2017 Payment Security Report

Executive Summary

Does payment security matter?

Ask yourself a simple question: would you be more likely or less likely to do business with a company that has been the victim of a data breach? Few of us would say more likely. Payment card security matters.

And the penalties for taking inadequate precautions are about to get worse for many organizations. Any company that does business in the EU will soon be subject to the new General Data Protection Regulation (GDPR). This includes provision for fines for failing to protect personal information – which includes payment card data[1] – of up to €20M or 4% of turnover, whichever's greater[2].

Despite the dangers, our research shows that while PCI DSS compliance is improving, even among the companies that pass validation, nearly half fall out of compliance within a year – and many much sooner.

Are you taking payment security seriously enough?

What is PCI DSS?

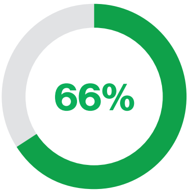
The Payment Card Industry Data Security Standard (PCI DSS) was set up by the leading card brands to help businesses that take card payments reduce fraud. While it's focused on protecting card data, it's built on solid security principles that apply to all kinds of data. It covers vital topics like retention policies, encryption, physical security, authentication and access control.

Find out more: PCISecurityStandards.org

Trust matters. Companies spend millions on loyalty programs, but just because customers have your plastic card doesn't mean that they're loyal. A better test of that is how they'd answer the question, "Would you recommend us to a friend or colleague?"

While many companies that have suffered a breach have seen sales recover to pre-breach levels, how much better could they have been doing if they hadn't been breached?

As well as the damage to their revenues, there are all the costs of remediation – including charges from the card issuers for the costs of replacing cards and identity theft protection. But perhaps even more importantly, while customers may ebb back, will they ever be as loyal as they once were?



say they would be unlikely to do business with an organization that experienced a breach where their financial and sensitive information was stolen[3].

Customers are getting more data savvy.

As we move further into the digital age, when a negative review can be shared around the globe in seconds, it's ever more important to maintain trust. Imagine your local hardware store has suffered a breach and lost payment card data. You might, reluctantly, go back to it the next time you need some paint because it's just down the street. But if it launched a new product line that let you control your heating and lighting from an app, would you trust it[4]? What about if it launched a new loyalty app that rewarded you with money off – would you sign up if it meant sharing your location data?

We're increasingly asking customers to trust us with more of their personal data. If we can't show that we're looking after their payment information, then we shouldn't be surprised if they say no[5].

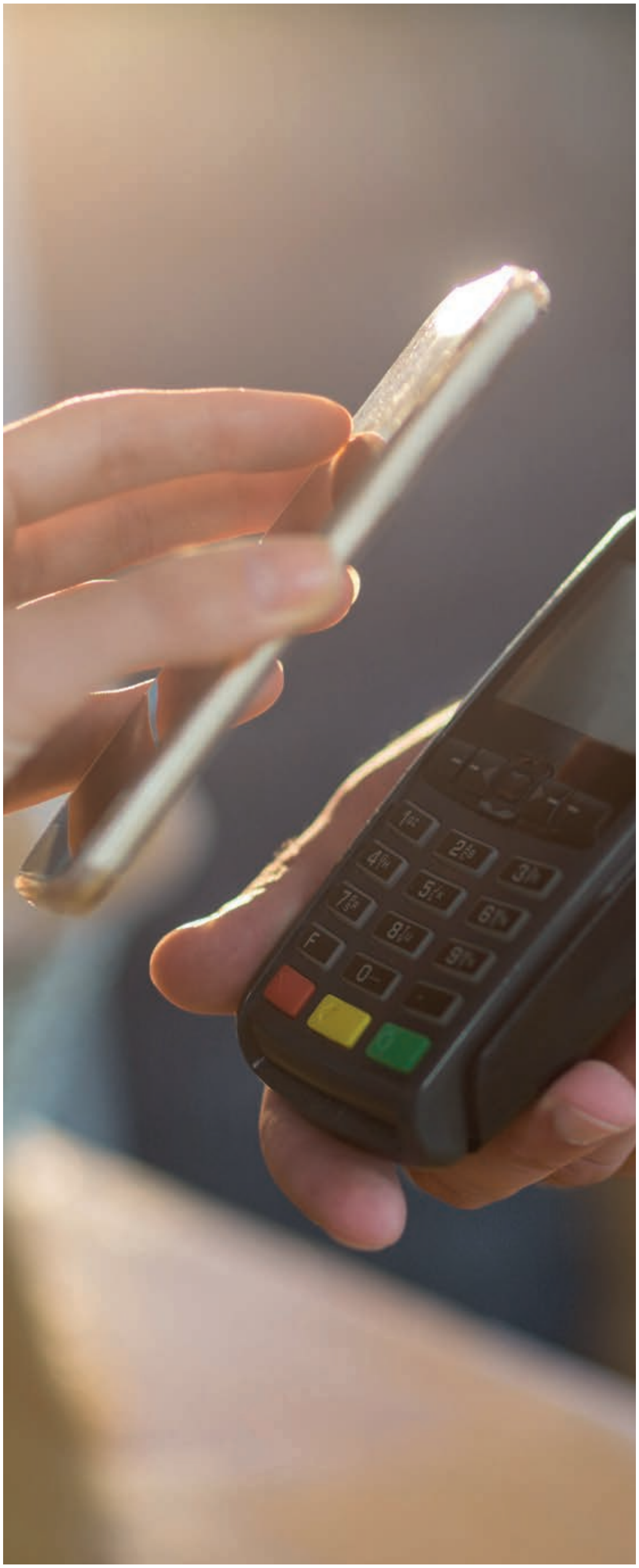
> A brand isn't what the owner tells people it is, it's what consumers tell others it is.

The goalposts keep moving.

How would your current defenses compare with what you had in place five years ago? Like most companies you've probably made great strides at improving your security in recent years.

Unfortunately, the attackers have also upped their game. Companies are locked in an escalating battle with increasingly well-organized and well-resourced cybercriminals.

Many data breaches now occur not because the company hasn't attempted to put defenses in place, but either because those measures weren't effective, or they weren't resilient enough to survive changes in the environment. Cybercriminals only need to find one weakness on one day.



The good news is that more companies passed their annual assessment of PCI DSS compliance – the global standard for companies that store, process or transmit card data – at the first attempt in 2016.

For the first time, more than half (55.4%) of companies we assessed were fully compliant at interim validation, compared to 48.4% in 2015. But that means that nearly half of stores, hotels, restaurants, practices and other businesses that take card payments are still failing to maintain compliance from year to year.

> Of all the payment card data breaches that Verizon has investigated between 2010 and 2016 – nearly 300 – not a single organization was fully PCI DSS compliant at the time of the breach.

Compliance versus security

Organizations that have implemented standards such as PCI DSS through dedicated security compliance programs tend to lose focus once initial compliance is achieved – this can leave them susceptible to data breaches. All too often, companies operate under the false assumption that being compliant means they're secure. It doesn't.

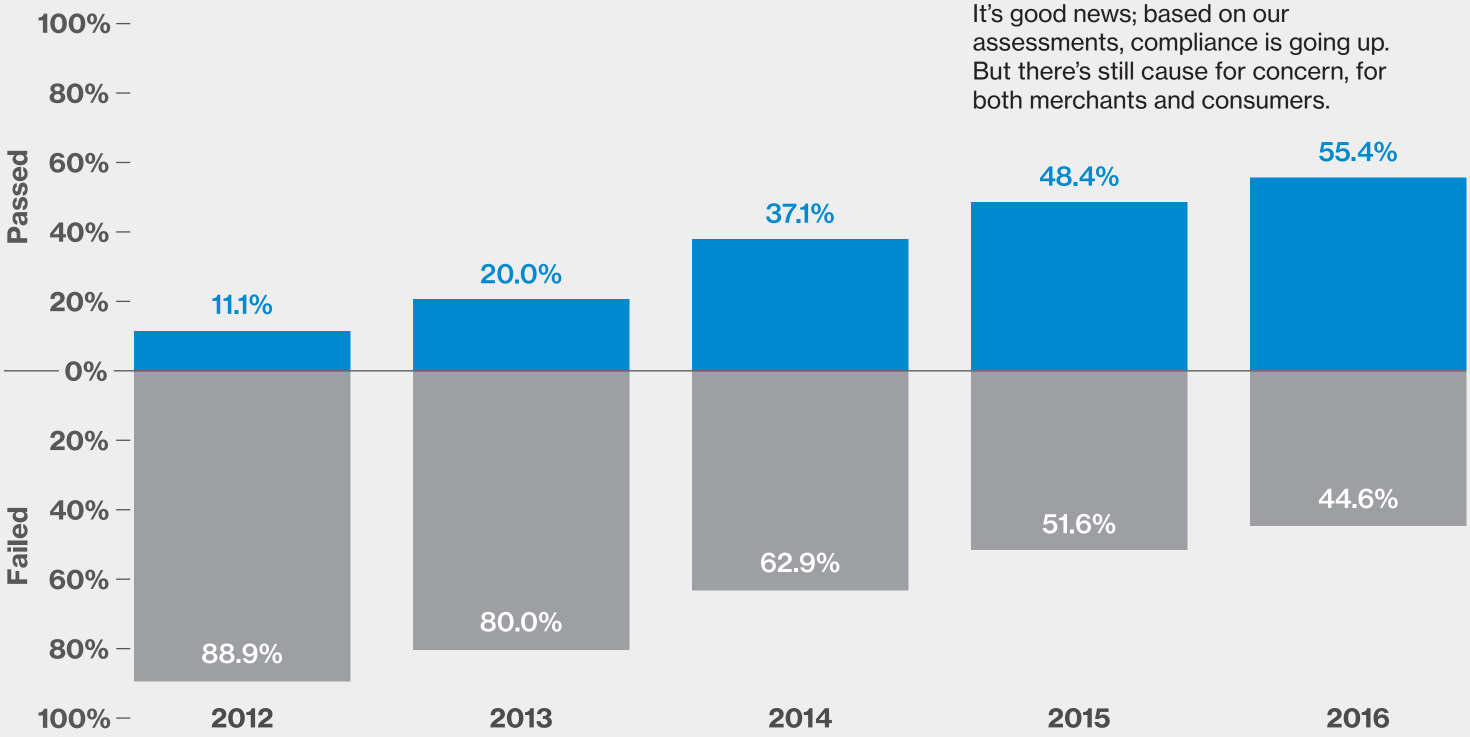
Passing validation doesn't mean that your systems are secure, just that no evidence of non-compliance was found during the assessment period – typically a week or two. But your security is probably tested every day.

> Organizations that make control sustainability and resilience part of their larger security program have a significant head start over those that focus solely on achieving PCI DSS compliance.

Consider this example: an organization has a well-segmented network. It keeps cardholder data separate from other types of data and only gives access to it on a "need-to-know" basis – a fundamental security practice that every company should follow. But the organization doesn't have a process in place to ensure that this segmentation remains intact after changes to the environment – such as adding a new branch, installing a new Wi-Fi router or replacing a business partner. A control is in place, but it isn't resilient.

Full compliance continues its upward progression.

It's good news; based on our assessments, compliance is going up. But there's still cause for concern, for both merchants and consumers.



While the number of organizations maintaining compliance increased, the control gap – the average percentage of controls which companies failing an interim audit did not have in place – widened. In 2015, companies failing their interim assessment had an average of 12.4% of controls not in place (6.8% across all companies). In the 2016 dataset this went up to 13.0% (5.8%).

These aren't just a few obscure, niggling rules. Many of the security controls that weren't in place cover fundamental security principles with broad applicability, and their absence could be material to the likelihood of suffering a data breach.

When a breach occurs, organizations often focus on investigating the failure of entry-point controls. They rarely dig into underlying failures in risk management, control lifecycle and effective control management.

For a control system to be effective, controls must be resource-efficient and budget-friendly, and able to react to changing business priorities and threats.

Control effectiveness

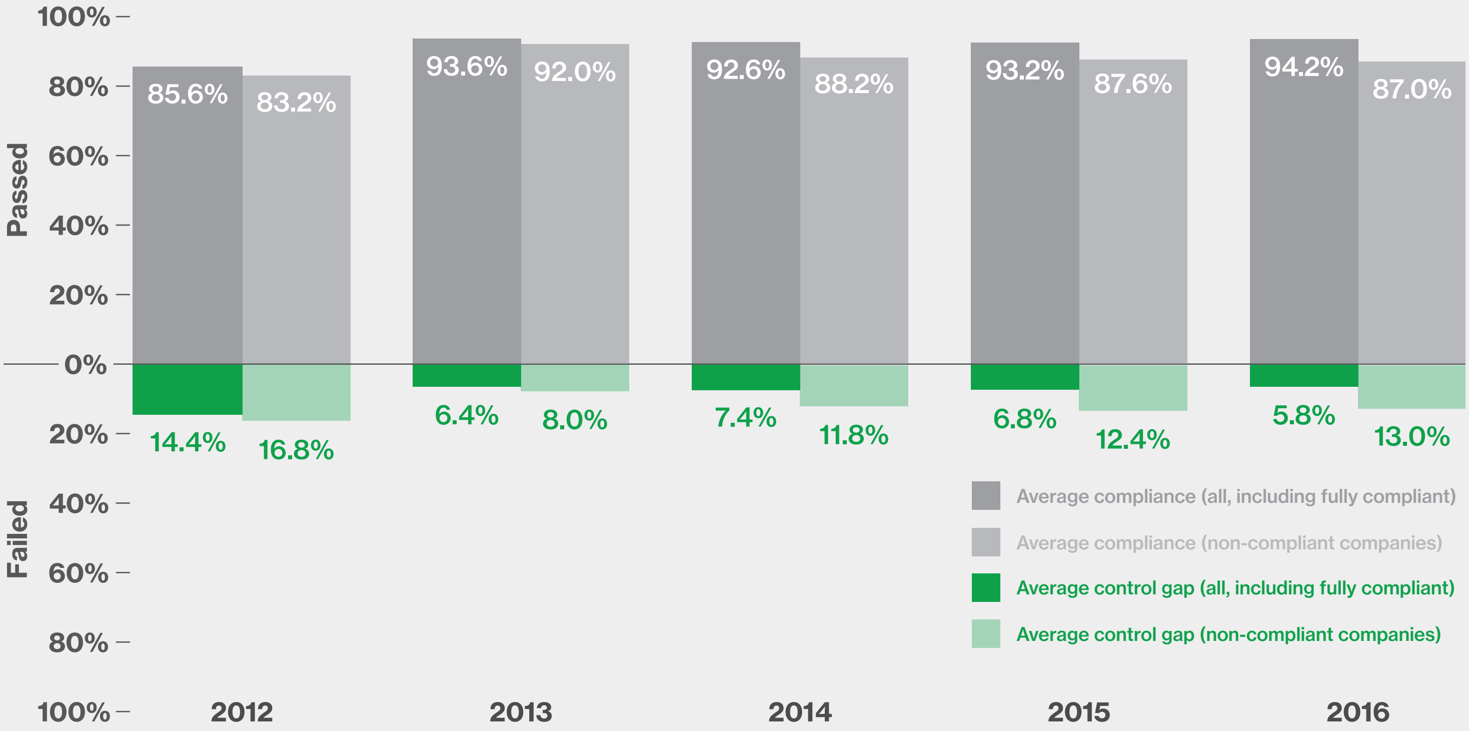
In a PCI DSS context, control effectiveness requires procedures to promote understanding of risk exposure, putting controls in place to address those risks, and effectively pursuing the cardholder data protection objectives. These include effective and efficient processes, reliable data protection, and compliance with policies, regulations and applicable laws.

To be effective, controls must be:

- Fit for purpose – capable of mitigating the vulnerabilities they are designed to prevent. Controls are seldom 100% effective, but they should reduce the risk to an acceptable level.
- Resilient – able to withstand changes to the environment. The control – both technology and process – shouldn't be made ineffective as the environment evolves.

A control that passes just the first requirement may be enough to pass a compliance validation, but it would not be sufficient to truly protect the company from the growing onslaught of increasingly sophisticated attacks. And what good is that?

But the control gap has widened.



Over the past five years we've analyzed PCI DSS compliance, the proportion of companies achieving 100% has gone up almost five-fold. Despite this general improvement, the control gap of companies failing their interim assessment has actually grown worse. Looking at it Requirement by Requirement, five out of six of the worst performers are the same now as they were in 2012.

This is not because companies aren't trying to improve their security. Often compliance and security failures are not down to controls not existing, but them being ineffective. There are two main causes of this.

- Inherent risk: controls that aren't effective, or which lose their effectiveness over time.
- Lack of resilience: controls that are not able to resist or recover from change.

The 2017 Payment Security Report (see next page) looks at why security controls fail, and how to build more effective and, crucially, more sustainable security programs. The advice in this report can not only help you simplify complying with PCI DSS, but also improve how you protect all kinds of data.

Looking back to 2010 when we first published a report on payment security, many things have changed. Back then few people had used their smartphone to make a payment and cybercriminals had access to far fewer resources than they do now.

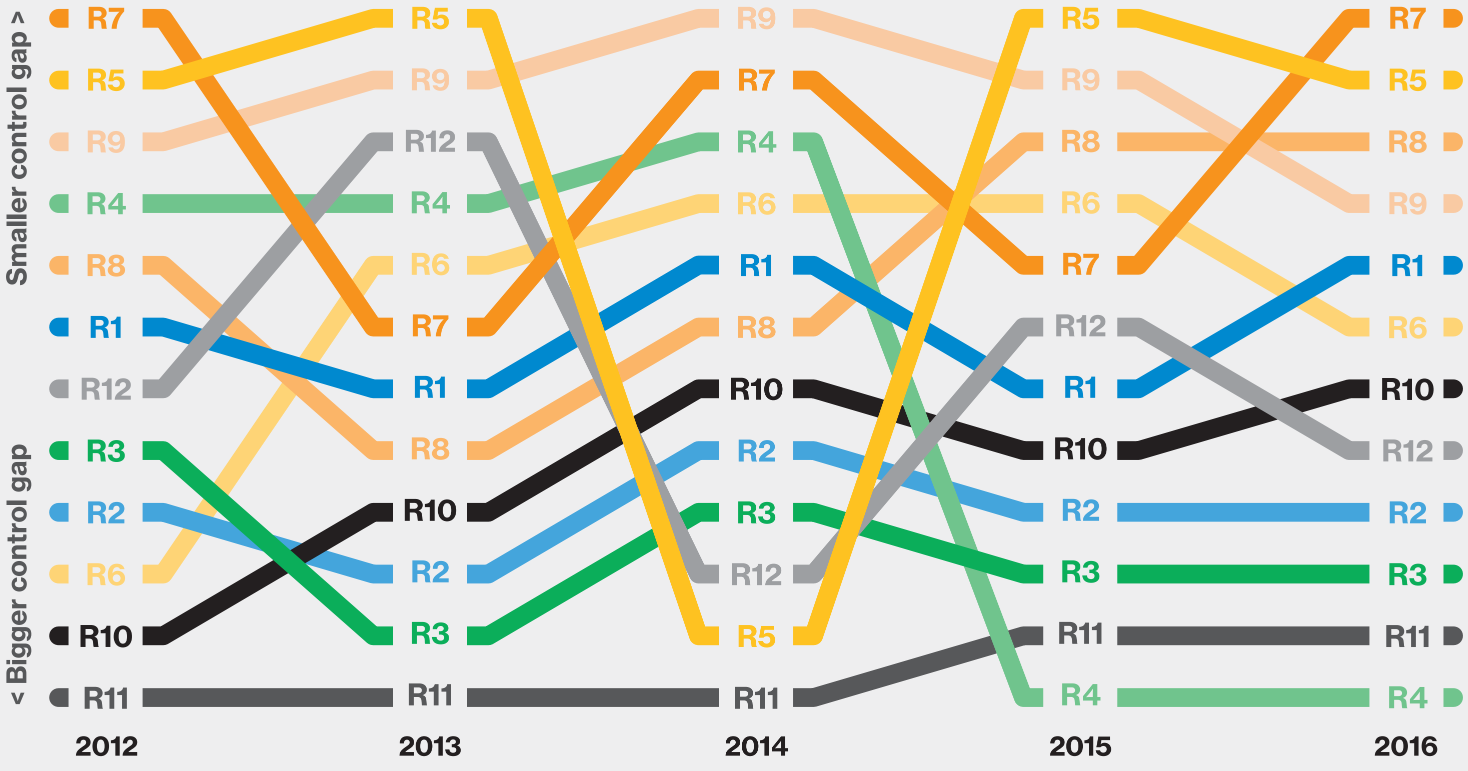
But for all the things that have changed, many things have stayed – disappointingly – similar.

One of these is the difficulty that organizations have complying with Requirement 11 of the PCI DSS [Regularly test security systems and processes]. Every year it has placed eleventh or twelfth out of 12. This is true for both full compliance (the percentage of companies having all the expected controls in place) and – as the diagram below shows – the control gap (the average percentage of those controls not in place).

Which elements of Requirement 11 do companies struggle with the most? What patterns do we see across regions and vertical sectors?

The answers to these and many more questions about PCI DSS compliance are in our 2017 Payment Security Report. If your organization processes mobile or card payments, this report is an important read.

We see the same problems time and time again.



Verizon 2017 Payment Security Report

VerizonEnterprise.com/PaymentSecurity

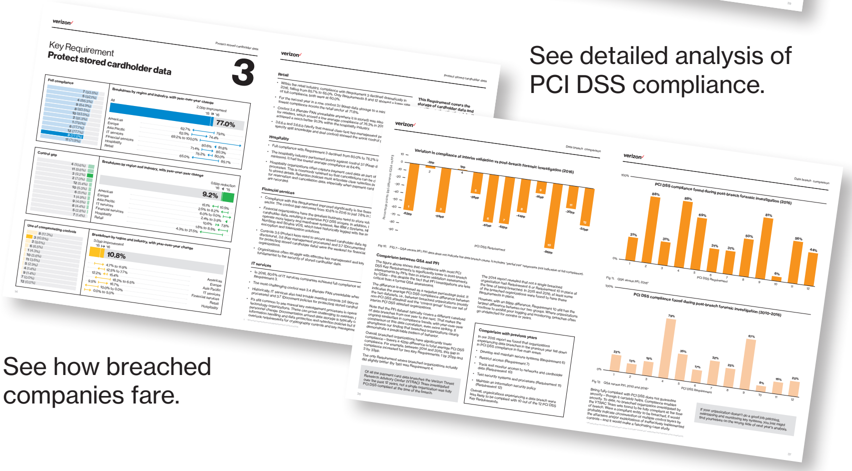
Main report

This report delves into the detail of payment security and specifically PCI DSS compliance. It is the only major industry publication based on data from real compliance validation assessments, conducted worldwide by Verizon. The inclusion of insights on companies suffering payment data breaches from our Data Breach Investigations Report makes it a unique resource for compliance professionals.

2017 Payment Security Report
Revealing the challenges in sustaining payment card security.
verizon

Find out how to build an effective control environment.

Learn about control resilience and sustainability.



See detailed analysis of PCI DSS compliance.

See how breached companies fare.

Infographics

Why payment security is important
45%
verizon
6%
What's happening in payment security?
Read the 2017 Payment Security Report

Get a snapshot of compliance.

See a breakdown of compliance challenges by industry.

References

1. Worldwide annual turnover of the business for the preceding financial year
2. To the extent that it meets the definition of personally identifiable data as defined in the GDPR
3. Gemalto, Customer Loyalty Study, 2016
4. EY, The Data Revolt—EY survey reveals consumers are not willing to share data, Herman Heyns (Partner, Big Data and Analytics)
5. As mentioned in Harvard Business Review, Customer Data: Designing for Transparency and Trust, Timothy Morey, Theodore “Theo” Forbath and Allison Schoop, May 2015

VerizonEnterprise.com