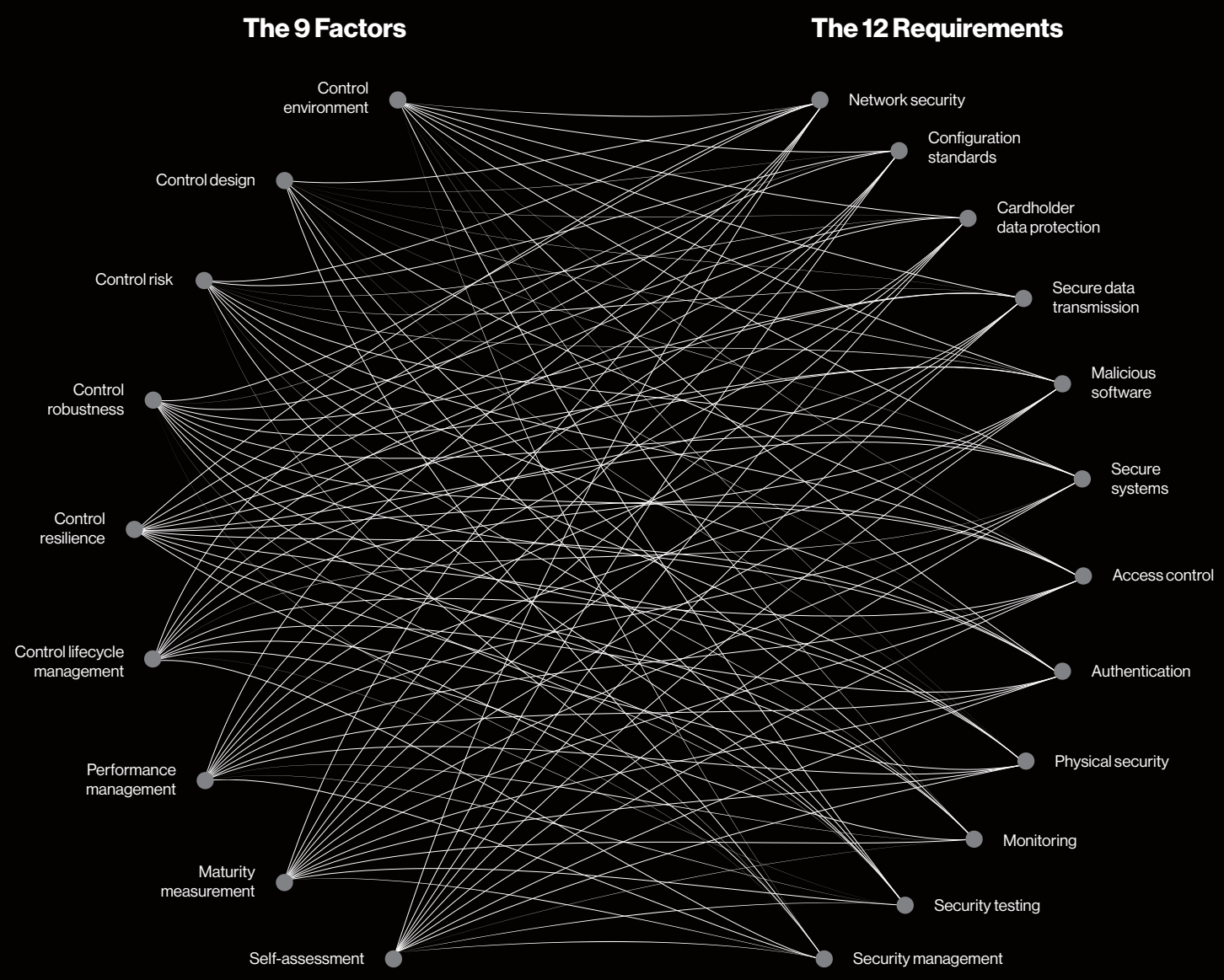
Executive summary

2018 Payment Security Report



verizon

The stakes just got higher

Not since Sarbanes Oxley (SOX) has compliance had so much media coverage. And not just the tech press. It's featured in all the heavyweight business titles, such as The Wall Street Journal and Financial Times.

The General Data Protection Regulation (GDPR) is a European Union (EU) law, but has had a global impact. It's been called the first of many data protection laws for the 21st Century. California has already beefed up its laws – other states and countries are likely to follow.

This year, Verizon has published its seventh report on payment card security and compliance with the Payment Card Industry Data Security Standard (PCI DSS). As well as a deep-dive into the specifics of what organizations find challenging about PCI DSS, it shares the lessons learned from decades of dealing with compliance, and more broadly building a sustainable security environment.

This makes the 2018 Payment Security Report vital reading not just for those tasked with PCI DSS compliance, but anybody responsible for data security or compliance with any security standard, be it GDPR, HIPAA, FISMA, all of them or something else.

About two thirds of organizations (65%) followed at least one other industry standard framework in addition to PCI DSS. Just under half (47%) said they were taking a unified approach to meet the requirements of multiple compliance standards.

The need to improve

The threat of massive penalties clearly focuses attention on compliance, but should not be the primary motivation for a compliance program. This can lead to a "teaching to the test" approach, rather than striving to achieve true data protection.

> Nearly half (47.5%) of the organizations Verizon assessed for interim PCI DSS compliance validation had not maintained all DSS controls.

As a PCI assessor, you see many organizations in various states of compliance maturity. You see some that are quite clearly out to play the system and do the bare minimum needed to comply. You see some that have gone beyond seeing compliance as an annual burden, something that has to be endured, to understanding the importance of not just passing the test but using the compliance framework to genuinely improve the cyber defenses of the company.

> Less than one in five organizations (18%) measure their DSS controls across their entire environment more frequently than the DSS requires[1].

Some dismiss compliance as a checkbox exercise. And that criticism can be valid, but it's not a reflection on the standard, more the company's approach to compliance. There's an obvious parallel with an exam. All a compliance assessment proves is that on the day, you'd done enough. The assessor wasn't able to find sufficient evidence that you hadn't met the grade.

But actually, compliance is more like a job interview than an exam. You might say all the right things on the day and get the job, but if your skills and experience aren't what you say they are, the chances are that you'll get found out pretty quickly.

> As we said in the 2015 report, being compliant doesn't mean that you are secure, but being found not compliant is a pretty strong signal that you are vulnerable[2].

And this matters. Imagine that the new hire was a surgeon about to operate on you. You'd hope that not only had they done enough to pass their exams, but that they'd also learnt the stuff that wasn't on the test. And furthermore, that they'd continued their development to learn about the new technologies and best-practices that had emerged since they put HB pencil to paper.

Upward trend in compliance over

While PCI DSS compliance has been going up year on year, our observations in the field gave us an early warning that this positive trend could be coming to an end. In fact, the drop is probably a little bit less than we expected, with full compliance dropping just under 3 percentage points (pp) to 52.5%.

What's more concerning is that the control gap, the average volume of individual controls failed – effectively a measure of "how badly" companies failed – went up to 16.4%. This is almost the level we saw back in 2012 when familiarity with PCI DSS was much lower, and full compliance was just 11.1%.

Full compliance by year

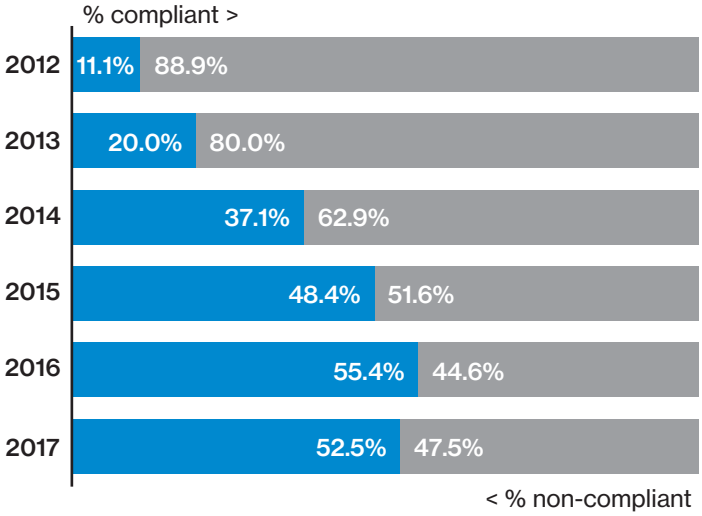


Figure 1. Full compliance at interim assessment by year

Control gap (non-compliant companies)

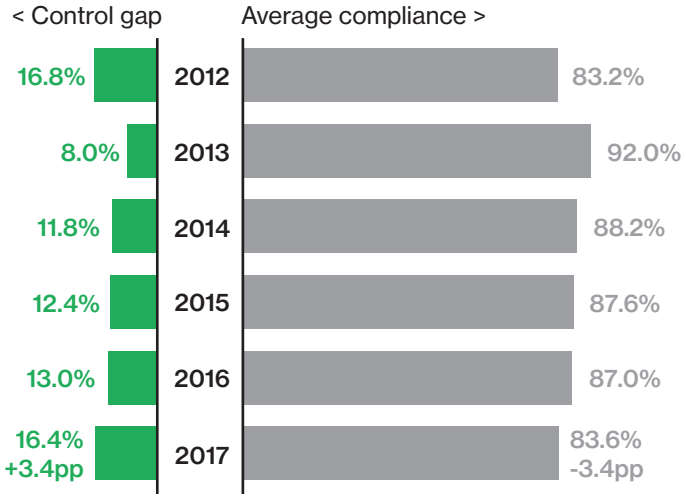


Figure 2. Overview of control gap at interim assessment, 2012–2017

Security standards are rarely comprehensive

It's important to remember that security standards are a set of minimum standards, and rarely, if ever, comprehensive.

You can only achieve real risk reduction by building a program that addresses all aspects of creating a secure environment. Putting in place a control that just meets the standard, assuming that it will retain effectiveness despite changes, and banking on it always being followed brings to mind a famous saying:

> To keep doing what you're doing and expecting different results is the definition of insanity.

The 2018 Payment Security Report is more than an analysis of compliance with PCI DSS – though it has lots of interesting stuff to say about that. It's a thorough examination of what makes a security program not just compliant, but effective and robust, able to stay effective as things inevitably change. It encapsulates decades of learnings built up from thousands of security assessments.

> Common program management pitfalls to avoid:
>
> - Looking only at the financial impacts of compliance
> - Taking a reactive approach to compliance performance management
> - Treating security control performance management as a checkbox to be ticked in order to pass an annual compliance assessment
> - Under-qualified staff or resources spread too thin, with not enough time prioritized for security-related tasks
> - Organizational silos, with the CISO and security team acting with weak or non-existent connections to other departments
> - Poor or non-existent support from executive management

Addressing sustainability

Organizations are coming to terms with being measured on 400-plus test procedures for their annual PCI DSS compliance validation, but they seem to fail in establishing continuous monitoring processes to support sustainable compliance performance.

> Organizations that demonstrate an inability to keep PCI DSS controls in place often lack insight into how control systems should be designed and function.

Based on our interviews with organizations worldwide, half (50%) of organizations manage their PCI DSS compliance programs as a standalone project and not as part of a broader data protection program initiative.

100% compliance isn't 100% secure

The PCI DSS evaluates aspects of the control environment, such as: policies, user training and awareness, risk assessment and network security. However, the PCI DSS does not directly address organizations' capability for assessing data protection governance, oversight, and commitment toward competence. Organizations need to take self-ownership of their responsibility to develop data protection governance capabilities.

> In terms of compliance reporting, two fifths (40%) only measure their PCI compliance annually for compliance validation purposes. Less than a quarter (19%) measure and report their PCI DSS compliance monthly.

The 9 Factors of Control Effectiveness and Sustainability

To help you build an effective compliance program that helps to improve security and reduce risk year-round, we've developed the 9 Factors model, shown below.

Figure 3. A relational model of the 9 Factors. Factor 1 is the core from which the other factors emanate. After achieving the objectives of the preceding factors, the final outcome is the ability to self-assess, the output of which can then be used to improve all the factors.

Factor 1. Control environment

The simple act of documenting the control environment is an important step toward more sustainable compliance. Once you have listed all the components, each can then be analyzed, and risk assessment carried out to evaluate the impact on payment security.

> Control failures do not happen in isolation; they often occur because the environment contributes toward weaknesses.

Any IT environment, payment card security ones included, can be susceptible to deficiencies in controls, leading to chain reactions that eventually result in control failures and vulnerabilities. While most PCI DSS control failures are detectable and avoidable, poor management of the control environment and control deficiencies can leave you unnecessarily prone.

> An effective control environment is one in which knowledgeable and mindful people understand their responsibilities, the limits of their authority are clear, and they are committed to doing what is right in the correct way.

Many organizations are overly dependent on compliance assessments performed by external assessors, such as PCI QSAs (qualified security assessors). This reliance on periodical reviews – like an annual PCI DSS compliance assessment – can leave organizations exposed to weaknesses. Not reviewing controls throughout the year can lead to failure to react to changes in the control environment quickly enough to maintain security. Organizations need to develop a program of ongoing internal reviews that evaluates control effectiveness.

Factor 2. Control design

Control environments differ substantially from one organization to the next. Implementing PCI DSS controls "out of the box" and expecting them to perform flawlessly usually isn't effective and, very likely, isn't sustainable unless the security controls include tailor-made documentation and specifications for operating within the specific environment.

It's not prudent to assume that controls will be sustainable and meet control objectives without first carefully evaluating how their design meets operational requirements.

We find that it's not that organizations are oblivious to these macro constraints; typically they are aware but suffer from over confidence surrounding them.

Some important questions to ask are:

- Can the people and technologies tasked with implementing and maintaining required security controls actually do so?
- Do they have the resources they need?
- Are there other demands placed on them that reduce their capacity and limit the efficacy of the control?
- Was the control designed in a way that ignores the day-to-day realities of an environment?
- Does the control consider how legacy software or hardware might behave?
- Does the control assume a full workforce – would it fail if some staff left or were let go?
- Does the control design follow best practice that assumes skills, software or hardware that are not present in the actual environment?

Factor 3. Control risk

Control risk deals with the tendency of controls to lose their effectiveness over time. This can be a result of deficiencies in initial design or operational failure. It can leave the assets the control was intended to protect exposed and the company vulnerable. Poorly designed internal controls and ineffective management of the control environment can increase the level of risk – i.e., the company's internal controls may fail and are not able to detect that failure.

Research by Carnegie Mellon University lists four key areas of weakness[1]:

- Actions of people: Action, or lack of action, either deliberate or accidental, that impact cybersecurity
- Systems and technology failures: Failure of hardware, software or information systems
- Failed internal processes: Problems in internal business processes that impact the ability to implement, manage and sustain cybersecurity
- External events: Issues beyond the control of the organization, such as natural disasters, legal issues and dependencies on third parties

Increased awareness about the importance of managing control risk is needed since any control failure can severely handicap an organization's ability to protect cardholder data.

Managing control risks also helps to reduce audit and assessment risks, thereby improving assurance of compliance with PCI DSS requirements. While the measurement of control risk is not explicitly defined as a requirement in the PCI DSS, it's mentioned in its information supplement: "Best Practices for Maintaining PCI DSS Compliance."

PCI DSS Requirement 1
More than four out of five (81.1%) organizations were compliant with Requirement 1 in 2017, a slight increase on 2016 (79.1%).

Two thirds (66.7%) of organizations assessed after a data breach were compliant with Requirement 1. This is a significant improvement over previous years. In fact, there has been consistent improvement in this area since 2010.

It is important to keep system and configuration documentation updated and fully integrate documentation maintenance and management into your change control processes.

PCI DSS Requirement 2
This Requirement addresses the default security settings that many products and services ship with. These can be easily found on the internet, making them next to useless.

Despite this, almost a quarter (23.8%) of the organizations that we assessed failed to maintain compliance with Requirement 2 year-on-year.This was a drop of 5.1pp and an all-time low.

Much of the non-compliance comes down to failures of control robustness, Factor 4. Maintaining robustness requires multiple levels of defense, including individual accountability and effective internal audit.

PCI DSS Requirement 3
PCI DSS Requirement 3 covers things like encrypting cardholder data and deleting it when you no longer need it.

Requirement 3 saw a small increase in compliance in 2017. More than three quarters (77.9%) of organizations were able to demonstrate compliance during their interim report on compliance assessment.

Factor 4. Control robustness

Some organizations' approach to preventing data breaches is to design robust controls: controls that are designed to prevent failure. But this can lead to rigid controls that are difficult to sustain in an environment where the list of threat actors and range of vulnerabilities can vary daily.

> A control environment that can operate according to its design specifications despite challenges is called "robust." When an environment cannot withstand additional pressures, but can deal with them through multiple layers of controls, thereby keeping data protected, then it's called "resilient."

Maintaining robust controls goes beyond maintaining processes that ensure IT components are up to date. It starts with establishing a sound control environment (see Factor 1), strengthening the design, operation and maintenance of security controls (Factor 2), and consistent management of control risk (Factor 3).

Factor 5. Control resilience

Control resilience refers to an organization's ability to design and operate security controls that are able to rapidly recover from disruptive events and to resume operating effectively after being exposed to adverse events, such as operational failures and attacks.

When a resilient security control is impacted, it's able to return to its former state due to fast detection and recovery from disruptive events.

Control resilience brings together the areas of data protection, business continuity, and organizational resilience. This enables continuous control operation and contributes toward keeping the control environment stable. It is distinctly different from control robustness, which is the ability of controls to withstand challenge and disruption.

A robust security control can absorb a significant amount of "damage" before it fails. A robust system is designed to operate the same way throughout changes in the control environment, and any breakdown of a robust system is likely to be a catastrophic failure of control performance.

The risk of such catastrophic failure underscores the need to integrate control resilience into control design and operation objectives.

PCI DSS Requirement 4
This Requirement is designed to protect cardholder data and sensitive authentication data transmitted over unprotected networks, such as the internet, where it is vulnerable to being intercepted.

Compliance with Requirement 4 was 86.9% in 2017. While full compliance went up just 0.6pp year-on-year, the control gap almost halved, dropping 4.5pp to 6.1%. This shows that even the companies that weren't able to fully sustain compliance got a lot closer.

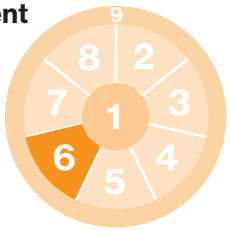
PCI DSS Requirement 5
This Requirement demands that antivirus software not only be in place, but kept up to date and be capable of detecting, removing and protecting against all known types of malware. It also governs the generation of audit logs and making sure scans are performed regularly.

Full compliance fell from 92.1% in 2016 to 87.7%, a drop of 4.4pp. It was still second best (to Requirement 7) the second time in a row.

PCI DSS Requirement 6
Requirement 6 covers the security of applications, including change management. It governs how systems and applications are developed and maintained, whether that's in-house or by third parties.

Compliance with Requirement 6 was largely unchanged this year, dropping just 0.6pp to 77.0%. This put it in the midfield, with seven requirements doing better, and five doing worse. Its control gap, 5.3%, was significantly better than the overall average. This would have been even better if it weren't for organizations in the Americas finding it so challenging – compliance, 65.5%; control gap, 10.9%.

Factor 6. Control lifecycle management



Security control lifecycle management (SCLM) defines a control's journey, from its conception and design, to its eventual retirement.

To sustain compliance, and security, it's essential that organizations understand how each stage of the control lifecycle influences the underlying support processes required, the control's operational efficiency and its effectiveness.

> We introduced the concept of the security control lifecycle as a way to support the development and maintenance of sustainable controls in the 2017 Payment Security Report.

Actively maintaining SCLM for all PCI DSS controls in a control environment offers immediate and long-term benefits to the effectiveness and sustainability of data protection and compliance efforts.

> The integration of SCLM into your compliance program gives you milestones to measure and record the effectiveness of security controls, and a framework to guide decisions about managing their effectiveness as they age and the environment evolves.

Factor 7. Performance management

To improve your data protection performance, you first need to know how you are doing already.

The four key elements of a data protection performance program are:

- Clarifying goals and objectives
- Setting standards
- Measuring and comparison
- Managing deviations

Performance management must be aligned with the strategic goals of an organization. Too often, data protection, security and compliance objectives are not addressed effectively within a corporate strategy. They are overlooked in performance management processes or siloed to particular teams or functions.

In reality, the responsibilities for security or compliance goals should be borne companywide. For many organizations, measuring and improving the actual effectiveness of security controls are seldom part of their program objectives.

> The bottom line is that what gets measured, gets done.

There is significant need to promote the use of tools and procedures to measure data protection and compliance performance.

PCI DSS Requirement 7
Requirement 7 covers access restrictions, a fairly fundamental layer to any security program. And actually, compliance is high, the highest of all 12 Requirements at 88.5%.

But that still means that nearly one in eight companies fail to maintain this most basic of controls. And at 5.7%, it has the 8th best (5th worst) control gap.

With roles constantly changing and applications coming and going, and evolving in-between, making sure that people only have access to the data that they need to do their job can be challenging. For restrictions to be sustainable, it's essential to continuously monitor them.

PCI DSS Requirement 8
This Requirement sets standards for credentials such as passwords and two-factor authentication, particularly for remote access. It helps prevent password cracking and governs how user credentials are protected at the time of use, during transmission, and in storage.

During the past year there was a 7.2pp drop in full compliance, falling to just over three quarters (76.2%).

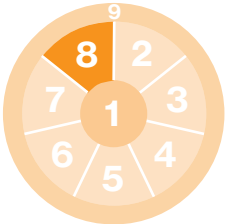
What's worse, the control gap nearly doubled. So it wasn't just that some companies failed to maintain 100%, the average performance of those that missed the mark dropped too.

PCI DSS Requirement 9
One area of control design, Factor 2, that is sometimes overlooked is physical access to data, covered by Requirement 9.

This governs the control of physical access to prevent unauthorized access to systems and data within the DSS scope. It stipulates that organizations must secure media that holds CHD, restrict sharing, and protect POS devices against tampering and substitution.

At 82.8%, a small drop on 2016, Requirement 9 came fourth in terms of full compliance. And this Requirement had the narrowest control gap in 2017, just 4.9%.

Factor 8. Maturity measurement



While current performance is obviously important, organizations should be equally concerned about the long-term development and maturity of their compliance programs.

Many organizations have a wash-rinse-repeat mindset to their data protection programs, focusing on the annual validation exercise rather than year-round protection.

> The PCI DSS still lacks standards for measuring compliance process maturity – it's not alone.

Understanding the maturity of the control environment, and the controls within it, can facilitate a meaningful dialog between all stakeholders about the state of data protection, its effectiveness and sustainability.

The responsibility for cybersecurity shouldn't be the exclusive preserve of the IT function. Building engagement with all the stakeholders can help simplify compliance and drive significant improvements in the organization's defenses every day of the year. It can also help muster the commitment and budget needed to facilitate change and improve performance.

Factor 9. Self-assessment

Developing an in-house self-assessment competency promotes proactive detection of potential issues, rather than waiting for an annual compliance assessment – or a hacker – to bring a problem to light.

This facilitates the re-engineering of controls as required throughout the year, keeping your defenses at a higher level and increasing your chances of passing compliance audits at first go.

Regular internal self-assessment can also improve communication about the overall state of data protection and compliance, and foster closer ties with the business units and other stakeholders. This, in turn, can help bolster confidence in the proficiency – capacity, capability and competency – of the internal compliance team.

PCI DSS Requirement 10
Performance measurement, Factor 7, is inextricably linked with PCI DSS Requirement 10, which covers the tracking and monitoring of access.

The controls within this Requirement can not just help improve security, but can also provide vital information to assist forensic investigation should a breach occur.

That is when performing as intended. Requirement 10 is another regular back marker. This year it came in 10th, with less than three quarters (73.0%) of organizations achieving full compliance.

PCI DSS Requirement 11
Resilience, Factor 5, and testing, Requirement 11, clearly go hand-in-hand. This is a perennial problem for organizations.

Organizations must rescan to verify "high risk" vulnerabilities are resolved, and also after any significant changes.

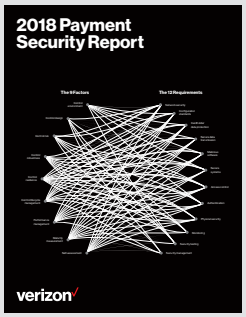
Every year that we have analyzed PCI DSS compliance data, Requirement 11 has come bottom of the pack. This year, full compliance dropped 3.9pp to 68.0%. And it had the largest control gap at 11.9%.

PCI DSS Requirement 12
Managing interval-based requirements (such as daily log reviews, quarterly scanning, firewall reviews, etc.) continues to be a challenge for most organizations.

Full compliance with Requirement 12 (Security management) dropped to 69.7% in 2017. Companies only fared worse at Requirement 11 (Test security systems and processes).

To help improve your performance with these recurring compliance tasks, we have included an updated PCI DSS compliance calendar in this year's Payment Security Report. Following the recommendations of this chart could help improve your compliance sustainability and overall security.

The 2018 Verizon Payment Security Report



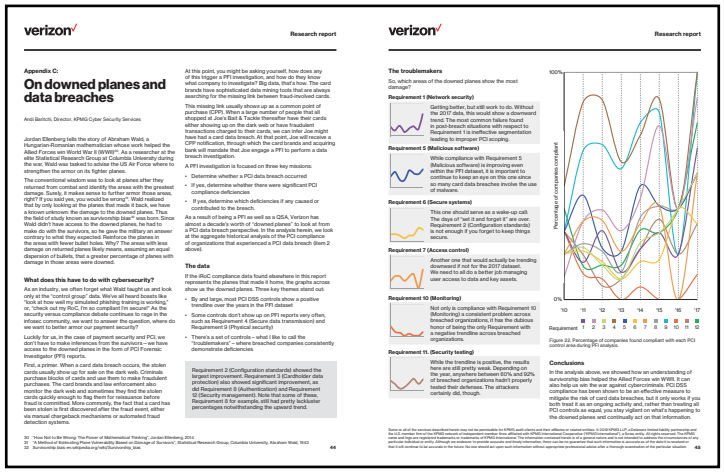
- An unparalleled look into PCI DSS compliance
- Unique analysis of compliance at post-breach organizations
- Expert guidance on building and improving your compliance program
- Insight into improving compliance sustainability

verizonenterprise.com/paymentsecurity

Now in its seventh edition, the Payment Security Report gives unparalleled insight into where companies struggle with maintaining compliance with PCI DSS. The database we've gathered over the years of writing the report is unmatched. This enables us to show the trends, and the interesting changes each year. It also lets us delve deeper, looking at where there are patterns by region or vertical sector. This detailed information could help you hone your own security programs and increase your chances of achieving 100% compliance first time around.

But the report contains so much more.

Learn from companies that have been breached


verizon Research report

Appendix C:

On downed planes and data breaches

Andi Barlotti, Director, KPMG Cyber Security Services

Jordan Ellenberg tells the story of Abraham Wald, a Hungarian-Romanian mathematician whose work helped the Allied Forces win World War II (WWII)[31]. As a researcher at the elite Statistical Research Group at Columbia University during the war, Wald was tasked to advise the US Air Force where to strengthen the armor on its fighter planes.

The conventional wisdom was to look at planes after they returned from combat and identify the areas with the greatest damage. Surely, it makes sense to further armor those areas, right? Wald surprised officials by suggesting the reinforcing that by only looking at the planes that made it back, we have a known unknown: the damage to the downed planes. Thus the field of study known as survivorship bias[32] was born. Since Wald didn't have access to the downed planes, he had to make do with the survivors, so he gave the military an answer contrary to what they expected. Reinforce the planes in the areas with fewer bullet holes. Why? The areas with less damage on returned planes likely means, assuming an equal dispersion of bullets, that a greater percentage of planes with damage in those areas were downed.

What does this have to do with cybersecurity?

As an industry, we often forget what Wald taught us and look only at the "control group" data. We've all heard boasts like "look at how well my simulated phishing training is working" or, "check out my RoC. I'm so compliant I'm secure!" As the security versus compliance debate continues to rage in the infosec community, we want to answer the question, where do we want to better armor our payment security?

Luckily for us, in the case of payment security and PCI, we don't have to make inferences from the survivors – we have access to the downed planes in the form of PCI Forensic Investigator (PFI) reports.

First, a primer. When a card data breach occurs, the stolen cards usually show up for sale on the dark web. Criminals purchase blocks of cards and use them to make fraudulent purchases. The card brands and law enforcement also monitor the dark web and sometimes they find the stolen cards quickly enough to flag them for reissuance before fraud is committed. More commonly, the fact that a card has been stolen is first discovered after the fraud event, either via manual chargeback mechanisms or automated fraud detection systems.

At this point, you might be asking yourself, how does any of this trigger a PFI investigation, and how do they know what company to investigate? Big data, that's how. The card brands have sophisticated data mining tools that are always searching for the missing link between fraud-involved cards.

This missing link usually shows up as a common point of purchase (CPP). When a large number of people that all shopped at Joe's Bait & Tackle thereafter have their cards either showing up on the dark web or have fraudulent transactions charged to their cards, we can infer Joe might have had a card data breach. At that point, Joe will receive a CPP notification, through which the card brands and acquiring bank will mandate that Joe engage a PFI to perform a data breach investigation.

A PFI investigation is focused on three key missions:

- Determine whether a PCI data breach occurred
- If yes, determine whether there were significant PCI compliance deficiencies
- If yes, determine which deficiencies if any caused or contributed to the breach.

As a result of being a PFI as well as a QSA, Verizon has almost a decade's worth of "downed planes" to look at from a PCI data breach perspective. In the analysis herein, we look at the aggregate historical analysis of the PCI compliance of organizations that experienced a PCI data breach (item 2 above).

The data

If the RoC compliance data found elsewhere in this report represents the planes that made it home, the graphs across show us the downed planes. Three key themes stand out:

- By and large, most PCI DSS controls show a positive trendline over the years in the PFI dataset
- Some controls don't show up on PFI reports very often, such as Requirement 4 (Secure data transmission) and Requirement 9 (Physical security)
- There's a set of controls – what I like to call the "troublemakers" – where breached companies consistently demonstrate deficiencies

Requirement 2 (Configuration standards) showed the largest improvement. Requirement 3 (Cardholder data protection) also showed significant improvement, as did Requirement 8 (Authentication) and Requirement 12 (Security management). With that some of these, Requirement 6 for example, still had pretty lackluster percentages notwithstanding the upward trend.

31 "How Not to Be Wrong: The Power of Mathematical Thinking", Jordan Ellenberg, 2014
32 "A Method of Estimating Plane Vulnerability Based on Damage of Survivors", Statistical Research Group, Columbia University, Abraham Wald, 1943
32 Survivorship bias en.wikipedia.org/wiki/Survivorship_bias

44

verizon Research report

The troublemakers

So, which areas of the downed planes show the most damage?

Requirement 1 (Network security)

Getting better, but still work to do. Without the 2017 data, this would show a downward trend. The most common failure found in post-breach situations with respect to Requirement 1 is ineffective segmentation leading to improper PCI scoping.

Requirement 5 (Malicious software)

While compliance with Requirement 5 (Malicious software) is improving even faster than the rest of the pack, it is important to continue to keep a hope on this one since so many card data breaches involve the use of malware.

Requirement 6 (Secure systems)

This one should serve as a wake-up call. The days of "set it and forget it" are over. Requirement 2 (Configuration standards) is not enough if you forget to keep things secure.

Requirement 7 (Access control)

Another one that would actually be trending downward if not for the 2017 dataset. We need to all do a better job managing user access to data and key assets.

Requirement 10 (Monitoring)

Not only is compliance with Requirement 10 (Monitoring) a consistent problem across breached organizations, it has the dubious honor of being the only Requirement with a negative trendline across breached organizations.

Requirement 11. (Security testing)

While the trendline is positive, the results here are still pretty weak. Depending on the year, anywhere between 60% and 92% of breached organizations hadn't properly tested their defenses. The attackers certainly did, though.

Figure 23. Percentage of companies found compliant with each PCI control area during PFI analysis.

Conclusions

In the analysis above, we showed how an understanding of survivorship bias helped the Allied Forces win WWII. It can also help us win the war against cybercriminals. PCI DSS compliance has been shown to be an effective measure to mitigate the risk of card data breaches, but it only works if you both treat it as an ongoing activity and, rather than treating all PCI controls as equal, you stay vigilant on what's happening to the downed planes and continually act on that information.

Some or all of the services described herein may not be permissible for KPMG audit clients and their affiliates or related entities. © 2018 KPMG LLP, a Delaware limited liability partnership and the U.S. member firm of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved. The KPMG name, logo and "cutting-edge, high-quality, value-added professional services" are trademarks used under license by the independent member firms of the KPMG network. No member firm is the agent of, or liable for the particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should act upon such information without appropriate professional advice after a thorough examination of the particular situation.

48

As the security versus compliance debate continues, the most pressing question for most organizations is, "Where should we strengthen our armor to improve payment security?"

While a researcher at the elite Statistical Research Group at Columbia University during the war, Abraham Wald was tasked to advise the US Air Force where to strengthen the armor on its fighter planes.

Wald surprised officials by suggesting reinforcing planes where they found fewer bullet holes. He realized that by only looking at the planes that made it back, there was a known unknown: the damage to the downed planes. And assuming an even spread of bullets, areas on returned planes with less damage would likely show more damage on the planes that were downed. This insight led to what is now known as survivorship bias.

The Payment Security Report is unique in looking at both compliance at the time of annual assessment (the planes that came home) and within companies assessed following a data breach (the ones that didn't).

Since 2010, not a single organization that we have assessed following a data breach was fully PCI DSS compliant. See Appendix C of the full report for a detailed analysis of post-breach compliance, including the list of six "Troublemakers."

Verizon Payment Security Report history

2010: Complexity and uncertainty

An exploration of the complexity of PCI security, the growing pains of PCI compliance regulation, and the need to evolve toward a process-driven approach for compliance.

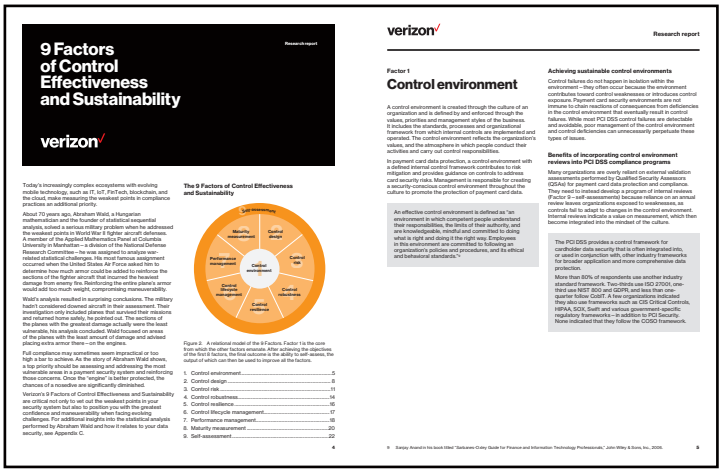
2011: Dealing with evolution

A review of the changing compliance requirements with insights into the importance of sound decision-making, and how organizations can position themselves for success.

2014: Simplifying complexity

A review of the value of compliance and the impact of PCI DSS standard changes, the need for sustainability, how to improve scope reduction and compliance program management.

Get our experts' advice on making security sustainable


9 Factors of Control Effectiveness and Sustainability

Research report

verizon

The 9 Factors of Control Effectiveness and Sustainability

Factor 1

Control environment

Achieving sustainable control environments

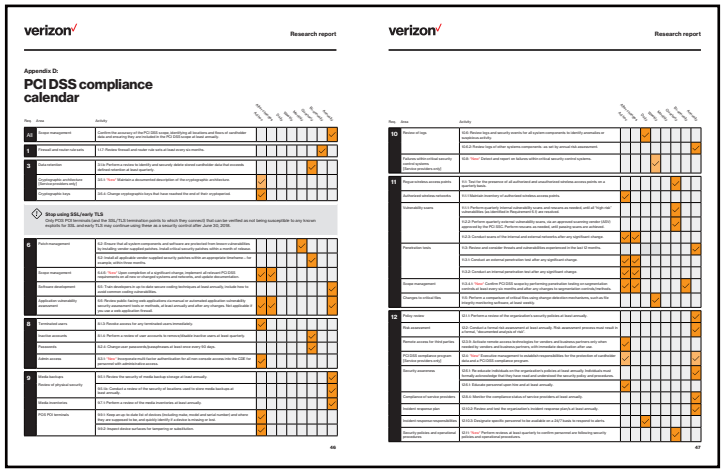
Benefits of incorporating control environment reviews into PCI DSS compliance programs

Our assessors have decades of experience, not just with PCI DSS but most of the major standards. This gives us a unique insight into the good, the bad and the ugly of compliance programs.

The 2018 Payment Security Report is packed with guidance on not just how to pass the test, but how to build the most effective compliance program possible. This includes the 9 Factors model, a look at the benefits of using maturity models and much more.

It can help you build a security environment that is able to adapt to change quickly, make intelligent decisions more rapidly, and turn security and compliance into a competitive advantage.

Plan your ongoing PCI DSS compliance activity


verizon

Research report

Appendix D:

PCI DSS compliance calendar

The PCI DSS compliance calendar (see Appendix D) provides valuable guidance on the regular activities required to comply with PCI DSS. This can help you maintain compliance throughout the year.

Questions? Comments?

We'd love to hear them.

Email us at: paymentsecurityreport@verizon.com

Find out more

For additional resources on this research and to find out more about Verizon's PCI Security compliance services, please visit:

verizonenterprise.com/paymentsecurity

Verizon Payment Security Report history

2015: Achieving sustainability

A focus on improving compliance sustainability, review of scope reduction, and a look at payment security innovation and the need to avoid over-reliance on technology.

2016: Developing proficiency

A look at developing data protection proficiency, the necessary skills and experience, and applying a structured approach to compliance management.

2017: Establishing internal control

A study of the need to establish and maintain an internal control environment and a holistic approach, including security control lifecycle management.

About the cover

The front cover depicts the 12 PCI DSS Key Requirements on the right and each of the 9 Factors for Control Effectiveness and Sustainability on the left. The lines show the numerous relationships between the two. To some, the image may resemble an abstract ball of yarn. That may perhaps be an apt analogy. In a way, if that yarn was a long, continuous length of interlocked fibers resembling a series of interlocked objectives, it represents the tightly woven relationships between the 9 Factors and Key Requirements, which are success factors for achieving an effective and sustainable data protection program.

1. resources.sei.cmu.edu/asset_files/TechnicalNote/2014_004_001_91026.pdf

verizonenterprise.com

© 2018 Verizon. All Rights Reserved. The Verizon name and logo and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. 09/18