

Forrester Consulting

MAKING LEADERS SUCCESSFUL EVERY DAY

September 2007

The State Of PCI Compliance

A commissioned study conducted by Forrester Consulting on behalf of RSA, the Security Division of EMC

FORRESTER®

FORRESTER

Headquarters

Forrester Research, Inc., 400 Technology Square, Cambridge, MA 02139 USA
Tel: +1 617.613.6000 • Fax: +1 617.613.5000 • www.forrester.com

Table Of Contents

Executive Summary	3
Introduction	4
Methodology.....	5
Merchants Typically Keep Too Much Data.....	6
Encryption and Access Control Are The Top Challenges.....	8
Conclusions	17

© 2007, Forrester Research, Inc. All rights reserved. Forrester, Forrester Wave, RoleView, Technographics, and Total Economic Impact are trademarks of Forrester Research, Inc. All other trademarks are the property of their respective companies. Forrester clients may make one attributed copy or slide of each figure contained herein. Additional reproduction is strictly prohibited. For additional reproduction rights and usage information, go to www.forrester.com. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

Executive Summary

RSA, the Security Division of EMC, engaged Forrester Research to conduct a study of both US and European organizations to better understand their priorities and challenges around data protection and Payment Card Industry (PCI) compliance. In order to meet this challenge, Forrester fielded an online survey in July 2007, to organizations in the US, UK, Germany, Spain, and France. Forrester also made an effort to spread responses across various industries and include the top-tier transaction processing organizations (i.e., PCI Level 1, Level 2, and Pre-level 2). Forrester synthesized the results of the survey with existing research and its industry expertise in order to create the following report.

The following are among the key findings from the study:

Merchants Typically Keep Too Much Data

- Organizations typically store much more about the credit card than just the card numbers.
- Organizations processing a high volume of transactions exhibit the most egregious behavior.
- The drivers behind keeping credit card data vary by geography and size.

Encryption And Access Control Are The Top Challenges

- IT owns credit card data protection, with a bulk of the responsibility falling on the CISO and CIO.
- Encryption and identity and access management top the list of challenges for protecting credit card data.
- Data segregation and encryption are the most commonly deployed credit card data protection mechanisms.
- Organizations are most worried about data classification and access control policies surrounding their credit card data.

Organizations Are Using PCI Compliance As An Opportunity To Increase Security

- Mitigating the risk of data breaches is the top driver for PCI compliance.
- ISO 17799 and 27001 remain the predominate frameworks being used to comply with PCI.
- A majority of US and UK respondents will be fully PCI compliant within the next year.
- Retail, Media and entertainment, Financial services, and Healthcare are the industries most compliant with PCI.
- Organizations spend a significant portion of their IT budget on credit card data protection.
- Access management is the top audit deficiency for PCI compliance.

Introduction

More than 100 million personally-identifiable, customer records have been breached in the US over the past two years.¹ Most of these breaches occurred at companies that are household names. These breaches solidified the threat for many executives who had previously not taken security very seriously. As a result, boards and top executives are demanding reports from their IT and security staff on the effectiveness of security controls within their organizations. Moreover business partners and customers are demanding that organizations demonstrate more clearly how well they are dealing with sensitive data.

Credit card companies, faced with a potential backlash of consumers discouraged from using credit cards because of security concerns, responded by creating stringent standards for how merchants store and process credit card data. The Payment Card Industry Data Security Standard (PCI DSS) was created in 2004 to address these concerns and reduce the risk of consumers being adversely affected by the theft of credit card information from merchants' IT systems.

Consequently, many organizations are scrutinizing their efforts around data security in general and more specifically, the measures handed down by PCI. They want to be able to claim that they have exercised due care in establishing the needed security controls. In the past, PCI compliance levels have remained low because the consequences for noncompliance were not clear. Lately, however, the credit card companies have been threatening their clients with severe punitive consequences for noncompliance — including fines or loss of privileges to use their brands. This is providing an incentive for companies to give PCI compliance a higher priority

RSA commissioned this study to determine:

- What are the drivers for credit card data protection?
- What are the top challenges and priorities for organizations when protecting credit card data?
- How are organizations approaching PCI compliance, and what is the current compliance status?
- How are spending priorities changing for credit card data protection in general and PCI compliance in particular?

Methodology

In July 2007, RSA commissioned Forrester Consulting to survey US- and European-based organizations to understand their priorities and challenges around data protection and PCI. In this online survey:

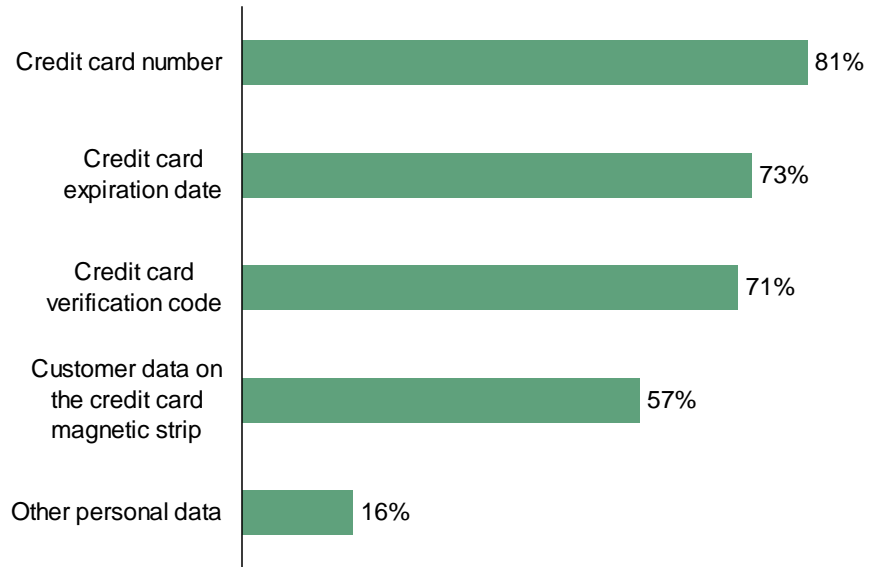
- Thirty-six percent of respondents were from the US, 23% from Spain, 19% from Germany, 17% from the UK, and 4% from France.²
- All respondents were involved with credit card data protection within their organizations.
- Ninety-four percent of respondents had management positions, and 68% of US respondents were from organizations with revenues more than \$1 billion, while 61% of European respondents were from organizations that had revenues more than €183 million.
- Of the US respondents, the following industries were represented: Retail and wholesale (22%), Financial services (20%), Consumer product manufacturing (18%), Telecommunication carriers (9%), Utilities and energy (8%), Hospitality (7%), Media and entertainment (5%), Insurance (4%), Healthcare (4%), and Higher education (3%).
- Of the European respondents, the following industries were represented: Hospitality (18%), Telecommunication carriers (16%), Consumer product manufacturing (11%), Utilities and energy (10%), Financial services (10%), Retail and wholesale (9%), Insurance (8%), Healthcare (7%), Media and entertainment (5%), and Higher education (4%).³
- Seventy-three percent of the respondents processed more than 1 million credit card transactions per credit card brand, 16% of respondents processed more than 6 million transactions, and 27% processed between 750,000 to 999,999 transactions per year.
- The respondents were categorized into three broad categories: Level 1, Level 2, and Pre-level 2 respondents. Level 1 respondents process more than 6 million credit card transactions per credit card brand, and they comprised 16% of the respondents. Level 2 respondents process more than 1 million transactions, but less than 6 million credit card transaction per card brand and made up 57% of the respondents. Lastly, Pre-level 2 respondents process more than 750,000 transactions but less than 1 million transactions per credit card brand and totaled 27% of the respondents. Overall, the Hospitality industry (23%), followed by the Retail and wholesale industry (18%), had the highest number of Level 1 providers.

Merchants Typically Keep Too Much Data

Forrester asked 677 respondents from the US and Europe about their current data retention practices. We found that:

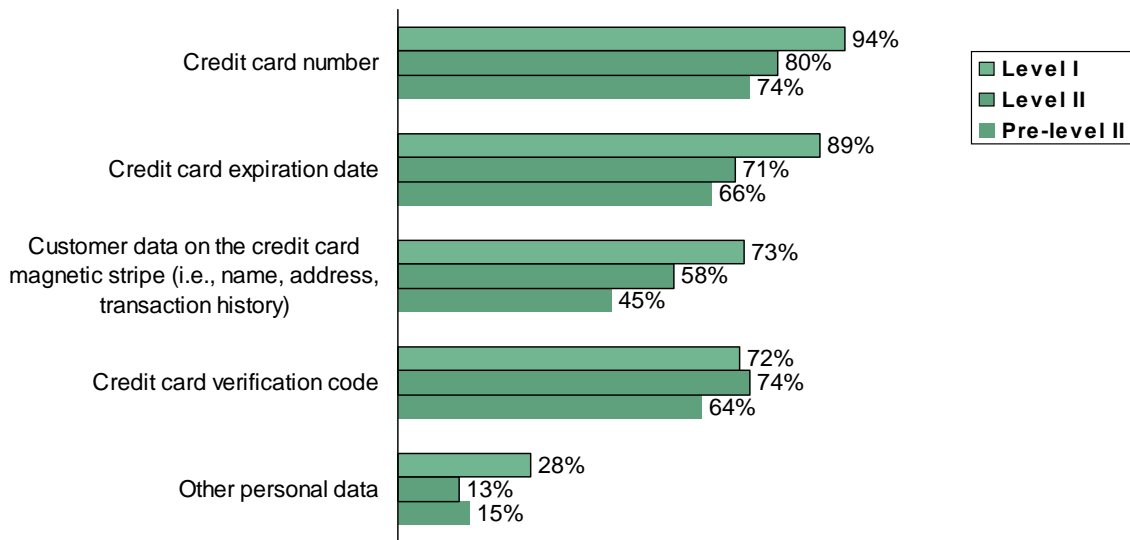
- **Organizations typically store much more about the credit card than just the card numbers.** A vast majority of the global respondents, 81% to be exact, retain credit card numbers (see Figure 1-1). Seventy-three percent store credit card expiration dates, and 71% store credit card verification codes. Fifty-seven percent of global respondents stated that they store magnetic stripe data in their environments.
- **Organizations processing a high volume of transactions exhibit the most egregious behavior.** Ninety-four percent of the Level 1 respondents retain credit card numbers, compared to 80% of Level 2 respondents (see Figure 1-2). Eighty-nine percent of Level 1 respondents retain credit card expiration dates, and 72% retain credit card verification codes, versus 71% and 74% respectively of Level 2 respondents. The Financial services, Healthcare, Insurance, and Higher education industries have the highest percentages for all stored data — including prohibited data.
- **The drivers behind keeping credit card data vary by geography and size.** Eighty-two percent of Level 1 respondents store credit card data for fraud analysis, compared to 66% overall (see Figure 1-3). Eighty percent of the Germans respondents store credit card data because they use it as a unique identifier, compared to the global average of 65%. Forty-one percent of the global respondents, versus 55% of the US respondents, use credit card data for business intelligence and analytics.

Figure 1-1: “What credit card data does your company store in its environment?”



(multiple answers accepted)
Base: 677 US and EU IT security decision makers

Figure 1-2: “What credit card data does your company store in its environment?”



(multiple answers accepted)
Base: 677 US and EU IT security decision makers

Figure 1-3: “What are the reasons why your company stores credit card data?”

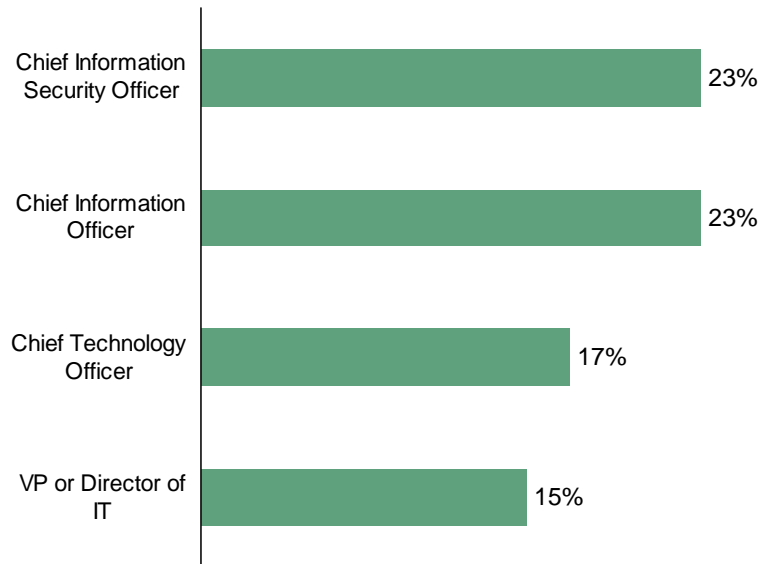


Encryption and Access Control Are The Top Challenges

Forrester then asked respondents about their priorities and challenges with regards to protecting credit card data. We found that:

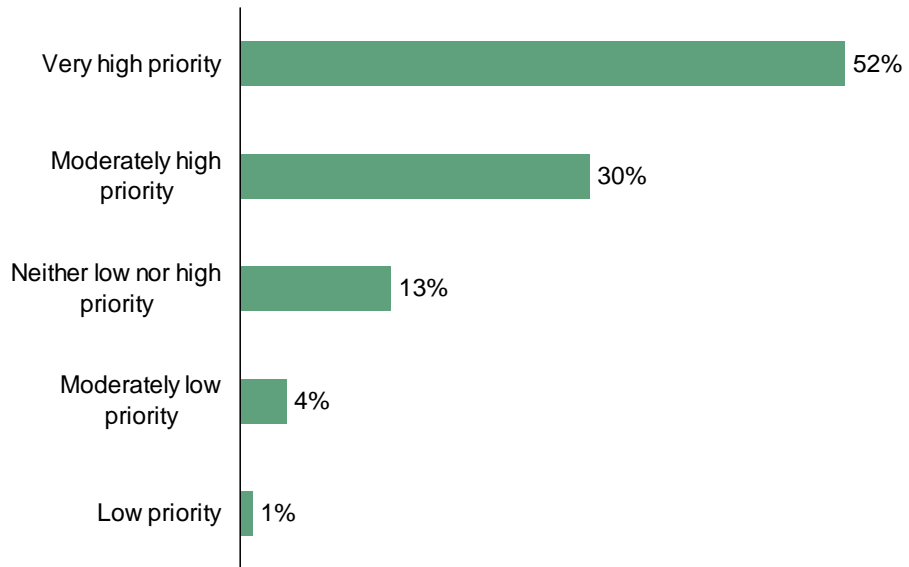
- IT owns credit card data protection.** Twenty-three percent of the global respondents reported that the CIO is responsible for credit card data protection (see Figure 2-1). Another 23% said their CISO is responsible, while 17% said their CTO. Fifteen percent pointed to a VP of IT or Security as the primary person in charge of credit card protection.
- Mitigating the risk of data breaches is a high priority.** More than 80% of the global respondents rated the importance of protecting against credit card data breaches as either a “very high priority” (52%) or “moderately high priority” (30%) (see Figure 2-2).
- Credit card data protection is a higher priority for organizations with higher transaction volumes.** Level 1 merchants are the most concerned with data breaches, with 72% of them rating this as a “very high priority” compared to 49% of Level 2 respondents (see Figure 2-3).
- Encryption and identity and access management top the list of challenges.** When asked what the most challenging area to protecting credit card data was, more than a quarter of the global respondents pointed to data encryption (27%) and identity and access management (27%) (see Figure 2-4). Almost half the respondents in US and UK cited these two challenges as their top challenges, whereas 69% of the respondents in Spain and France cited this as their top challenge. The remaining respondents rated their challenges as infrastructure (16%), system event monitoring (13%), policy enforcement (10%), and data discovery (6%).

Figure 2-1: “What executive in your firm is the most responsible for ensuring the protection of credit card data?”



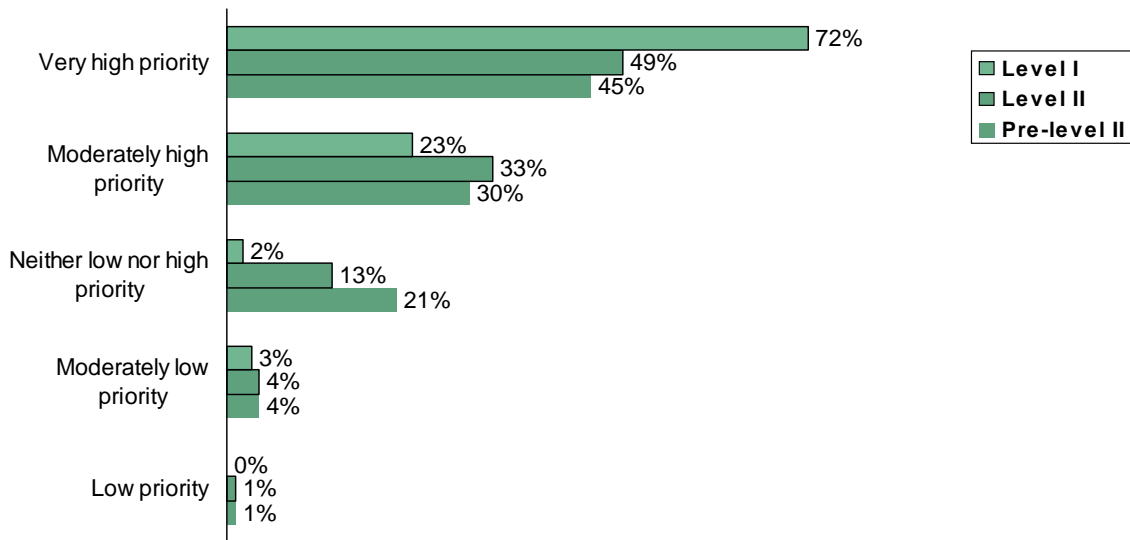
Base: 531 US and EU IT security decision makers

Figure 2-2: “How important of a priority for your firm’s management is it to protect against credit card data breaches?”



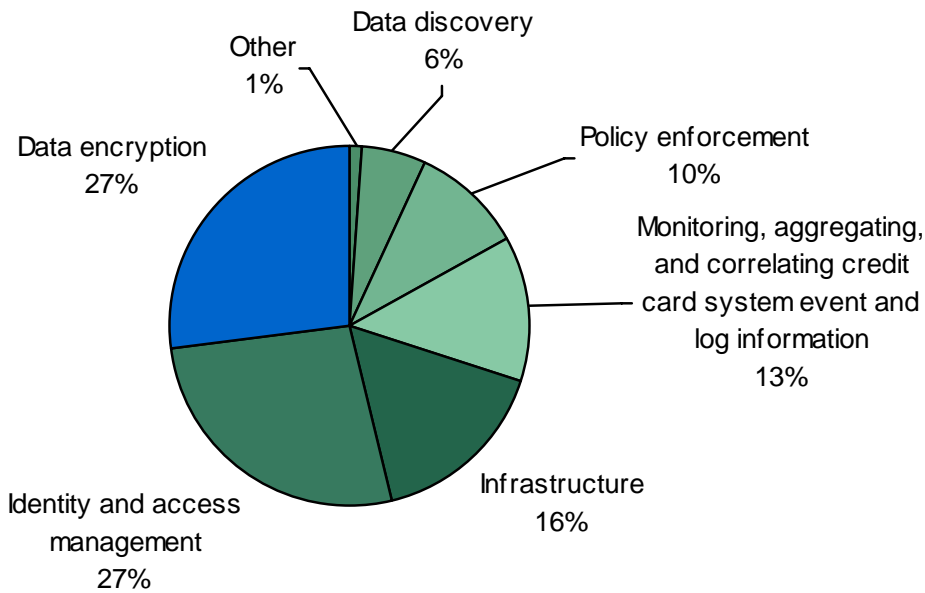
Base: 677 US and EU IT security decision makers

Figure 2-3: “How important of a priority for your firm’s management is it to protect against credit card data breaches?”



Base: 677 US and EU IT security decision makers

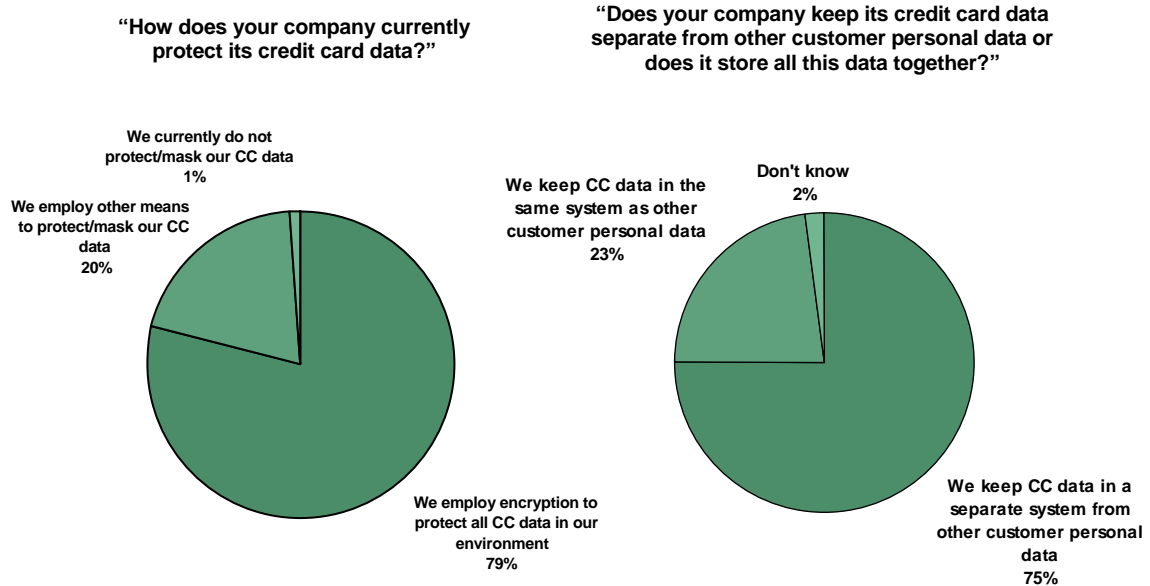
Figure 2-4: “What is the most challenging area in your environment to protecting the credit card data?”



Base: 677 US and EU IT security decision makers

- Data segregation and encryption are the most prevalent protection mechanisms.** The majority of the global respondents (79%) employ encryption to protect all credit card data in their environments (see Figure 2-5). Twenty percent employ other means to protect or mask credit card data, while only 1% currently do not protect or mask their credit card data. When segregating credit card data, 75% of the global respondents separate credit card data from other customer personal data, while 23% keep credit card data in the same system as other customer personal data.

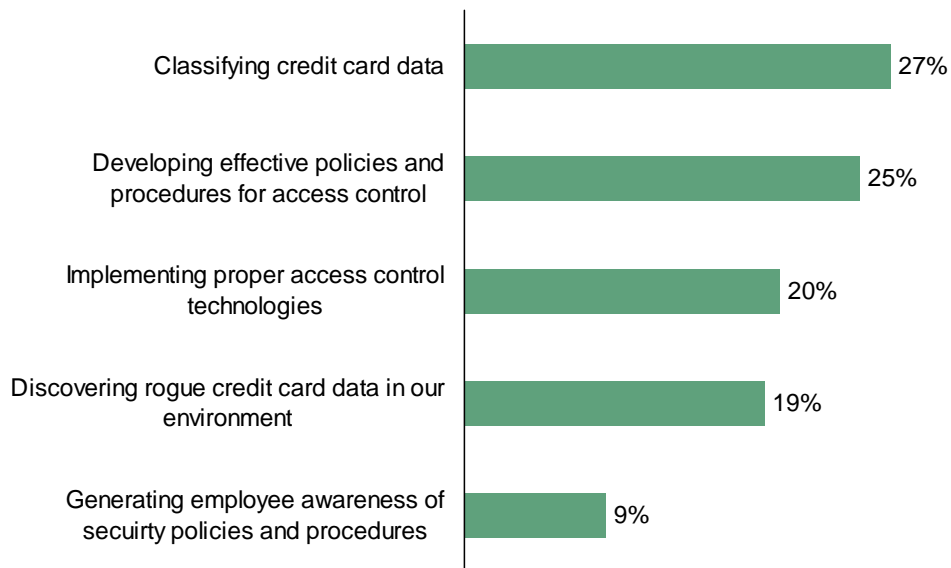
Figure 2-5: Protecting and storing credit card data



Base: 677 US and EU IT security decision makers

- **Data classification and policies top the list of access control concerns.** More than a quarter of respondents (27%) rated classifying credit card data as the single most significant challenge in controlling access to credit card data, while 25% thought developing effective policies and procedures for access control was the most difficult (see Figure 2-6). Implementing proper access control technologies, discovering rogue credit card data in their environment, and generating employee awareness of security policies and procedures were also rated as high concerns. Data classification was the biggest concern amongst the Insurance industry (53%) and in the Spain and France region (47%).

Figure 2-6: “What is the most significant challenge in controlling access to credit card data?”



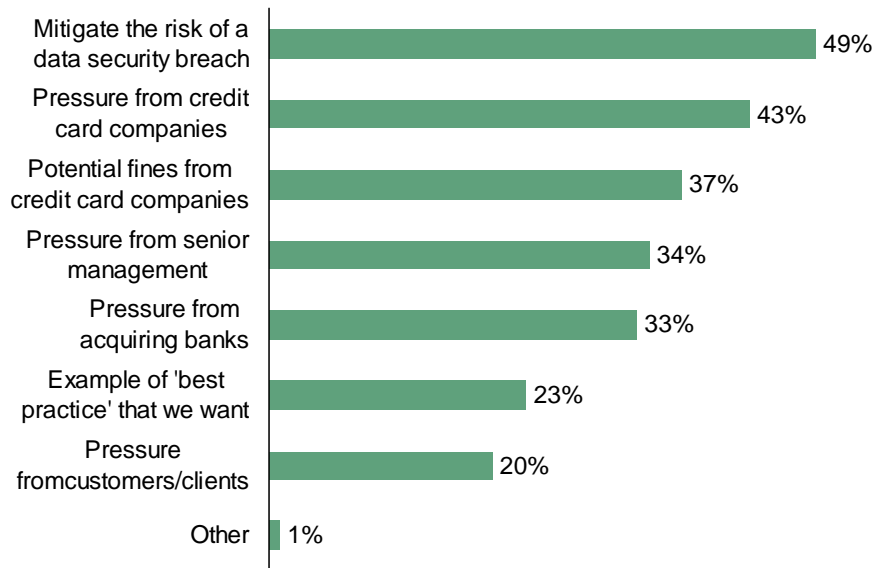
Base: 677 US and EU IT security decision makers

Organizations Are Using PCI Compliance As An Opportunity To Increase Security

Forrester asked the respondents about their plans for compliance, with particular focus on what frameworks would be utilized and what were their timelines for compliance. We found that:

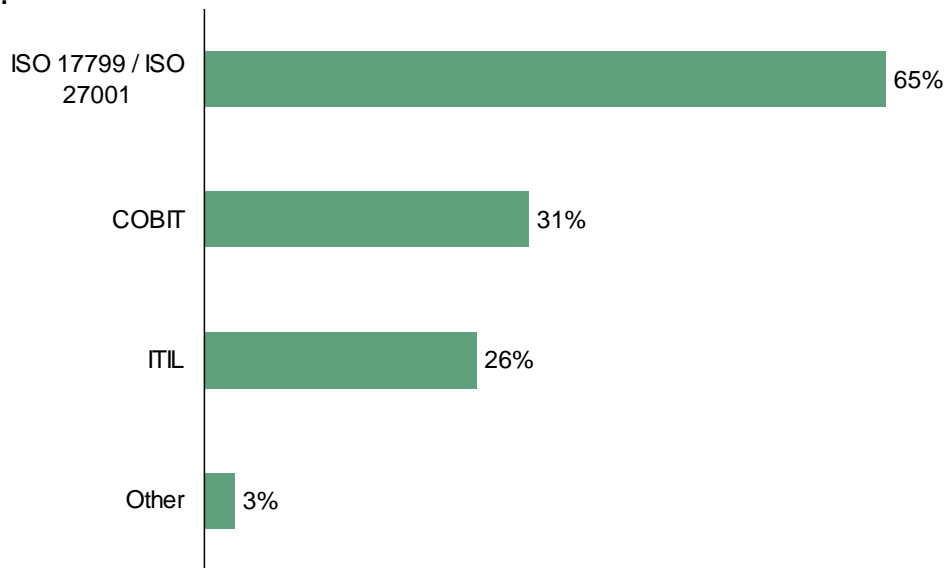
- **Mitigating the risk of data breaches is the top driver.** When asked about the current drivers for PCI compliance, 49% of the global respondents pointed to mitigating the risk of a security breach as the top driver (see Figure 3-1). Forty-three percent cited pressure from credit card companies as the top driver, followed by potential fines (37%), pressure from management (34%), pressure from acquiring banks (33%), desiring “best practices” (23%), and pressure from customers and clients (20%).
- **ISO remains the predominant framework being used to comply with PCI.** Sixty-five percent of the global respondents plan to utilize ISO’s 17799 and 27001 frameworks for deriving controls to address PCI compliance (see Figure 3-2). COBIT and ITIL came in at 31% and 26% respectively. Three percent of respondents plan to utilize some other framework or none at all.
- **A majority of respondents in the US and UK will be compliant within the next year.** Sixty percent of respondents in the US and 57% in the UK plan to be fully compliant in the next year, while 51% of Germans and 40% of Spaniards and French are planning to take more than one year to comply with PCI (see Figure 3-3). Twenty-two percent of the global respondents plan to take at least 2 years or more before becoming fully PCI compliant.

Figure 3-1: “What are the current drivers in your organization for complying specifically with PCI?”



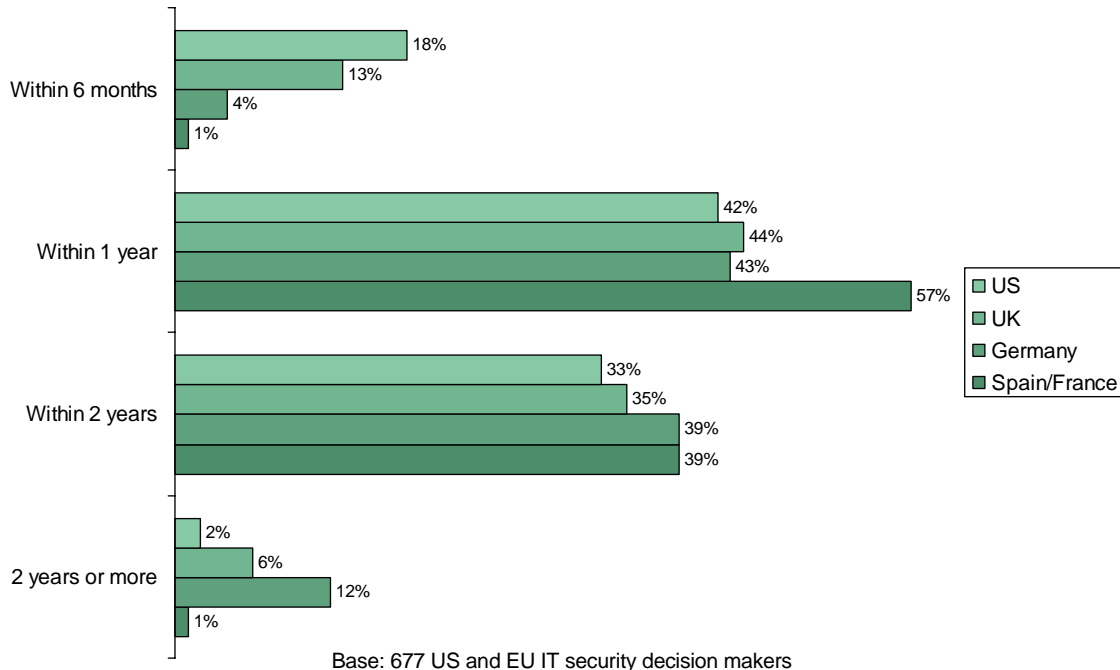
Base: 677 US and EU IT security decision makers

Figure 3-2: “Are you using any standards or frameworks for PCI compliance other than the PCI-DSS?”



Base: 677 US and EU IT security decision makers

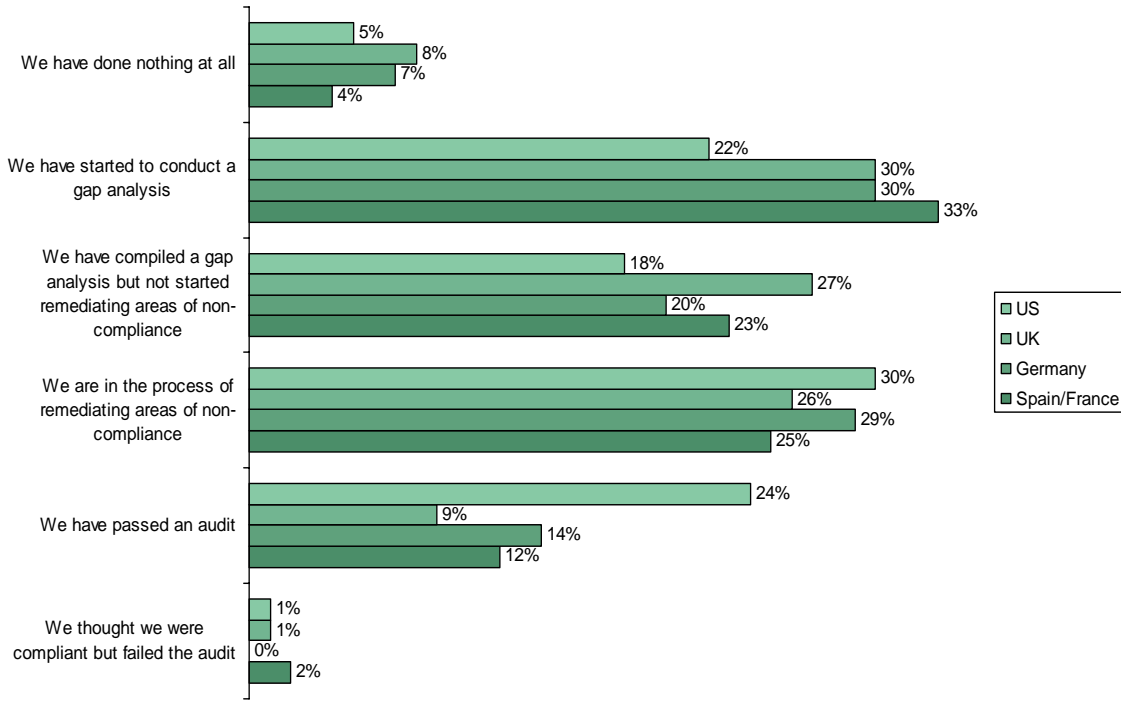
Figure 3-3: “What is your timeframe for full compliance with PCI?”



- Retail, Media and entertainment, Financial services, and Healthcare are the industries most compliant to PCI.** Fifty-eight percent of respondents in the Media and entertainment industry were in the process of remediating areas of non-compliance or had already passed an audit, along with 44% in the Retail and wholesale industry and 45% in the Hospitality industry. Thirty-four percent of the Healthcare respondents, 19% of Retail and wholesale, and 19% of Media and entertainment respondents said that they had already passed the PCI audit, while the Insurance (11%) and Telecom (11%) industries had the lowest percentage of passed audits. Twenty-four percent of the respondents in the US, 9% in UK, 14% in Germany and 12% in Spain and France said that they had passed the PCI audit (see Figure 3-4).
- Organizations spend a significant portion of their IT budget on credit card data protection.** More than half of the global respondents (55%) plan on spending between 2% to 4% of their IT budget on credit card data protection in the future (see Figure 3-5). For a vast majority (76%) of the respondents it was an increase from 2007 budgets.
- Access management is the top audit deficiency for PCI.** Forty-six percent of respondents reported the lack of appropriate access management (access control, identity management, physical security) as the top area of non-compliance (see Figure 3-6). The remaining top areas include lack of appropriate monitoring and testing (39%), lack of appropriate infrastructure management (36%), lack of credit card data protection controls (23%), and poor security policies (8%).

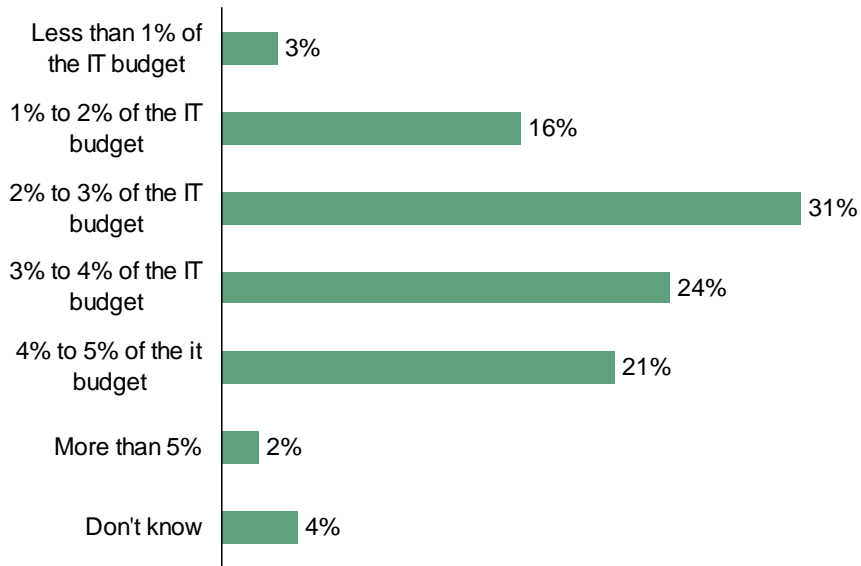
The State Of PCI Compliance

Figure 3-4: “Which statement best describes your current status with respect to PCI?”



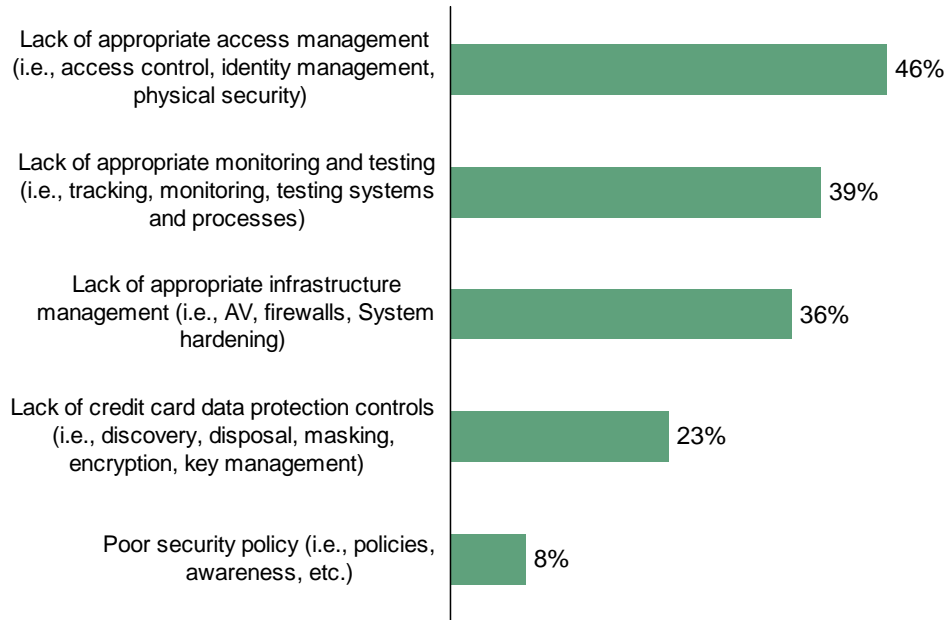
Base: 677 US and EU IT security decision makers

Figure 3-5: “What are your organization’s current budget trends for supporting/assisting credit card data protection for the next 12 months?”



Base: 677 US and EU IT security decision makers

Figure 3-6: “What are your current areas of non-compliance?”



Base: 677 US and EU IT security decision makers

Conclusions

The survey data suggests that respondents around the globe are aware of the PCI standard and are working towards becoming compliant, but there are some significant differences by industry, geography, and the organization's transactions volume. Specifically, we found that:

- **Organizations need to reengineer business processes to protect credit card data.** Although many have separate credit card environments today, they still report multiple problems in dealing with credit card data appropriately, with data discovery and data retention still as significant issues. This is because they have protected the credit card environment, but they have not developed the needed processes in order to manage the flow and protection of data as it flows outside of those environments.
- **As compliance programs mature the focus shifts to risk management.** A majority of the global respondents reported using the ISO framework for PCI compliance, having a desire for an integrated product suite, and that their top driver for PCI compliance was to manage the risk of data breaches. All of these factors point to a maturity in security and compliance programs, where the focus has shifted from merely complying with the letter of the standard, to a more holistic view of managing the risks.
- **Organizations will continue to spend significantly on PCI compliance.** A majority of the global respondents said that they are spending more on credit card data protection than in the past and will continue to focus on securing credit card data in the future. Organizations are spending a significant portion of their IT budgets on credit card data protection not just because of PCI compliance, but also to protect their organization against breaches.

Recommendations

- **View compliance as part of your risk management strategy — not a stand alone project.** If security and compliance are not aligned there usually is a lot of duplication and inefficiency. Organizations should be looking to align security controls and develop a framework that can fulfill the requirements of both simultaneously.
- **Protect the data, not just the environment where it is stored.** Spending on encryption and access control will help you protect the data while it resides within a controlled environment. However, with today's business demands for sharing data with internal and external environments, ensuring that the data is appropriately protected as it takes on different forms and flows into other environments will be essential. Map out all the places credit card data is stored and processed inside and outside of your environment, and make sure it is protected at all times during its lifecycle.
- **Make people and process a priority to maximize technology investment.** People and process issues will dominate future spending. In the past, companies have spent a majority of their budgets on technology to protect their environments, but as companies start to take a risk-based approach they are realizing that focusing on people and process will be just as important in protecting the organization. Future spending will need to account for areas like awareness, as well as training and improving internal process to protect against breaches and improve efficiency.

The State Of PCI Compliance

¹ Source: www.privacyrights.org

² Numbers do not add up to 100% due to rounding.

³ Numbers do not add up to 100% due to rounding.