may put downward pressure on annual QSA assessment fees as merchants weigh the costs and benefits of using internal auditors instead.

Protecting Cardholder Data

Four years after the introduction of PCI DSS, QSAs find merchant networks and databases most at risk of being breached. QSAs agree on encryption for end-to-end protection but see tokenization as a promising option. And while encryption key management is challenging, QSAs view hardware security module (HSM) technology as a way to help ease the burden.

Why store cardholder data anyway?

Significant efforts of the PCI SSC, along with the PCI DSS and supporting documentation, are focused on reducing storage cardholder data by merchants. Eliminating storage of cardholder data would not only reduce the risk of breaches but also likely reduce the scope for audits, saving time and money. So why do merchants keep cardholder data around?

QSAs find that significant business processes rely on retaining and using cardholder data. QSAs report the most frequent reason for storing cardholder is to handle chargebacks (the result of issuing card banks reversing transactions). Typically initiated by cardholders, chargebacks are commonly caused by customer disagreements with merchants, as well as fraud. Merchants use stored cardholder data to identify transactions.

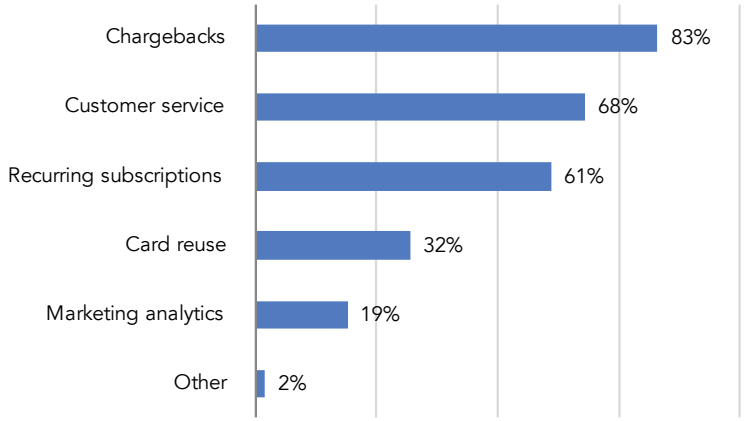


Figure 14: Reasons for merchant storage of cardholder data

As shown in **Figure 14**, other common reasons merchants store cardholder data, according to QSAs, is to handle customer service questions, such as finding a transaction for refund, and processing recurring transactions. For compelling business reasons like handling fraud and increasing revenue with recurring subscriptions, it seems merchants are unlikely to move away from storing cardholder data anytime soon.

Merchant networks and databases most at risk

From the initial transaction capture at point of sales (POS) terminals, cardholder data may cross multiple merchant networks, be processed by multiple applications, be transferred to payment processors for authorization, and be stored in merchant databases. At any of these points, cardholder data may be at risk of being breached. Criminals could be listening to networks, malware could be trapping data on servers, or an insider could steal data dumps from databases.

During annual assessments, QSAs look in these places and others as they assess merchant compliance. As shown in **Figure 15**, QSAs reported the two systems most at risk are merchant networks (51 percent) and databases (43 percent).

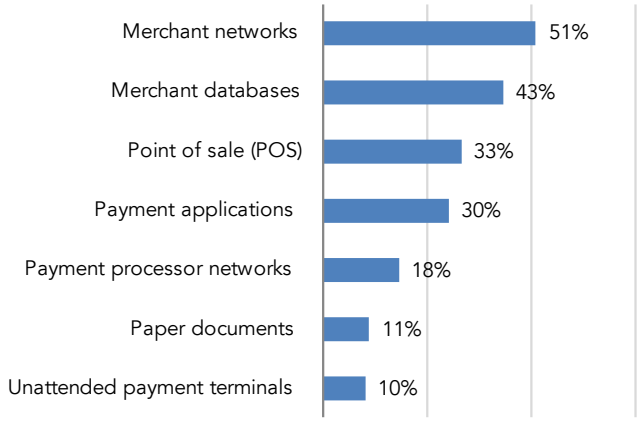


Figure 15: Systems most at risk for cardholder data breaches

While payment applications and payment processor networks have been sources of high-profile cardholder data breaches, these are generally not part of merchant QSA assessments. Payment applications, including POS systems, used by merchants must meet the requirements of the Payment Application Data Security Standard (PA-DSS). These applications go through vendor-managed certification. Most merchants must use PA-DSS-certified applications by July 2010.

QSAs' preference for end-to-end protection

What if cardholder data could be secured from the time a card transaction is captured, through processing, and as long as the referenced cardholder data was required? This goal, commonly referred to as end-to-end cardholder data protection, has been a popular topic in the PCI community. Merchants and payment processors are especially interested in the possibility of dramatically reducing the scope of PCI DSS audits by implementing end-to-end protection.

Fueled by this and other interest, the PCI SSC commissioned PricewaterhouseCoopers to investigate PCI community recommendations for new technologies, especially those that might deliver end-to-end protection and scope reduction.[4] Four technologies closely examined included end-to-end encryption and tokenization.[5] End-to-end encryption extends the use of encryption throughout the payment lifecycle. Tokenization replaces card numbers when accepted with a unique reference value that looks and acts like card data.

[4] *PCI security standards council selects PricewaterhouseCoopers for emerging technology review and recommendations project*, PricewaterhouseCoopers, 24 June 2009, http://www.pwc.com/us/en/press-releases/PCI-security-standards-council-selects-pwc.jhtml
[5] *PCI Council examines merits of new technologies*, SC Magazine, 25 September 2009, http://www.scmagazineus.com/pci-council-examines-merits-of-new-technologies/article/149709/

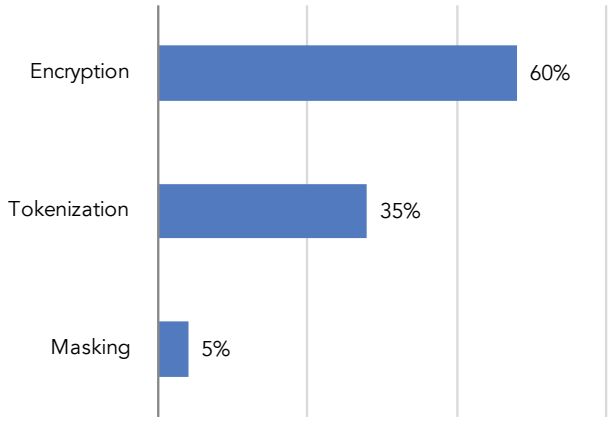


Figure 16: Preferred method for end-to-end cardholder data protection

As shown in **Figure 16**, QSAs overwhelmingly prefer encryption (60 percent) and tokenization (35 percent) to deliver end-to-end cardholder data protection today. While an "Other" category was provided, none of the 155 survey participants selected the response. Encryption and tokenization are clearly the two technologies to watch as cardholder data protection continues to evolve.

Protecting data in databases and beyond: encryption and tokenization rule

With QSAs most concerned about cardholder data traveling across networks and stored in databases (see **Figure 15**), validating the protection of this data is a high priority in the assessment process. For 51 percent of QSAs, encryption is the preferred means to protect cardholder data stored in the database. However, **Figure 17** shows that when data is transferred outside of a database for use with other applications, tokenization is an increasingly preferred option, recommended by only 6 percent fewer QSAs than encryption.

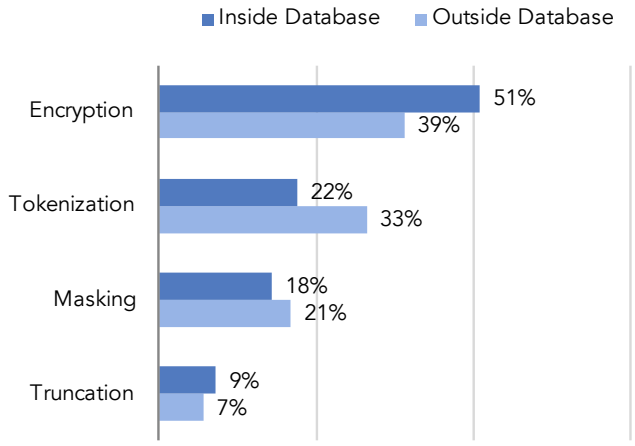


Figure 17: Recommendations for protecting cardholder data in databases and applications

These differing preferences suggest that QSAs appreciate tokenization's ability to fit with existing applications and data formats. New methods of encryption, sometimes referred to as format-

preserving encryption, can also retain the attributes of card numbers but are relatively new to the market.

Over a quarter of QSAs recommend masking or truncation for protecting cardholder data inside and beyond merchant databases. Unlike encryption or tokenization, these methods permanently alter card numbers by dropping digits. While card numbers can no longer be reconstituted, this data is recognized as out-of-scope for PCI DSS compliance and eliminates the risk of data being used for fraud.

Encryption key management challenges

When encryption is used to protect cardholder data, PCI DSS Requirement #3 – *Protect stored cardholder data* specifies how encryption should be managed. Access to encryption keys must be tightly controlled and regular maintenance performed to ensure that using encryption doesn't provide a false sense of security. Key management is not only important for applications such as web or database encryption; tokenization systems also use encryption to protect the primary store of reference card numbers.

PCI DSS Requirement #3.5 mandates that encryption keys be protected from misuse and limits the number of locations where encryption keys are stored. Requirement #3.6 requires that key management practices be documented and implemented that include changing keys periodically (referred to as rollover) and controlling access to keys.

41 percent of QSAs find the most challenging aspect of key management for clients is controlling access to keys. While encryption keys may be password-protected, frequently keys are stored on file systems, and decryption passphrases are shared among administrators. This makes controlling access and use of keys difficult. 30 percent of QSAs find that key rollover is the second most challenging aspect of key management under the PCI DSS, which requires keys to be changed to reduce the risk of a single older key being compromised and used by criminals.

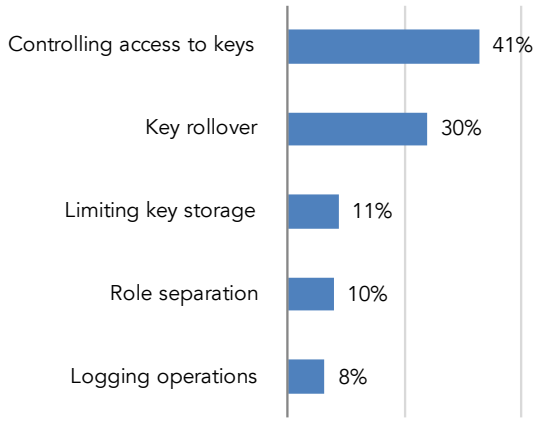


Figure 18: Most challenging aspect of encryption key management for PCI DSS compliance

One way businesses are making compliance with PCI DSS Requirement #3 easier is the use of HSMs. HSMs move key management functions such as storage, access control, and rollover to dedicated appliances. By eliminating manual processes and additional documentation, IT teams can spend less time, and in the end less money, on showing compliance with key management

requirements. 63 percent of QSAs agree that HSMs reduce the time spent demonstrating PCI DSS compliance when using encryption (see **Figure 19).** In fact, 35 percent of QSAs require HSMs to be used and another 46 percent of QSAs recommend HSMs to their clients (see **Figure 20**).

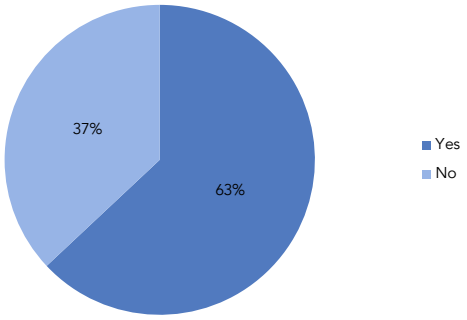


Figure 19: Hardware security modules reduce time spent on PCI DSS compliance

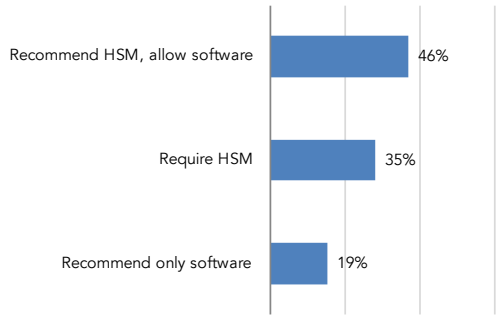


Figure 20: QSAs recommend hardware-based key management

Conclusion

Based on their experience with hundreds of PCI DSS assessments, QSAs paint a consistent picture of PCI DSS compliance today. They consider the implementation of restricting controls – whether they be to restrict viewing of cardholder data or access to database encryption keys – the most important aspect of compliance but also the most difficult aspect for clients to achieve. And while QSAs report that the vast majority of their clients are passing audits, roughly half of the merchants are relying on QSA-approved compensating controls (a finding relatively unknown until now). These organizations' ability to weather evolving threats and changes to the PCI DSS is unknown and needs to be closely watched.

Not surprisingly, QSAs are in agreement that merchant networks and databases continue to be the most vulnerable components of the payment system. Well-engrained business practices like handling chargebacks and new revenue opportunities like subscriptions will keep merchants storing cardholder data. To protect this information, encryption is the preferred method of QSAs. They agree that encryption can best protect data in databases and applications, but are attracted to tokenization's ability to fit nicely with merchant applications. This attraction may represent a growing trend. Finally, with over three-quarters of QSAs recommending hardware security modules (HSMs) to clients, the use of the devices may well become more than just a best practice in future PCI DSS updates.

Based on the insights into QSA perspectives outlined in this report, merchants and service providers should review their approach to cardholder data protection. A focus on protecting cardholder data itself is the best way to secure customer trust and achieve compliance. Otherwise, complying with PCI DSS will always be a game of catch-up.

By focusing on cardholder data protection, merchants and service providers can address QSAs' concerns about restricting access to cardholder data. The QSA process and technology recommendations highlighted in this report, especially encryption, tokenization, and hardware-based key management, can help businesses prioritize their investments. With this approach, access can be controlled and data protected, whether data is travelling across networks or stored in databases. Putting data protection first will also better position merchants to stop the range of evolving threats facing the payments industry—threats that could result in changes to the PCI DSS. In the end, this approach will make compliance an easier endeavor for everyone involved.

Following the publication of this research, a companion report will soon be available. It will focus on issues impacting the QSA business model and the changes QSAs expect in the upcoming 2010 update to the PCI DSS. The report will also include more information on assessment fees and how changes to the PCI DSS and card brand actions might affect demand for QSA services.

About Ponemon Institute

Ponemon Institute was founded in 2002 by Dr. Larry Ponemon. Headquartered in Michigan, Ponemon Institute is considered the pre-eminent research center dedicated to privacy, data protection and information security policy. Our annual consumer studies on privacy trust are widely quoted in the media, and our research quantifying the cost of a data breach has become valuable to organizations seeking to understand the business impact of lost or stolen data.

Our research has made Ponemon Institute a thought leader on trends in corporate and government practices, consumer perceptions, and potential cyber and insider threats that will affect the collection, management, and safeguarding of sensitive and confidential information. Our benchmark studies on privacy and data security practices provide guidance on how organizations can become better at building trust with their customers, employees, and business partners.

For more information about our institute and the services we offer, please contact us at 1.800.887.3118 or email us at research@ponemon.org.

About Thales

Thales is one of the world leaders in the provision of information and communication systems security solutions for government, defense, critical infrastructure operators, enterprises and the finance industry. Thales's unique position in the market is due to its end-to-end security offering spanning the entire value chain in the security domain. The comprehensive offering includes architecture design, security and encryption product development, evaluation and certification preparation, and through-life management services.

Thales has an unrivalled 40-year track record of protecting information ranging from "sensitive but unclassified" up to "top secret," as well as a comprehensive portfolio of security products and services, including network security products, application security products, and secured telephony products.

To learn more, please visit http://iss.thalesgroup.com.