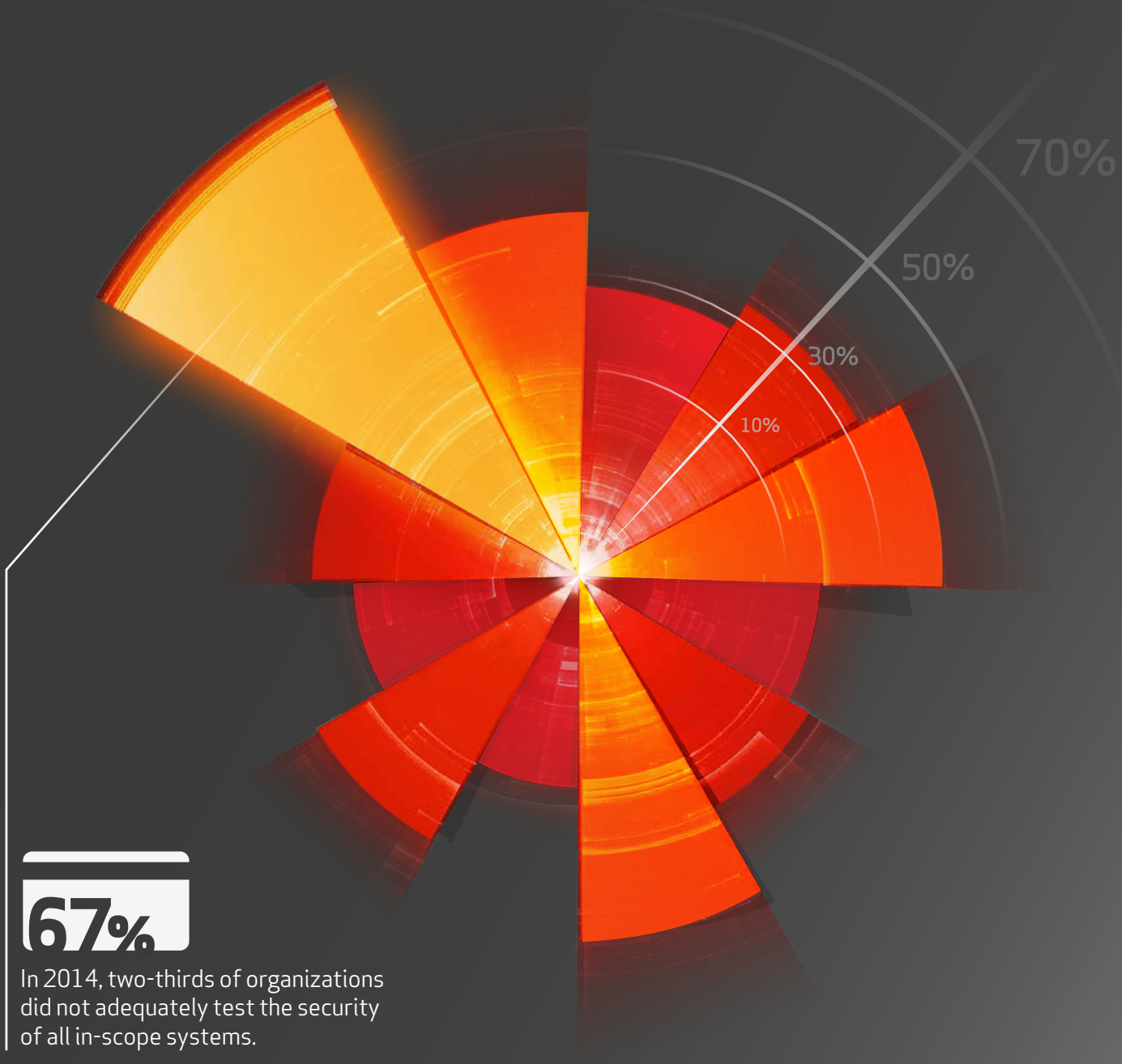
verizon

Verizon 2015

PCI COMPLIANCE REPORT

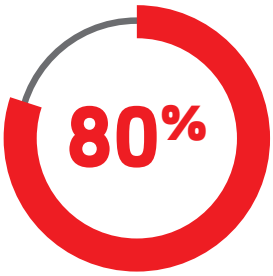
Insight for helping businesses manage risk through payment security.



67%

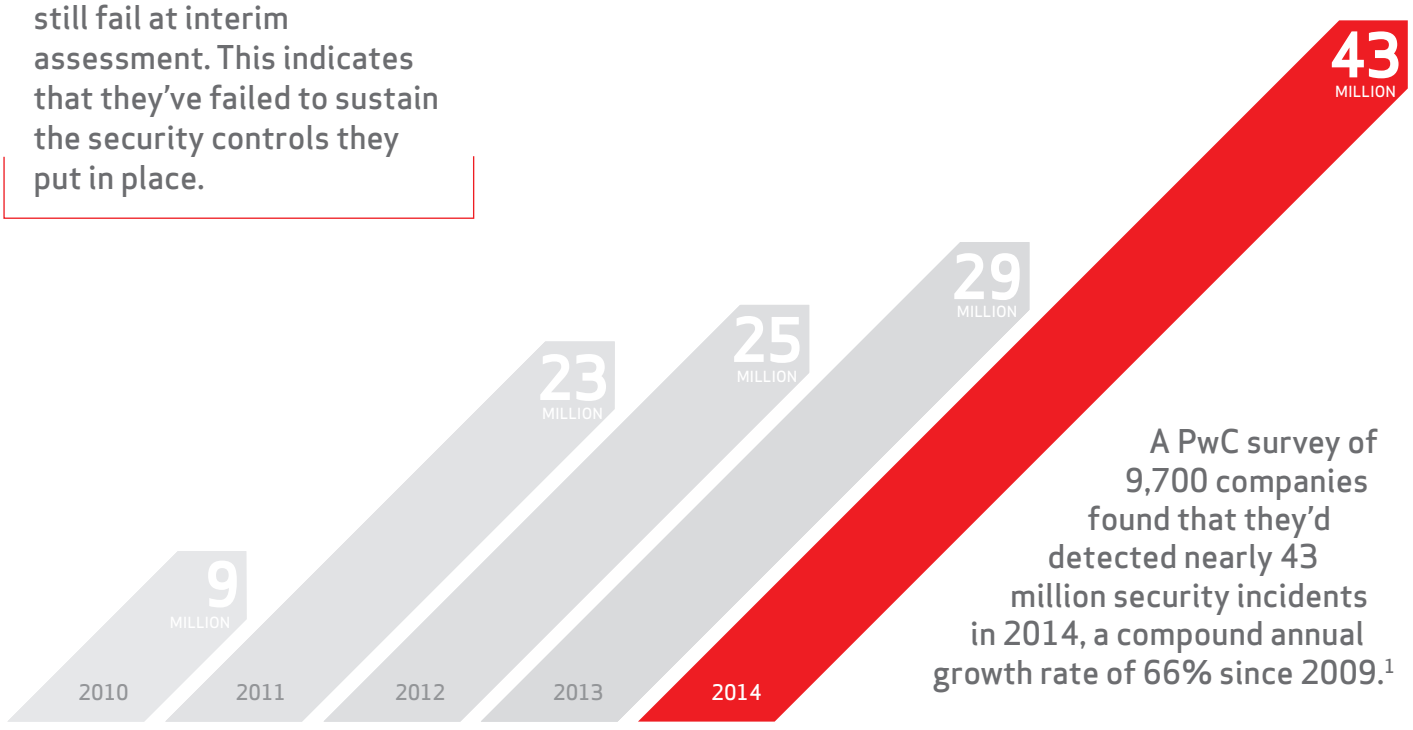
In 2014, two-thirds of organizations did not adequately test the security of all in-scope systems.

This year we've expanded this report, our fourth on PCI DSS compliance, to give even greater insight into payment card data security. As well as looking at compliance, we investigate the sustainability of security controls and ongoing risk management.



Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to improve, but four out of five companies still fail at interim assessment. This indicates that they've failed to sustain the security controls they put in place.

Did you suffer a data breach in 2014? Even if you avoided a breach, it's likely that you saw an increase in the number of security incidents — according to PwC research, since 2009 the volume has grown at an average of 66% per year.[1] It seems that it's only retailers and entertainment companies that make the headlines, but organizations of all kinds are affected. In this report we look at how well prepared companies are to withstand attacks and mitigate the impact of breaches, and recommend how you can improve.



A PwC survey of 9,700 companies found that they'd detected nearly 43 million security incidents in 2014, a compound annual growth rate of 66% since 2009.[1]

Executive summary

This year we've studied even more data and broadened our analysis to give a more complete picture of the state of payment security and insight into the challenges of managing risk. In what we believe is an industry first, this year's report includes analysis of the use of compensating controls and the sustainability of compliance.

On the face of it, an 80% increase in the number of companies that are validated as PCI DSS compliant at interim assessment would seem like a cause for celebration. But when you look at the numbers and see that four out of five companies are still failing (88.9% in last year's report) it's clear that there's a lot more to do.

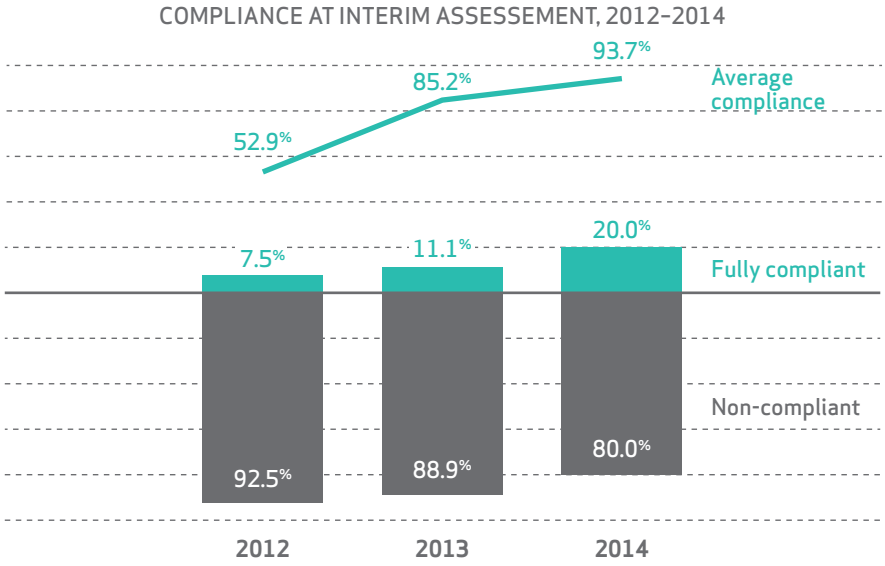


Figure 2: The overall state of PCI DSS compliance at interim assessment, 2012 to 2014

WHY PAYMENT SECURITY MATTERS

Your customers put their trust in you every time they make a purchase. They trust that you will not only deliver the product or service promised, but also that you'll keep their details safe. But every new report about a data breach makes them a little more concerned about their personal information being compromised.

Will your company be next? And what might that mean for your brand, your sales pipeline, your share price? That's why whether you're the CEO, CMO, CIO or CFO, payment security should matter to you.

The PCI Data Security Standard (PCI DSS) provides a very useful framework for looking at the state of payment card security. We've gathered a wealth of data during compliance assessments, enabling us to provide a quantified analysis. This is our fourth report on payment card security and each year we've looked at more data in order to provide richer and more informative insight.

TAKEAWAY 1: COMPLIANCE IS UP

Between 2013 and 2014 compliance went up for 11 of the 12 PCI DSS Requirements — the average increase was 18 percentage points. The biggest increase was in authenticating access [Requirement 8]. The only area where compliance fell was testing security systems [Requirement 11], from 40% to 33%. In fact, 14 of the 20 subcontrols and testing procedures with the lowest compliance were within Requirement 11.

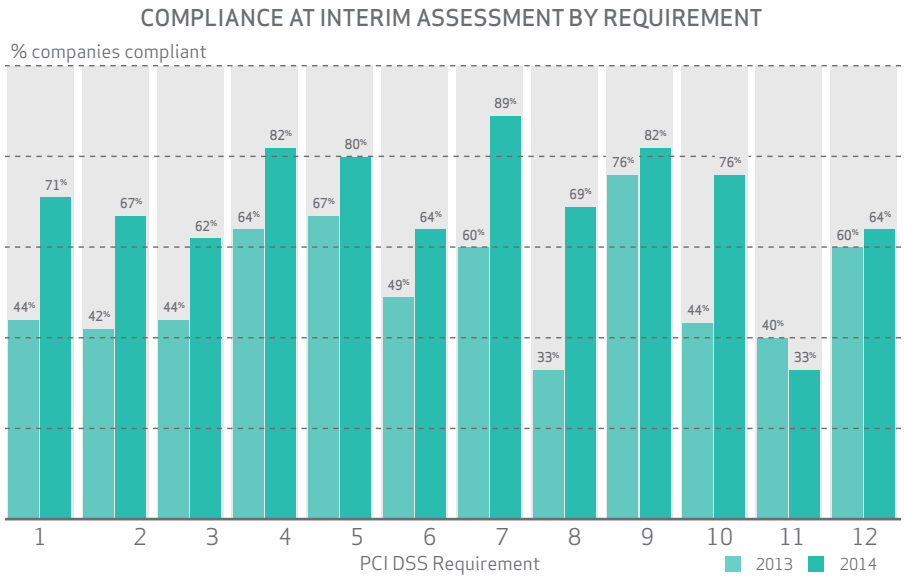


Figure 3: Compliance at interim assessment by Requirement, comparison of 2013 and 2014

TAKEAWAY 2: SUSTAINABILITY IS LOW

This year we've extended the report to look at where companies are most likely to fall out of compliance. The news isn't good: less than a third (28.6%) of companies were found to be still fully compliant less than a year after successful validation. There are a number of possible reasons for this. First, it's very easy to fall out of compliance if you don't have robust procedures in place for managing and maintaining it. And second, a compliance assessment can only ever be a snapshot. All it in fact proves is that the company was able to demonstrate compliance at that moment, for the selected sample of sites, devices and systems checked.

The takeaway is that companies should focus on building a robust framework with security policies, procedures, and testing mechanisms, as this will increase the chance of being compliant — and customers' data being protected — not just at the point of validation but every day of the year.

TAKEAWAY 3: DATA SECURITY IS STILL INADEQUATE

The volume and scale of data breaches in the last 12 months make it clear that current techniques are not stopping attackers — in many cases they aren't even slowing them down. In last year's report we talked about deficiencies in the PCI DSS, including its over-reliance on prevention and lack of attention to detecting attacks, mitigating damage, and identifying residual risk. But our viewpoint has always been that the PCI DSS is a baseline, an industry-wide minimum acceptable standard, not the pinnacle of payment card security.

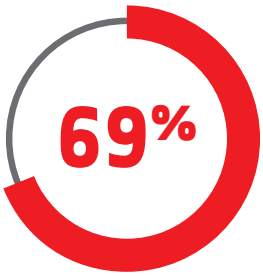
PCI DSS compliance should not be seen in isolation, but as part of a comprehensive information security and risk-management strategy. A PCI DSS assessment can uncover important security gaps that should be fixed, but it is no guarantee that your customer's data and your reputation are safe. Of all the data breaches that our forensics team has investigated over the last 10 years, not a single company has been found to be compliant at the time of the breach — this underscores the importance of PCI DSS compliance.

THE LONG GAME

Data breaches are rarely "smash and grab" affairs. Often criminals will try various types of attack looking for a weak spot. Increasingly this includes attacking the systems of partners and then using their "trusted" access to compromise your systems. Another common tactic is to target less critical systems, say the company intranet, and once in look for ways to "hop" into other systems. So if you leave your payment systems vulnerable to attack, it's not just your customers' card data that you could lose, but just about everything.

As an example, as we were writing this report a quite staggering data breach was unfolding. A plethora of commercially sensitive data has been published online — not just customer information, but also embarrassing internal communications, HR data that commentators believe could lead to discrimination cases, security certificates that could be used to make malware appear legitimate, and the list goes on.

Why payment security matters



of consumers would be less inclined to do business with a breached organization.[2]

DATA BREACHES ARE A SERIOUS BUSINESS

In the year since our last report we've seen many new headlines about customer data being stolen. And the impact stretches far beyond IT. The CEO of one of the world's biggest retailers resigned as a direct result of cardholder data being stolen and millions of cards compromised. Other companies that have suffered a breach have seen loyal customers desert them and their share price tumble. And most people only ever hear about a few of the breaches that happen.

Figure 4: Global cost of payment fraud (source: BI Intelligence[3])

Looking at the media it would be easy to conclude that it's only retailers that are affected by payment card data breaches, but that's far from the truth. From airlines to zoos, any business that takes card payments is a potential target. That's not just retailers: banks, processors, acquirers and card issuers are at risk too. And governments aren't immune, as more services are being charged for — like the use of public facilities — and put online — like parking permit applications. If an organization stores, processes, transmits, or otherwise touches payment card data, it's potentially a valuable target for attack.

Many of the stories that reach the papers and TV news are from the US, but data breaches happen everywhere — Verizon's 2014 Data Breach Investigations Report (DBIR) analyzed breaches from 95 countries. But when a breach happens in the US we are much more likely to hear about it. 47 of the 50 US states have mandatory notification laws, forcing companies to publicly disclose any loss of data. Other countries have similar laws and many more are considering introducing them — the European Parliament has approved the first draft of a law that would affect all member countries. In short, no country, no industry, and no company is safe.

Cards aren't going away, use is growing

Card payments matter. News of their demise, to be replaced by apps and mobile payments, has been greatly exaggerated. The day will come when using a payment card is an anachronism; but for now, spend continues to grow in every region. In 2015, total world card payments are expected to exceed $20 trillion[4].

CARD PAYMENTS BY REGION, 2012–2018

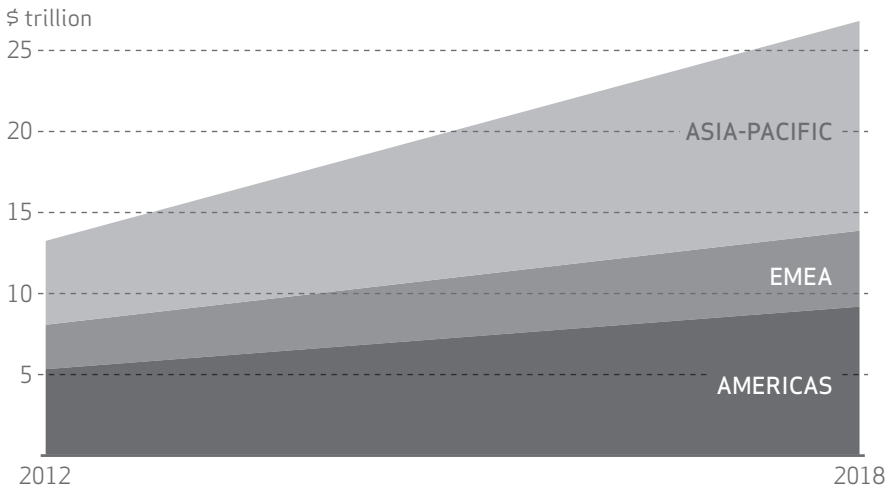
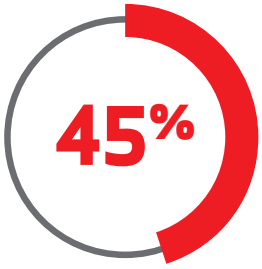


Figure 5: Total value of payments by card by region (Source: PNC Payment Solutions News, Spring 2014[4])

Put in context of total purchases, this figure is even more impressive. Taking the US as an example, credit and debit cards account for two-thirds of purchases by value. A further $2.17 trillion is spent via electronic methods[5], such as PayPal and mobile payments — many of which are ultimately backed by card transactions.

SPLIT OF PAYMENTS (US)

Figure 6: Split of payments by type in the US (Source: The Nilson Report, 2014[5])



"45% of Americans say they or a household member have been notified by a card issuer, financial institution, or retailer that their credit card information had possibly been stolen as part of a data breach."[5]

The effect of payment innovation

Credit and debit cards have been with us for more than 40 years, and the fundamental idea has remained unchanged. But there has been significant innovation by the card brands and banks, both to improve the customer experience and decrease the risk of fraud.

We've seen processing become electronic, signatures replaced by PINs, magnetic stripes replaced by chips, and interactions become contactless. These changes have been partly motivated by efficiency, speed and convenience for the user; but security is also a key driver. Not all innovations are obvious to the user. Behind the scenes, we've seen fraud identification augmented by sophisticated business rules using cardholder behavior, location and other contextual information to supplement basic verification information.

SMARTER CARDS

EMV cards (referencing the founding members: Europay, MasterCard, and Visa), commonly known as "Chip and PIN" or "CHIP and signature", these cards have become familiar around the world. Since 2005, many payment networks implemented liability shifts (see glossary), region by region, to promote the adoption of EMV for ATM, point of sale, and unattended payment terminal transactions. In the US, most of the major card brands have set October 1, 2015 as the liability shift for point of sale terminals, and October 1, 2017 for automated fuel dispensers.

But EMV is not a panacea. Experience from other countries suggests that it displaces fraudulent activity rather than stamping it out. Once EMV increases the security of card present transactions, attackers may focus their attention on "card not present" (CNP) transactions, including online shopping. Taking Canada as an example, following the introduction of EMV in 2008, the fall in counterfeit and lost/stolen crime has been surpassed by the growth in CNP fraud (see Figure 7).

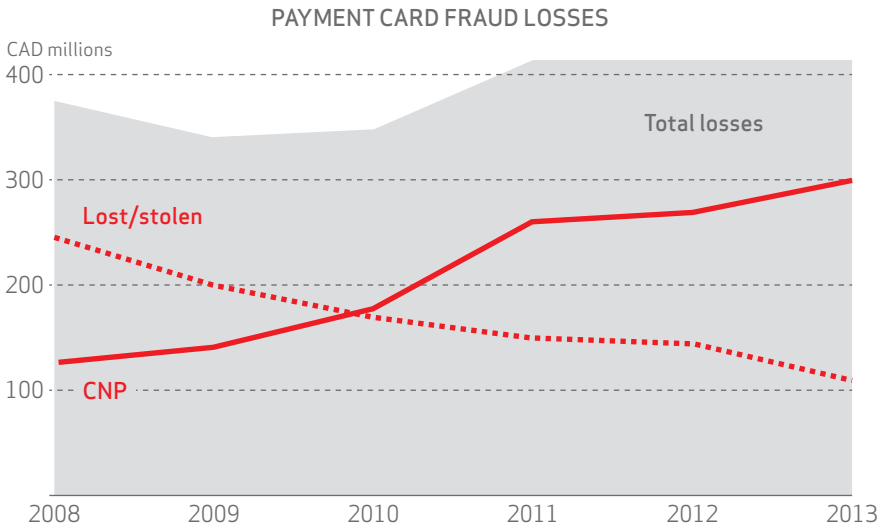


Figure 7: Card fraud in Canada, 2008 to 2013 (data from Canadian Bankers Association[7])

This is not a new phenomenon. Whenever one means of attack is thwarted, criminals rarely decide to change profession — they simply look for alternative vulnerabilities to exploit.

CRYPTOCURRENCIES

There continues to be a certain amount of interest in cryptocurrencies, such as Bitcoin. While these do have a place and may even be preferred for some transactions, they are still regarded as a high-risk option by most consumers and not really part of the mainstream payment infrastructure. However there are signs that these currencies are becoming mainstream: Bitcoin is now accepted by hundreds of retailers, including Amazon, Sears, Target, and Subway.

Banks and card issuers have responded to the increase in CNP fraud by introducing:

- **3D Secure**: Requires the cardholder to enter a password based on the issuer and the assessed level of risk. 3D Secure has been popular with e-commerce due to low integration costs and has been reasonably successful in containing fraud.
- **Tokens**: EMV secures communications between the card and the POS terminal, using dynamic data to effectively prevent counterfeit fraud. But it does not encrypt transaction data, this still flows "in the clear" once in the merchant system. Tokenization can take over at this point, replacing the card data with a secure token.
- **Behavioral analytics**: These tools assess the fraud risk of each transaction by detecting suspicious activities or behavior patterns. This might include unusually large purchases, using a channel (such as a mobile app) that you don't normally use, or attempting to make purchases in two far apart places within a short period of time.

CONTACTLESS PAYMENTS

Instead of requiring the payment card's magnetic stripe to be swiped, or the card to be placed in a reader, contactless payments use radio frequency (RF) technology to send payment account information to the merchant's POS terminal. There is nothing to sign and no numbers to enter, but the value of transactions is limited — from September 2015 the limit in the UK will increase to £30 ($45). The transaction has the same fraud guarantee protection as a normal card payment, and includes added security technology both on the contactless device as well as in the processing network to prevent fraud.

Despite being available since 1997, the use of contactless payments has remained relatively low. Recently many payment card networks have started issuing debit and credit cards with contactless technology as standard, and this has led to growing use.

MOBILE PAYMENTS

Consumers can now pay using their smartphones through a range of payment technologies, which offer convenience and speed. These may include:

- Mobile-based readers or terminals that work with payment cards and replace traditional POS card machines. Square's dongle-based service has processed more than a billion transactions since its launch.
- Mobile apps that use the phone's near-field communication (NFC) or other close-range communications technology to make payments by interacting with a POS terminal. In 2014, Apple launched Apple Pay, which uses biometrics, tokenization and NFC; Starbucks has another approach — its app displays a unique barcode linked to the consumer's Starbucks account, which the barista simply scans.
- Mobile apps that make payments or peer-to-peer transfers via the internet, without any direct local interaction with in-store systems.

While we believe that the actual payments will still be handled through the existing card brands and banking systems, this appears to be a significant trend and the beginning of the end of the plastic card.

Mobile solutions may collect, store and use payment data in different ways and different locations. And although payment applications developed for use on customer mobile devices are not currently subject to PCI PA-DSS requirements, they still need to comply with the secure application development controls in PCI DSS. The SSC has recently updated existing guidance for developers to clarify this.

Mobile Payment Acceptance Security Guidelines for Developers v1.1

Mobile Payment Acceptance Security Guidelines for Merchants as End-Users v1.1

Cellphone companies, including Verizon, are working with banks to use their data to make behavioral analytics even more effective. One example of this is using location data from a consumer's cellphone as an additional factor when scoring the risk of a transaction — if it's a cardholder-present transaction and their phone is 500 miles away, the chances of it being fraudulent are much higher.

Migrating to new POS systems is costly and takes time, but it does provide an opportunity to introduce point-to-point encryption (P2PE) solutions, which can make a major contribution to security and compliance.

The impact of changes in the IT environment

As well as changes in the threat landscape and payment technology, the last few years have seen significant changes in the corporate IT architecture. The growing prevalence of new technologies like cloud is redefining the environment within which payment systems must operate.

MOBILITY

Mobile devices are an increasing data protection risk for enterprises. They are large in number, can be easily lost or stolen, and introduce a wide range of new security risks, including vulnerabilities in their operating systems and user-installed apps. Although mobile device management (MDM) solutions are fairly widely used, many enterprises and security vendors are inexperienced in mobile application security. New platform versions — such as Android Lollipop — are shipping with major security and manageability improvements, including more secure configurations enabled out of the box.

Access to applications and data is no longer limited to company-owned devices, using company-controlled networks, to access company-hosted applications. Staff and customers use a broad range of devices, many of which are personally owned, and access applications around the clock from a range of locations outside of the company perimeter. They're accessing data in many more applications, which may be hosted on virtualized or shared cloud platforms around the world.

IT departments already use a range of security techniques and approaches — from DLP, SIEM and IPS to anti-virus, encryption and mobile device management — but these often rely on having full access to and control of application servers and endpoint devices.

VIRTUALIZATION

The business case for consolidation often focuses on cost reduction and ignores the potential impact on compliance. What then happens is that the security controls on the whole environment can be dictated by the compliance requirements of a single application, such as payment processing. This is an issue we regularly encounter when performing an assessment: although the virtual server processing payment data is included in the DSS scope, the hypervisor and all its management processes and systems have been missed.

Infrastructure architects should carefully consider the following before deciding a virtualization solution is the best platform for payment solutions:

- Bringing the hypervisor into DSS scope may add a significant burden. If the CDE only consists of a few servers, the benefit is unlikely to outweigh the additional compliance effort required. For smaller environments, moving all services into their own virtualized environment can provide an easy way to create a complete PCI DSS environment of its own and improve availability, making maintaining the scope boundary easier.
- Virtualization can be very difficult for companies that are subject to both PCI DSS and PCI PIN, typically issuers and acquirers. The very strict separation requirements can be extremely costly to implement in a standard virtualized environment, making leaving these systems outside of the virtualization the best option.
- In a virtualized environment the boundary between volatile (in memory) data and stored data is eliminated. It is very easy to store a snapshot of an entire running system (including encryption keys and CHD stored in memory) to disk.
- The rapid provisioning of new servers is one of the benefits of a virtualized environment, but this poses another challenge for compliance. When new security controls need to be implemented or new security patches are rolled out, the templates for new servers must also be updated.

CLOUD

Moving solutions from an internal environment to an external cloud-based solution has many implications for compliance, including the need to:

- Document and agree in writing what the obligations of the service provider will be — DSS 3.0 has made this clearer by adding control 12.8.5.
- Ensure that the cloud provider will support any forensic investigation you might be subjected to. No matter what you outsource, the liability for payment compliance remains yours.

Enterprises should weigh the promise of cloud with their liability (specifically the cloud provider will be subject to all the requirements of control 12.8) and balance the direct savings with the additional controls required to maintain compliance.

Alternatively, if a strict scope boundary can be created by tokenizing, hashing or encrypting CHD before it is sent to the cloud, this could keep the service provider and its cloud out of scope. But this will mean ensuring that the encryption, tokenization, and key management processes are out of reach of the service provider.

Many acquirers' contracts require much stricter "right to audit requirements" for your third parties than PCI DSS does.

See PCI DSS 2.0 Cloud Computing Guidelines for more helpful advice on the impact of cloud on PCI DSS compliance.

SECURITY TOOLS

In an uncertain and constantly changing IT landscape, where endpoints may not be trusted, effective access control is key. Static access control lists (ACLs), identity-based access control (IBAC) or role-based access control (RBAC) are no longer sufficient.

In the next-generation network, attribute-based access controls (ABAC) and authorization-based access controls (ZBAC) can evaluate a range of factors — including location, network, time, user identity, role, device, past activity, overall risk level, and application — and govern access granularly to sensitive resources on a case-by-case basis. For instance, if a formerly trusted device suddenly repeatedly attempts access from a new and untrusted location, the system may ask for more verification or restrict the level of access offered. Importantly, these kinds of access controls do not depend on devices being managed or enterprise-issued.

Alongside adaptive access controls, authentication mechanisms need to change too.

Many system administrators, let alone users, admit to writing down and sharing privileged passwords — an unwanted but understandable behavior given how many passwords are needed across the IT estate. Unfortunately, passwords remain a critical and fundamental weak spot. There are a number of solutions:

- **Multi-factor authentication**: Augmenting authentication with one-time codes, tokens or biometric information can help lock attackers out even if they have access to the user's password.
- **Secure single sign-on (SSO)**: SSO can help overcome "password fatigue", giving users access to a range of services using a single set of credentials. In combination with multi-factor authentication this can be a powerful solution.
- **Privileged access management (PAM) systems**: Enables companies to replace shared, static and insecure passwords with personal, frequently changed, strong authentication. Also allows fine-grained authorization logic and extensive audit logs.

The IT department can no longer even begin to "wrap its arms around" the company's data or the infrastructure that carries it. This is a real challenge, especially when security attacks are growing more sophisticated and more frequent.

Analysis of Microsoft Security Bulletins from 2013 by Avecto found that 92% of "critical" vulnerabilities would be mitigated by removing administration rights across an enterprise.[8]

PCI DSS compliance drives payment security

This section explores how PCI DSS compliance is connected to what really matters, security.

With no slowdown in sight for data breaches, it's no secret that the effectiveness of the PCI DSS continues to be a hotly debated topic. Skeptics claim that the DSS is too difficult and doesn't do enough to address enterprise security, often forgetting that the PCI SSC's mission is specifically to bolster payment security.

While we'd love to grow PCI-DSS-compliant and non-compliant organizations in a lab and compare payment breach rates between the two, that technology is still a few years out. But with the help of some of our colleagues elsewhere in the Verizon security practice, we did the next best thing.

As well as being an approved Qualified Standard Assessor (QSA) company, Verizon is also an approved PCI Forensics Investigator (PFI) company. Our team of forensic investigators step in after a compromise has occurred to help companies stem the breach and identify the weaknesses that allowed it to happen. In other words, we have the luxury of seeing payment security, and insecurity, from both sides of the fence. While there are differences between the two types of assessment (see box left) looking at the data can still give us a more complete view of the connection between compliance and security.

Think of the QSA clients as the control group, and the PFI ones as the breached "test" group. If we compare the two sets of data we can answer a very valuable question: what are the breached organizations doing differently to the control group?

COMPARISON OF PCI DSS COMPLIANCE AT INTERIM ASSESSMENT VS POST BREACH

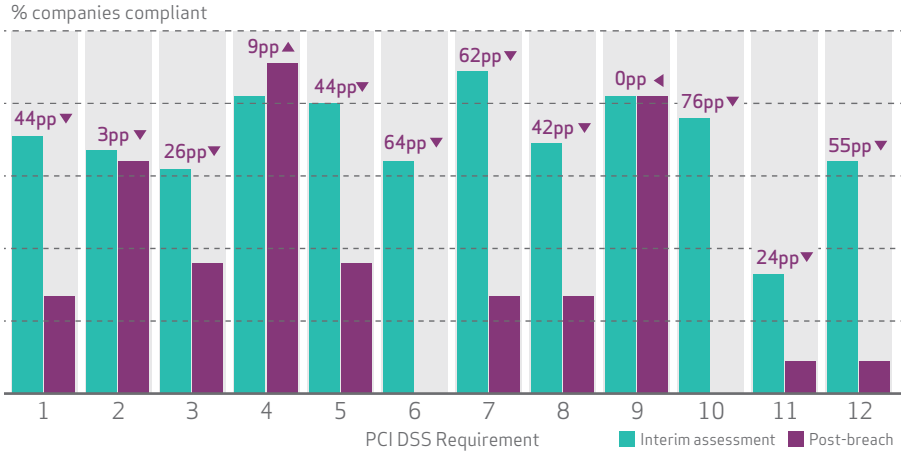


Figure 8: Compliance observed during QSA assessments and PFI post breach assessments, 2014 dataset

It's clear from the chart above that the companies that we visited post-breach as a PFI were significantly less PCI DSS compliant than our control group of QSA customers.

Not only were breached companies less likely to be found compliant overall, they were also less likely to be compliant with 10 out of the 12 Requirements individually. On average, the control (un-breached) group outperformed the post breach group by 36 percentage points. This certainly suggests a strong correlation between not being PCI DSS compliant and being more susceptible to a data breach involving payment card information.

PCI DSS ASSESSMENTS: FORENSIC INVESTIGATION VERSUS COMPLIANCE ASSESSMENT

Rather than diving into the specifics of each control and subcontrol as a QSA would, a PFI's task is to make a high-level assessment as to whether the organization was compliant with each of the 12 PCI DSS Requirements at the time of the breach. The PFI doesn't attempt to validate compliance (a positive), but rather looks for non-compliance (a negative).

Given these differences, it's likely that the PFI data will show a more optimistic picture of compliance by Requirement.

Lessons Learned from Payment Breaches

LOGGING, MONITORING, PATCHING AND MAINTAINING

Although we're still seeing breaches even with good system hardening [Requirement 2], none of the companies that had suffered a breach complied with the requirements for maintaining systems and software security [Requirement 6] or logging and monitoring [Requirement 10]. Patching, maintaining, and monitoring key systems is critical for achieving sustainable security. And companies that exhibit poor logging and monitoring are likely to take longer to spot breaches, giving criminals more time to do more damage. As reported in the DBIR each year, many breaches go undetected for months or even years.

GOVERNANCE

The next major delta between our datasets is on Requirement 12, which demonstrates the importance of strong and consistent security governance. With the renewed focus on security as business-as-usual in DSS 3.0, this gap will likely widen in the years to come.

ACCESS CONTROLS

There was also a large disparity between QSA and PFI clients on restricting access [Requirement 7]. Most security professionals are very familiar with the concept of least-privilege access, but as business demands and complexity grow, so too do the administrative challenges of adhering to it in practice. Apparently, breach victims struggle with this much more than other organizations. Breached companies were equally bad at authenticating access [Requirement 8], though the difference between the two groups was less due to lower compliance in the QSA dataset.

PERIMETER SECURITY

Every day, attackers are vigorously and repeatedly probing your defenses and trying to penetrate your perimeter, and the firewall is your first line of defense. Firewalls only work effectively if architected, tuned, and maintained properly. 71% of our QSA clients met all the controls associated with maintaining firewalls [Requirement 1] at the time of their interim assessment. In comparison, just 27% of breached organizations did. This suggests that ineffective perimeter security is a key contributor to the likelihood of suffering a breach.

Keep in mind that, for perimeter security to work, it is imperative that the perimeter is properly defined. Our forensic investigators often see network segmentation that's ineffective. DSS 3.0 addresses this problem with updated controls on penetration testing and the validation of segmentation.

DEFEATING MALWARE

Malware is another major threat. And again, we see a large gap between the groups on maintaining anti-virus [Requirement 5]. 80% of our QSA clients maintained all the controls in this area, compared to just 36% in the group of breached companies. CHD breaches typically involve a number of techniques, but many culminate in dropping a piece of malware on a high-value system. Having anti-virus software on all in-scope systems isn't just a PCI DSS requirement, it should be a fundamental part of any security program.

Traditional signature-based protection anti-virus scanners are largely reactive and not sufficiently effective to counter new and emerging threats — such as zero-day and social-engineering-based attacks. Therefore, organizations should use more sophisticated technologies that include proactive behavior detection, sandboxing, whitelisting, application control, cloud-enabled threat intelligence, heuristics, and reputation analysis.

It's important to note that traditional anti-virus relies on blacklists and is thus susceptible to false negatives, especially with the advent of customized malware. We recommend employing whitelisting in blocking mode as additional protection for key systems, such as point-of-sale systems.

PROTECTING STORED DATA

Protecting stored cardholder data [Requirement 3] is also important, but the gap between the two groups has been shrinking over the years. The QSA group is doing a decent, but not great, job with 62% of companies compliant. In the breached group just 36% are compliant. As more organizations shift to encryption, tokenization, and/or not storing CHD at all, we expect this requirement to further converge in the years to come.

0 IN TEN YEARS

Of all the companies investigated by our forensics team over the last 10 years following a breach, not one was found to have been fully PCI DSS compliant at the time of the breach.

TESTING SECURITY SYSTEMS

The area where companies in our QSA dataset fared worst was testing security systems [Requirement 11], with just 33% passing all the PCI DSS controls and testing procedures. In the group of breached companies this came joint 9th, with just 9% of companies passing. The lesson is clear: as an industry, breached and non-breached organizations alike, we all need to do better at testing our defenses.

REQUIREMENTS SHOWING LOW CORRELATION WITH DATA BREACHES

Requirements 4, 9, and 2 showed no discernible difference between the two datasets. Requirements 4 and 9 are not surprising: few, if any, large organizations transmit sensitive data in the clear over the internet, or leave hard drives out for the taking. Even fewer breaches occur due to such mistakes. It's surprising that Requirement 2 [Basic security hardening] isn't a more significant differentiator between breached and non-breached organizations. We theorize that, as an industry, we're doing a lot better than we used to at securely configuring systems before putting them in production. But, as the huge difference in Requirement 6 shows us, breached companies tend to do a much worse job at keeping those systems secure over the long run.

BIGGEST SECURITY BANG FOR YOUR COMPLIANCE BUCK

If we had to pick a Requirement as the biggest inverse indicator of potential breach, it would be 6 [Develop and maintain secure systems and applications]. We cannot overemphasize the importance of making sure that vulnerabilities are patched in a timely manner. Honorable mention goes to Requirement 10 [Track and monitor all access to network resources and CHD]. We must, as an industry, move away from the paradigm of configuring new systems and forgetting about them. We need to embrace a culture of security as business-as-usual throughout the entire systems lifecycle.

COMPLIANT VERSUS SECURE: SOME DEFINITIONS

VALIDATED PCI DSS COMPLIANT

A company that's passed a full assessment can be said to be "validated as compliant". It may or may not be fully compliant — the areas of non-compliance could just not have been identified during the validation assessment. And even if it was compliant, it may fall out of compliance — for instance by failing to perform regular scans.

COMPLIANT

Actually being PCI DSS compliant means achieving and maintaining all the PCI DSS controls throughout the year.

REASONABLE ASSURANCE

Compliance doesn't guarantee that an organization is secure (see across), just that it has an acceptable level of security in place — as defined by a standard like PCI DSS. There is always a possibility that a security control failure cannot be prevented, detected, and corrected in time. It is the responsibility of management to govern and manage inherent-, residual- and control-risks.

SECURE

No organization can ever be fully secure. "Secure" is an absolute and it is not possible to say with certainty that a breach cannot occur. To do so you'd need to have complete knowledge of all threats, established and emergent.

In the last few years our forensics experts have seen an increase in the number of data breaches carried out by government-sponsored agents. Faced with the resources that a government could put behind an attack, even national security agencies are concerned about being hacked. And new actors and threats are emerging all the time.

RESILIENCE

Some people think that not having been breached proves that the company is secure. This isn't the case. You could leave your car unlocked and come back to find that it hadn't been stolen, but it wouldn't be accurate to say that your car was secure while you were away. A resilience-focused system accepts that failure is inevitable and focuses instead on early discovery and fast recovery from failure.

The knock-on benefits of compliance

Many people see compliance as a burden. And with pressure to reduce costs, business leaders are asking tougher questions about what is being done, how and why.

There will always be constraints on the amount of people and money available, and it can be a challenge to convince senior management that these resources should be focused on "compliance" rather than, say, developing a new product line.

Unless they can see the relationship between the effort that they put in to compliance and the benefits they get out, the logical approach would be to do the bare minimum to comply. This is a challenge when security and compliance are there to avoid a possible negative outcome: how can you measure the cost of a breach that you avoided?

Many organizations are still either not sufficiently aware, or not capable of measuring the benefits of PCI DSS compliance to justify the investment in not just complying with the letter, but also the spirit of the rules.

There are many benefits of taking a holistic approach to governance, risk and compliance, both regulatory and operational.

This section explores how PCI DSS compliance can add additional value, and explores in more detail how to measure the cost and return on investment of your compliance initiatives.

REDUCED DATA BREACH COSTS

Since 2009 our research for the PCI Compliance and Data Breach Investigations Reports has shown a strong correlation between compliance and data protection. Organizations that had suffered a data breach showed lower than normal compliance with a number of PCI DSS controls. While compliance is no guarantee that you won't be breached, it should reduce the likelihood — that's why the PCI DSS exists.

This is important, because there are many costs associated with breaches:

- Fines for non-compliance.
- Notification, card reissuance, and credit monitoring costs for affected parties.
- Forensic investigation and remediation costs.
- Reputational damage, reduced partner and/or consumer confidence and lost business.
- Lower share price and impact on your ability to raise capital.
- Negative impact on user and consumer trust.
- Increased interchange rates charged by banks and/or processors.

Consumers are increasingly aware of the value and risk associated with their data, and when choosing providers (from retail to financial) they make decisions about whether they can trust the provider's tills, ATMs, websites, and mobile apps. Compliance with PCI DSS can help build trust by demonstrating your commitment to following best practice and protecting your clients' data.

A STEPPING STONE TO HOLISTIC GOVERNANCE AND RISK MANAGEMENT

The PCI security standards are evolving toward an integrated approach to governance, risk, and compliance. They are designed to promote unified and continuous compliance. To achieve PCI DSS compliance, organizations must review business processes, IT infrastructure and architecture, the flow of CHD, business partners and data sharing, user security education, awareness and competency to design, implement and maintain security controls, and so on.

One of the criticisms of the PCI DSS, in common with any set of standards, is that focusing on compliance validation could actually be a distraction from achieving and maintaining genuine security. But for most companies the DSS provides a useful baseline. While validation is no assurance of security, not being compliant is pretty much a guarantee that you're not secure.

A PCI DSS compliance program is a great opportunity to uncover and correct:

- Ineffective oversight mechanisms.
- Organizational silos and wasted resources and information.
- Poor architecture designs.
- Unnecessary complexity.
- Lack of data and security integrity.

PCI DSS presents opportunities for operational optimization well beyond data protection and compliance, and many organizations use the annual PCI DSS compliance program business case as an opportunity to tackle a range of other organizational challenges, like:

- Increasing employee awareness of security and creating a more active and alert security posture across the organization.
- Simplifying and consolidating IT architecture through redesign, hardware and software purchases, business process correction or optimization — often leading to savings.
- Improving business processes and process management — for instance as a result of greater transparency into data flows or through following best practices.
- Building better partner and supplier relationships — through greater clarity over roles and responsibilities.

Continuous measuring and monitoring of the operational benefits of compliance drives increased understanding and support for data protection, compliance and eventually the acknowledgment that compliance can make a substantial contribution toward more effective business management. How do you put a value on compliance? Unlike many business investments, the ROI of compliance may not be immediately obvious in terms of bottom-line benefits.

COMPLIANCE, DATA BREACHES, AND THE LAW

The PCI security standards are not law (except in a couple of US states) and so non-compliance is not punishable by imprisonment; instead, it's enforced through terms of business as part of the contract between the merchant, acquirer, and other parties. Companies that choose not to comply are likely to get less beneficial commercial terms (and may even be refused service), and those that suffer a breach and are found to have fallen out of compliance are likely to face significant penalty fees.

While PCI DSS compliance is not a legal requirement, many territories already have data breach disclosure laws and the coming few years are likely to see a significant increase in the coverage and power of these laws.

In January 2015, President Obama outlined a plan to push for a federal data breach disclosure law covering all US companies. The proposed law would oblige companies to notify potential victims of a suspected data breach within 30 days. Almost all states already have a data breach law, and many of those are more stringent than Obama's proposal. Some only cover defined industries — typically insurance and healthcare — but set tighter time limits, as little as five days, and several include financial penalties.

In March 2014, the European Parliament approved the European Commission's draft proposal to overhaul the 1995 data protection directive. This would establish a single, pan-European law for data protection with a supervisory authority. Companies that fail to comply could be fined up to 5% of their annual revenue. The law would apply to all companies selling to EU citizens, regardless of where the company is based.

Another area where the law is having an effect on information security is insurance. Several recent cases have confirmed that insurers are not liable to pay out for the cost of breaches under commercial general liability policies. And a growing number of companies are finding their claims under specialized data breach insurance policies rejected because they have failed to take adequate security measures.

There are a number of sources that can help calculate the value of compliance:

- **Expert reports**: Several firms, including some of the big consultancy firms have published detailed reports and models on calculating the cost of a breach in different industries and countries.
- **Peer filings**: The public records of fines, penalties and settlements can show how your peers are performing. Does a similar compliance spend (as tracked, for example, in annual reports) produce the same levels of fines?
- **Ratings agencies**: Compliance failures can tarnish an organization's brand. Ratings agencies covering different sectors and industries allow companies to determine a value for failure — and therefore the brand value of compliance.
- **Internal KPIs**: Key performance indicators can indicate improved quality and speed of tasks, reduction in errors, and the deduplication of tasks after process reengineering and automation.

By establishing clear targets for ROI and processes to measure it, companies can better track their performance year-to-year. It's important that these measures are broad, strategic and comprehensive. Everything should tie back to strategic risk management and to the long-term journey of compliance in the organization, including forecasts and projections.

CALCULATING TCO

Any major initiative that needs organizational funding should have a total cost of ownership (TCO) assessment encompassing direct and indirect expenses, both in terms of upfront costs and ongoing maintenance and operations across the solution lifetime or a specified number of years. Without a true understanding of TCO, it is impossible to measure ROI, or to fairly choose the best option from competing alternatives.

Costs will obviously vary depending on the size and complexity of the organization and its IT infrastructure and processes; the existing security measures in place and overall risk-management maturity; and any scope-reduction efforts put in place.

But the scope of PCI DSS is broad and the changes involved can be too. Costs include:

- **Infrastructure**: Additional IT hardware and software for encryption, anti-virus, firewalls, intrusion detection, log management, and more, with associated purchase, licensing, installation, migration and integration, upgrade, operation and support costs.
- **Services**: Consulting, assessment and regular vulnerability scanning services, as well as process changes, staff training and user education during change-management activities. Given how fast-paced the security market is, it's important to factor in ongoing upgrades and changes to security frameworks.
- **Staff time**: IT and business staff will devote some or even all of their working week to planning, actioning, reporting on and auditing PCI DSS controls, instead of their 'day job'.

Some may compare the cost of investing in PCI DSS compliance to the cost of a data breach and say that this is a case where the remedy is worse than the ailment.

But while an awareness of cost efficiency is important, the answer is not simply to pare compliance funding to the minimum. Reducing TCO should be approached as part of a larger ROI discussion. It's better thought of as optimizing TCO, on the understanding that cost is balanced against other factors such as business risk, compliance, operational resiliency, and business control and agility.

There is a TCO model associated with doing nothing, too, and that may include the cost of running legacy infrastructure that a PCI DSS program may have replaced, as well as anticipated breach costs that a PCI DSS program may have avoided. Although TCO calculations will not measure "soft" benefits such as better customer trust or staff productivity, TCO should factor in direct cost savings that the investment can produce.

Throughout this research report we'll make reference to specific Requirements described in the PCI DSS 2.0 and 3.0, and related standards such as PA-DSS and P2PE. These documents can be obtained from the PCI SSC document library: pcisecuritystandards.org/security_standards/documents.php

Analysis of the state of PCI DSS compliance

In this and the following sections we take an in-depth look at the state of compliance. We look at the changes since version 2.0 of the standard and how compliance has changed since our report last year. In addition, we report on the use of compensating controls and methods to simplify compliance and make security controls more sustainable.

COLOR CODING

Throughout this report we use the following color-coding in charts to help identify which measures we are comparing.

- Compliance observed by a QSA at IRoC stage.
- Compliance at the time of a breach identified by a PFI.
- Compliance sustainability, based on revalidation assessments.
- The use of compensating controls.
- Degree of change between DSS 2.0 and 3.0.

WHAT'S NEW?

With three years between DSS 2.0 and 3.0, it's hardly a surprise that there are a lot of changes. There are many changes in technology and the threat landscape to address. But as PCI DSS is a mature standard, many of the updates are clarifications and small changes rather than entirely new requirements.

Any attempt to quantify the scale of changes will obviously be somewhat subjective, but we have attempted to be as impartial as possible. We analyzed the number of controls and testing procedures that were entirely new and revised, and scored each Requirement accordingly. We then summed up all the scores to show the overall change by Requirement on a scale of 0 to 12. This provided some interesting results: for example, in our mapping visualization Requirement 8 stood out as having the most numbering changes, but in this analysis Requirements 11, 9, and 12 showed significantly more change.

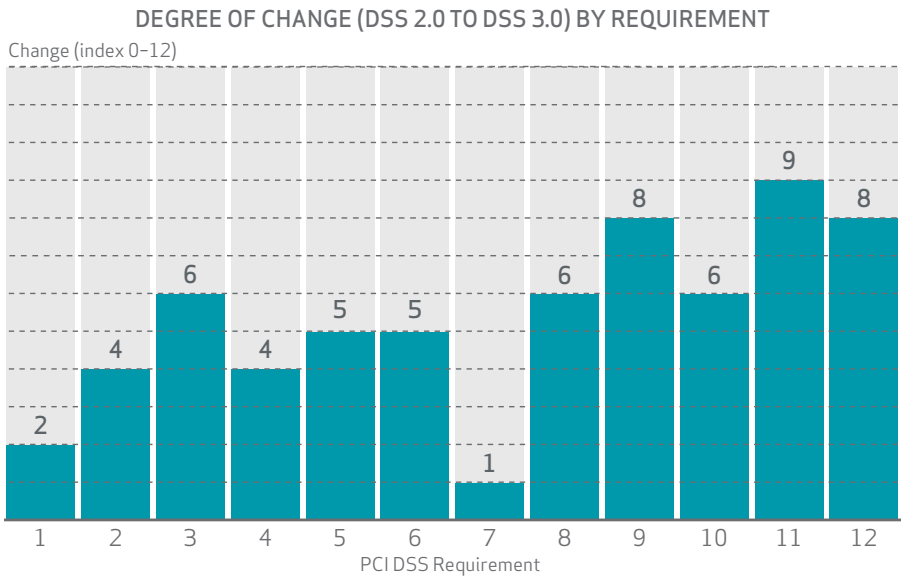


Figure 9: Degree of change between DSS 2.0 and DSS 3.0 by Requirement

In February 2015 the PCI SSC announced that, due to recently discovered vulnerabilities, no version of the secure sockets layer (SSL) technology meets its definition of "strong cryptography". The relevant PCI standards will be revised to reflect this, and the SSC will issue an FAQ to clarify the impact of these revisions.

Many applications have been developed with the SSL vulnerabilities, and may require a complete rewrite of code. Additionally, many security appliances will require vendor involvement to apply fixes.

While there's no practical way to remediate vulnerabilities in the SSL protocol, there are alternatives. Organizations should use alternative methods such as IPsec and SSH where practical to encrypt cardholder data on the client before it's sent to the server. Even TLS v1.2 contains some vulnerabilities, and may not be fully secure in some implementations.

THE STATE OF COMPLIANCE

In 2014 we saw a significant increase in compliance, but still only 20.0% of organizations were fully compliant at the IRoC stage.

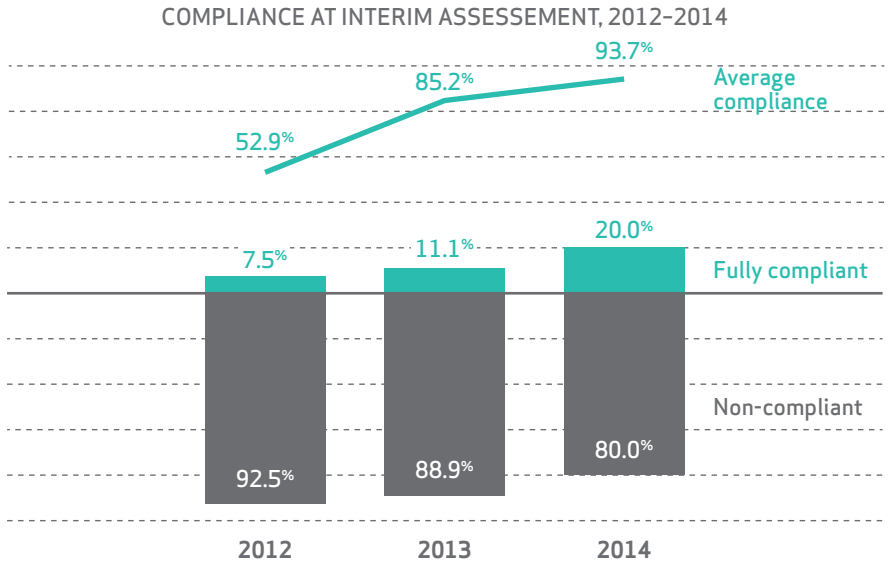


Figure 10: The overall state of PCI DSS compliance at interim assessment, 2012 to 2014

Across the board, the average increase in compliance by Requirement was 18 percentage points. But the variation was quite large — from Requirement 8 that went up 36 percentage points to Requirement 11 that fell by 7 percentage points.

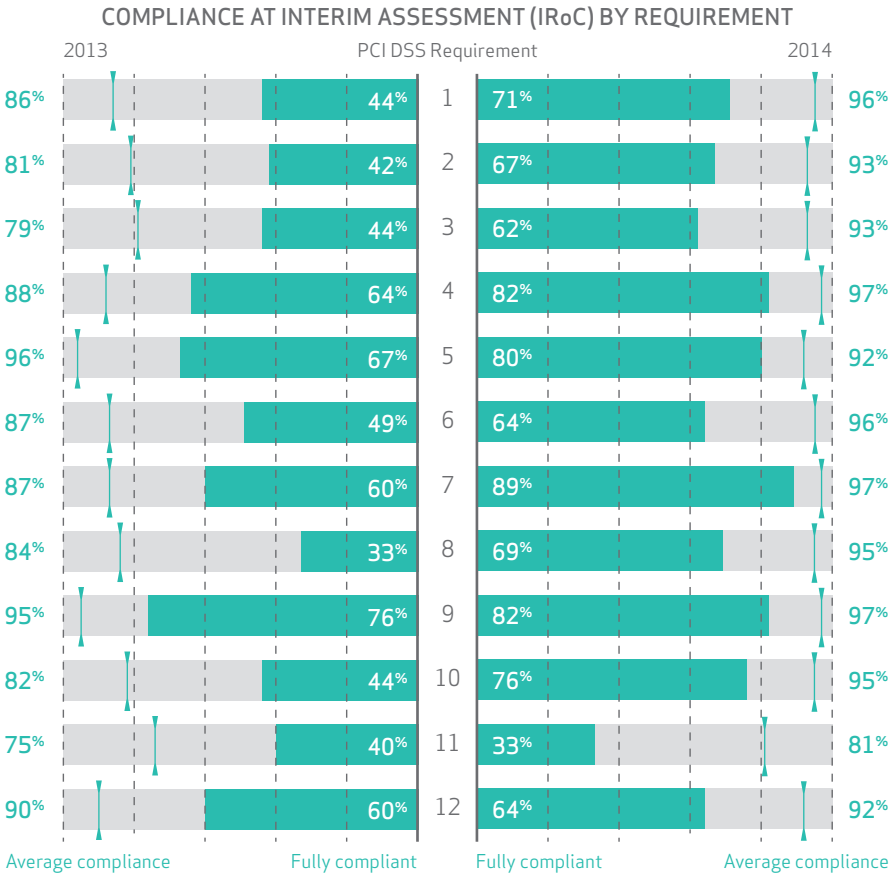


Figure 11: Full and average compliance by Requirement, 2013 versus 2014

KEY TERMS

Throughout this report we use the following two terms to describe the systems being discussed:

- **CDE:** The cardholder data environment.
- **DSS scope:** The CDE, all connected systems, plus any other systems that either support the security of the CDE or that if compromised could affect the security of the CDE.

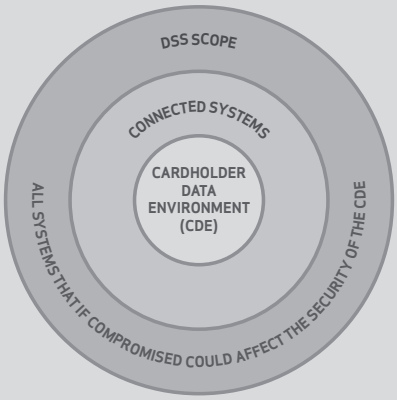


Figure 12: Scope terms

We also use the following terms for the payment card data itself.

- **CHD**: Cardholder data.
- **SAD**: Sensitive authentication data.

For more information, see the glossary on page 75.

Over 90% of all controls, subcontrols, and testing procedures were passed by 80% of companies — a marked increase over last year. And 25% were passed by all companies that we assessed — the highest any control scored last year was 98%.

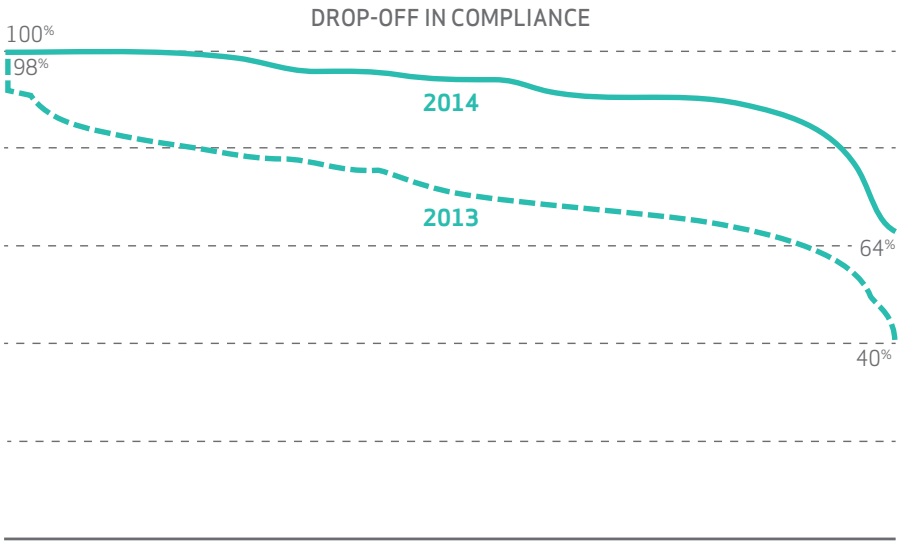


Figure 13: Dropoff in compliance 2013 versus 2014

As well as compliance by company, we also looked at average compliance. We worked this out by looking at all the of lowest-level subcontrols, and testing procedures (those that don't have any other subcontrols, and testing procedures beneath them) under a particular requirement (eg, all those under Requirement 3), and divide the number that were passed by the total. Comparing this data with the compliance by company (full compliance) provides some interesting insights:

Looking at this data over the last three years, we've seen overall average compliance grow from 53% to 94%, a 77% increase. Over the same period full compliance grew from less than 8% to 20%, 167% increase.

The picture gets even more interesting when we look at the picture by Requirement. Average compliance rose for 11 of the 12 Requirements, the exception being Requirement 5 that fell from 96% to 92%. All the Requirements now show average compliance of over 90%, except Requirement 11.

Not only does Requirement 11 lag on compliance by company, it's also the last in the pack when it comes to average compliance. But actually, average compliance grew from 75% to 80% while full compliance dropped from 40% to 33%. So while companies are generally getting better at meeting the demands of this Requirement, they are struggling to get from mostly compliant to fully compliant. And the area where they most often fall down is control 11.2 (see page 64 for details).

Bottom 20

The testing procedures with the lowest pass rates in 2014.

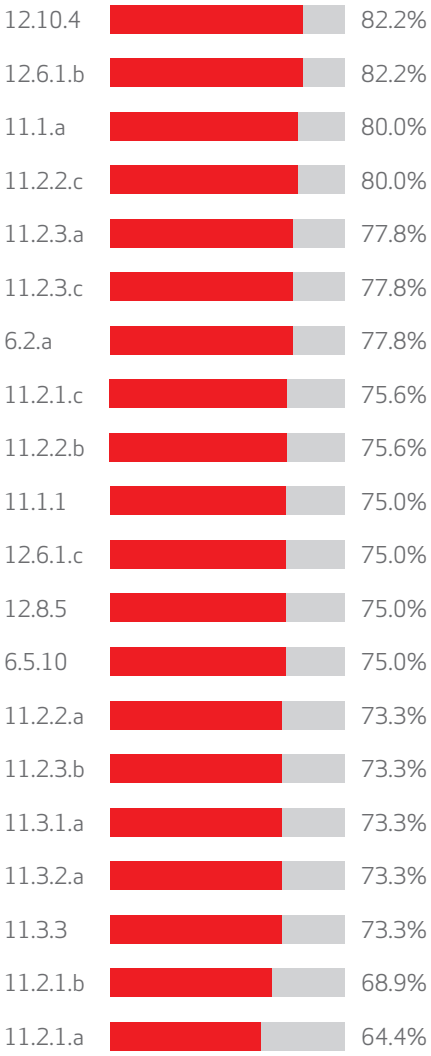


Figure 14: Least compliant testing procedures in 2014 interim assessments

Use of scope-reduction

SCOPING IS THE FOUNDATION FOR COMPLIANCE

The bigger and more complex your processes and systems for storing, processing, transmitting and accessing CHD, the harder it will be to achieve and maintain compliance. Scope reduction is the primary means by which you can limit the size of the compliance task. But it's not just about compliance.

Cutting the DSS scope will result in lower total cost of ownership, make maintenance of security controls easier, and reduce risk by limiting the attack surface.

For all these reasons, it is strongly recommended that organizations look at implementing a sound scope-reduction strategy. This should be done right at the start of your compliance initiative as practically everything else is based on the defined compliance environment.

Scope reduction may involve fundamental changes to network architecture and to business processes, and it's not always an easy task. The challenge is how to do it without adversely affecting service or incurring prohibitive costs.

There are several key issues:

- **Defining what "out of scope" means:** The PCI SSC has given guidance on what "out of scope" means: a system component must be fully isolated from the CDE, such that even if the out-of-scope system component was compromised it could not impact the security of the CDE.
- **Handling "connected systems":** The CDE and all connected systems are considered in-scope. A "connected system" is considered to be any system component that establishes or participates in any communication (this is, connectivity) with any system component within the CDE, regardless of the reason for the connection, the type of communication protocol used, or which device initiates the communication session. A system component is therefore considered to be not connected (isolated), and out of scope of compliance only when it cannot communicate with any component within the compliance environment, and has been evaluated to confirm that it is unable to compromise the security of the CDE. Isolated networks must still be documented in the report on compliance (Requirement 1).
- **Verifying what is out of scope:** DSS 3.0 requires organizations to "Implement a methodology for penetration testing, and perform penetration tests to verify that segmentation methods implemented are operational and effective." The SSC has not issued specific technical guidance or specifications to define the approved and recommended scope-reduction methods, and this is an important gap. The industry desperately needs a guidance document that clarifies the methods for controlling and reducing the scope of compliance. This would help organizations understand how they can avoid needlessly including components in scope as a result of uncertainty on the PCI SSC's intentions.

If you can take systems out of scope you can avoid the cost and effort of involving them in PCI DSS compliance activities, both in terms of regular activities (such as patching or vulnerability scans) and the annual assessment.

EXAMPLE OF A "CONNECTED" SYSTEM

A good example of such a case would be an administrator's laptop used to connect to the CDE through a restricted jump host. This laptop:

- Does not store, process, or transmit CHD, and is therefore not a CDE system component.
- Does not have the ability to directly connect into the CDE (the CDE would deny it).
- Can only connect to the CDE through the jump host.

But if the laptop was compromised, it could have a significant impact on the security of the CDE. The new "if compromised" language forces organizations and QSAs to consider all risks to the CDE when making decisions around scope exclusions.

Components and systems excluded from scope must still be reevaluated as part of each validation assessment to confirm that their exclusion is still justified.

NOT JUST WHERE DATA SHOULD BE

In payment security, just like any other security initiative, it is important to follow the guiding principle that you can't secure something unless you first understand it.

A proper scoping exercise starting with business process analysis and data flow mapping is an important prerequisite to any PCI DSS endeavor.

The PCI SSC has made it clear that scoping of the CDE must be based on a thorough evaluation of CHD locations and flows. This means not just documenting where data should be, but verifying where it might have ended up — including in mobile devices, email inboxes, office documents, zip files and locked files.

Few organizations do this kind of data discovery and scope verification during assessments, and indeed doing it effectively is impossible if relying on manual methods. A new wave of discovery tools automates scanning and reporting for location of CHD and SAD across the IT estate, including mobile platforms. These tools should integrate with SIEM tools (to alert and react to improper movement of CHD) and with DLP platforms (to detect and block improper transmission of data in real time).

In addition to the risk assessment and evaluation of all components within the DSS scope, DSS 3.0 also requires verification of excluded system components to confirm that their exclusion from the scope of compliance is valid. Therefore, organizations should perform a risk assessment on connected systems as well as on the excluded system components, to determine whether excluded components, if compromised, could impact the security of the CDE. If the answer is "yes", they must be included in the scope.

Many organizations claim that the requirement to continuously maintain full isolation of the CDE is complex and cost-prohibitive — particularly considering the cost, effort and resources needed to continuously maintain all applicable DSS compliance requirements on connected systems, and complexity around shared systems within trusted environments.

REDUCING THE SCOPE (DATA)

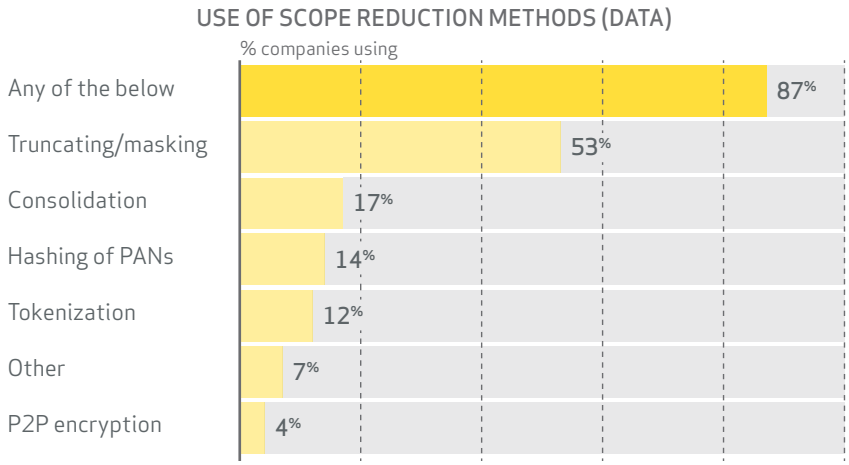


Figure 15: Breakdown of scope reduction methods (data) seen in FRoCs, 2012-2014

There are several ways in which organizations can limit their DSS scope by reducing the number of places where CHD or SAD is at risk, including:

Truncating/masking: Components using or storing appropriately truncated PAN data — and it's rare that full PAN data is required — reduce the risk of compromise, and can in most cases be removed from scope. 53% of organizations in our dataset applied adequate truncation of PANs.

Consolidation: Using a detailed, up-to-date CHD flow map, organizations can physically and logically consolidate all systems that store, process or transmit CHD, and eliminate redundant storage, systems and applications. In our sample, 17% of organizations achieved a significant amount of consolidation.

Hashing of PANs: Using strong cryptography to replace the PAN with a fixed-length message digest that it is computationally infeasible to revert to the PAN. 14% of organizations reduced their scope by storing and transmitting hashed PANs.

Tokenization: Organizations realized the benefits of moving away from encryption, in particular due to the challenges around cryptographic key management, and the increased frequency of attacks where memory parsing malware is used to extract keys or sensitive data directly from RAM. In 2014, 12% of organizations in our dataset used tokenization.

There have been significant improvements in tokenization solutions, including solutions by the card brands themselves. Tokenization as a Service (TaaS) is gradually gaining ground. Traditional designs are being replaced with innovations such as vaultless and in-memory tokenization that reduce complexity and provide significant advantages in performance.

Several organizations now prefer to combine advanced point-to-point encryption with a hosted tokenization solution, since it offers a flexible and comprehensive way to protect data at every point in the transaction lifecycle while still providing the opportunity for data mining and detailed customer analytics based on tokens.

Point-to-Point Encryption (P2PE): This is a very important data protection method recommended for all merchants. In 2014, only 4% of organizations in our dataset implemented P2PE within their compliance environments. The number of approved P2PE solutions, in particular those that offer payment terminals that also support EMV, is still very limited.

Only a handful of validated P2PE solutions were available in 2014, but is expected to steadily increase in 2015. The announced update of the P2PE standards will provide more granular certification solutions also aimed at increasing the amount of validated solutions.

REDUCING THE SCOPE (SPAN OF CONTROL)

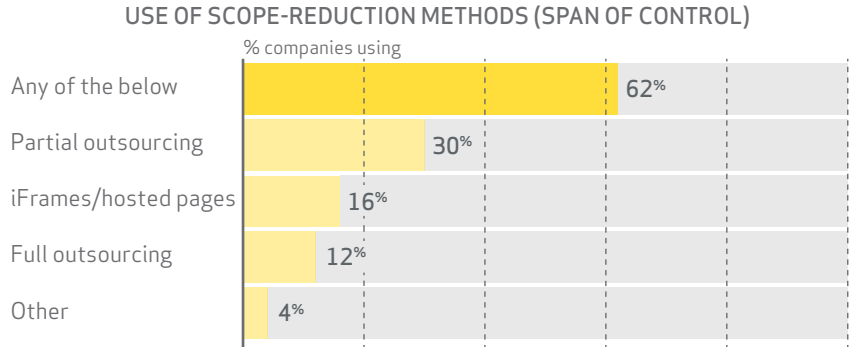


Figure 16: Breakdown of scope reduction methods (span of control) seen in FRoCs, 2012-2014

Partial outsourcing: More than half of organizations outsourced some aspect of their PCI DSS compliance. More organizations are realizing the benefits of outsourcing particular PCI DSS operational tasks and responsibilities to third parties.

A third (30%) of organizations contractually transferred the execution of aspects of their CHD storage, processing and handling operations to a third-party provider to partially eliminate CHD from their CDE. The elimination or reduction of CHD is achieved by either by not storing CHD at all, or by retaining only truncated or tokenized PANs.

System components that receive CHD (such as payment terminals, web server applications etc.) and critical security systems responsible for implementing required data protection functions, remain in scope of PCI DSS compliance and validation. Some organizations outsourced the capturing of payment card data entirely to avoid receiving and storing CHD on devices under the control or ownership of the organization.

The responsibility for PCI DSS compliance cannot be outsourced. Organizations must continually monitor all third-party organizations that could impact the security of CHD.

Iframes/hosted pages: 16% of organizations used inline frames (iFrames) or hosted pages (pages hosted by their payment gateway). These methods enable merchants to capture information about the transaction (such as the transaction amount, customer details and the transaction results) but avoid collecting CHD. Some 'payment page solutions' can be styled to look like part of the merchant's website. The process can be made transparent to consumers — avoiding redirecting them to an external website or URL.

Full outsourcing: 12% of organizations outsourced either all, or substantial parts, of their CHD processing to third parties. In several cases, this included the execution of their PCI DSS compliance management, monitoring, and maintenance. This can prove to be more cost-effective than managing the operations and retaining the expertise in-house.

By limiting the number of places where CHD is stored or accessible, and introducing security controls that prevent unauthorized access to the CDE, you will significantly reduce the probability of a payment card data breach.

DISTANCE DOESN'T MATTER

Our QSAs have faced some interesting arguments when validating the scope of compliance, particularly when it comes to network segmentation. Some companies have justified excluding systems based on distance, that is the number of "hops" to get from the system to the CDE. At a recent PCI community meeting it was suggested that only systems within three hops of the CDE could be considered to be connected, a "three hop" rule. If only IT security were that simple, we could all add a few routers and gateways around the CDE and our data would be safe. This is akin to saying that an unlocked door is a security risk, but three unlocked doors that must be navigated in turn is perfectly secure. Any system that's connected to the CDE, regardless of physical or logical distance, role, or function must be considered.

of companies used some form of network separation.

MODULAR, DYNAMIC NETWORKS ARE KEY

The increasing use of internal network zones shows that organizations realize the need to redesign their networks to achieve better security and operational efficiency.

Organizations should reduce internal system architecture complexity and fragmentation by defining and maintaining network zones that separate systems and networks based on security and communication needs. Consolidation of multiple devices, especially security systems within the DSS scope, will also lead to simplification and higher efficiency of both security and compliance monitoring and maintenance operations.

Key to this relatively new network model is a new class of network security device, called next-generation firewalls or network segmentation gateways. These embed all the capabilities of standalone security appliances into a single integrated solution and are designed to securely segment modern networks.

REDUCING THE SCOPE (INFRASTRUCTURE)

98% of the organizations that we looked at used firewalls or a combination of firewalls and routers as their primary means to implement effective access controls to isolate in-scope networks, and to establish internal boundaries between various network zones. Only 2% of organizations opted to apply PCI DSS across all system components across their entire organization, without using any form of scope reduction.

USE OF SCOPE-REDUCTION METHODS (INFRASTRUCTURE)

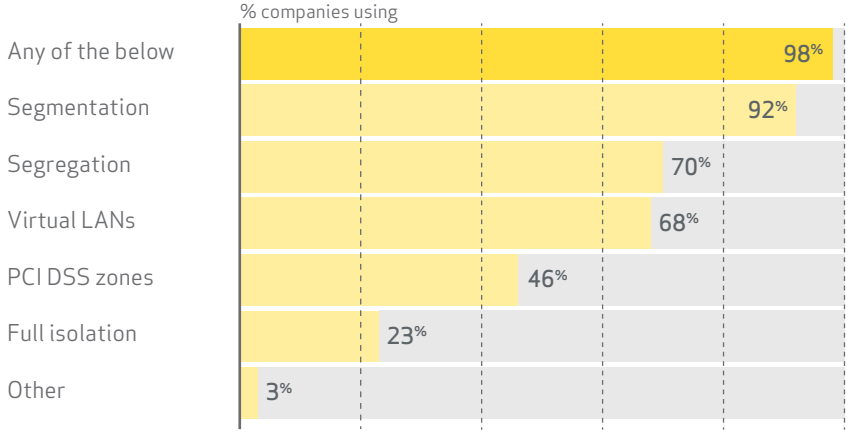


Figure 17: Breakdown of scope reduction methods (infrastructure) seen in FRoCs, 2012-2014

Segmentation: 92% of organizations used firewalls (or combination of firewalls and routers) to enforce partition networks and enforce network zones. Organizations that deployed next-generation firewalls as "segmentation gateways" benefit from increased effectiveness of external and internal perimeter access control and simpler administration of rulesets. A number of organizations still rely solely on outdated stateful-inspection firewalls or have not yet optimized the configuration of their next-generation firewalls to make full use of their capabilities.

Segregation: To establish and control secure communication between networked devices, they should be segregated using a combination of methods such as IP address restriction, communication protocol restriction, port restriction, and in particular application-level restriction. The restrictions are enforced by developing and maintaining device-specific rulesets on each of the networked devices. In addition to network segmentation, 70% of organizations also implemented secure system (host level) segregation within the CDE, as a part of their defense-in-depth approach to data protection.

Virtual LANs: More than two-thirds (68%) of companies in our dataset implemented VLANs with strong ACLs within their CDE. Segmentation was enforced by the VLAN in combination with properly configured firewalls and routers.

PCI DSS zones: Many large organizations, especially in the financial services sector, attempt to reduce the complexity of scope control by defining "PCI security zones", and then relocating all, or most of the system components that store, process or transmit card data, and connected systems, into those "zones". 46% of organizations in our sample used this technique to reduce DSS scope. Typically this approach requires the corporate network architecture to be redesigned, and includes network partitioning (segmentation), and system segregation according to system security and data sensitivity classifications. Sustaining the zones' integrity and boundaries requires rigorous enforcement of security standards, policies and procedures to control network and system operations.

Full Isolation: Less than a quarter of organizations (23%) achieved any notable degree of success in scope reduction when they attempted to implement and maintain full isolation across their entire compliance environment. This is largely due to the lack of clear specifications around how full isolation can be practically implemented and sustained, year-round — especially within large, complex networking environments.

Use of compensating controls

WHAT ARE COMPENSATING CONTROLS?

After data removal, network segmentation, and/or tokenization, there may still be PCI DSS control objectives that the organization cannot implement in such a way that would pass all the PCI DSS testing procedures due to some business or technical constraint.

This is where "compensating controls" come in. Compensating controls were introduced in PCI DSS 1.0. Since then the guidance has been updated to include stricter language about how each compensating control must be reviewed, documented, and validated as part of each annual compliance validation assessment.

A compensating control is a risk-based workaround for a constraint: it allows organizations to comply with the spirit of a particular requirement in an alternative way, a way that would count as satisfying the intent of the original security control.

Organizations can choose to meet almost any part of PCI DSS using compensating controls. They are, understandably, a very popular topic and an important safety valve for organizations facing difficulties. They show that the PCI DSS's mission is helping organizations control risk, not forcing them to follow a prescriptive path by only allowing one way of testing for compliance.

Compensating controls are only allowed when there is a legitimate technical or documented business constraint that prevents passing the standard validation testing procedures. The continued validity of all constraints needs to be rechecked each year, and if the constraint is no longer valid the compensating control discontinued. Therefore, in most cases compensating controls are not a long-term solution.

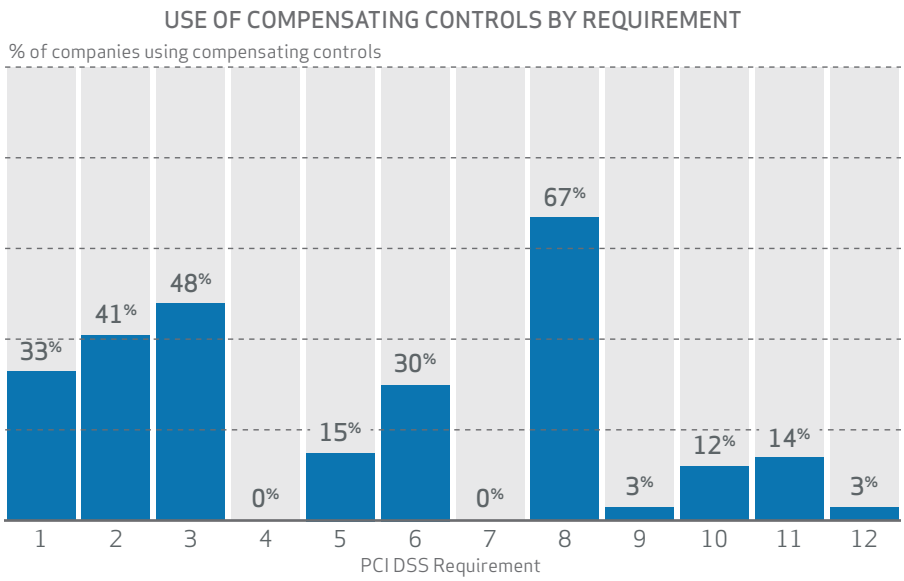


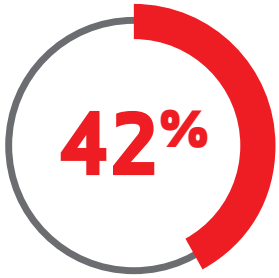
Figure 18: Use of compensating controls by Requirement, 2012–2014

USING COMPENSATING CONTROLS

Compensating controls are not an easy way out for any situation where a requirement might merely be hard to comply with. There are several limitations:

Validation is subjective

The organization must have a legitimate technical or documented business constraint to justify the use of a compensating control. This process is therefore subjective, based on each organization and assessor's view of "legitimate and documented" and their



In the companies that we looked at, the area where a compensating control was used most often was testing procedure 3.4.a — with 42% of the organizations not passing the defined testing procedure.

understanding of the objective and goals of each requirement and control. For example, the cost of implementation alone is not a legitimate constraint, though inability to fund the implementation might be. While assessors do their best to be consistent and fair, the individual's judgment will vary depending on circumstance and what one QSA/ISA might accept, another might reject. Currently, there is no publicly available repository or database of best practice scenarios that assessors can generally access, maintain, use as a guide, or use for performing intra-industry comparisons on the use of compensating controls within particular industries.

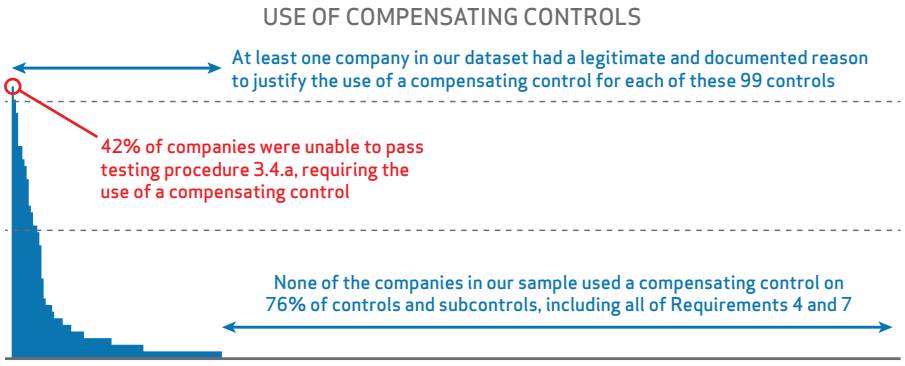


Figure 19: Subcontrols where a compensating control was used in descending order, 2012–2014

They're rarely a permanent solution

Companies must re-evaluate all constraints at least annually. In some cases — for example a legacy mainframe application lacking appropriate password controls — this is unlikely to change. But in many cases — for example being unable to upgrade a system in time — the constraint may no longer be valid.

The standards are high

Compensating controls must live up to the same standards as any other control approach. They're not a quick patch or a limited mitigation of a risk; they must fulfill the same intent as the requirement they're addressing, deliver the same or higher standard of protection, and avoid generating any knock-on risks. All of this must be fully planned and documented using the "Compensating Control Worksheet", either by itself (during self-assessment) or by the QSA. This risk analysis will cover areas like:

- What are the legitimate constraints preventing meeting the original requirement?
- What is the compensating control?
- What are the identified risks posed by the lack of the original control or introduced by the implementation of the compensating control?

Building effective compensating controls that pass the scrutiny of both a QSA and acquirer takes work. To be approved, the company must:

- Demonstrate that the compensating control is required due to either a legitimate technical constraint and/or a documented business constraint.
- Provide evidence that the compensating control sufficiently mitigates the risk associated with the requirement.

While some organizations may see them as a shortcut around a difficult control, in our experience compensating controls rarely take less time and effort than simply meeting the original requirement.

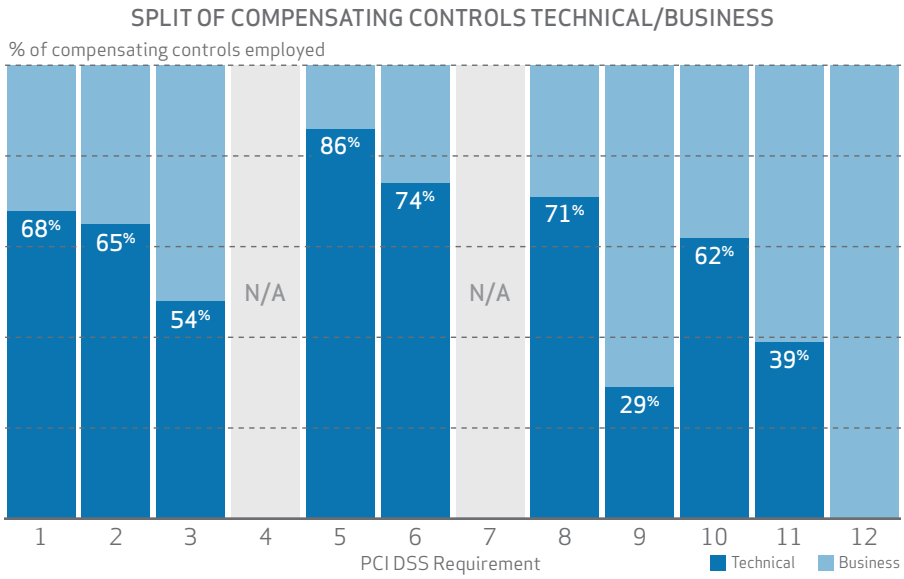
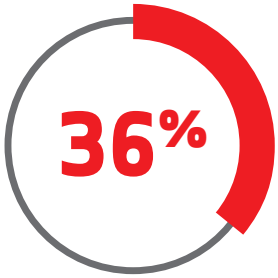


Figure 20: Split of constraints justifying the use of a compensating control technical/business, 2012-2014



of compensating controls addressed a technical constraint. Constraints included end-of-life software that could not be upgraded in time, security hardening settings that impacted the functioning of critical business applications, and the inability to apply critical patches within the required time frame.

TECHNICAL CONSTRAINTS

About one-third (33%) of all technical constraints are related to operating systems or applications which have a limitation that prevents or hampers the implementation of a particular control, or some restriction that prevents that control from meeting the intent of the requirement.

Less than a quarter of all technical constraints (21%) are due to a combination of infrastructure or architecture and application issues. A minority of technical constraints (12%) are due to third-party vendors placing restrictions on the use and modification of specific system configurations as part of their services agreement to support or maintain a device, platform, or facility. An example would be where an organization is unable to install additional software on a system because it will result in the termination of vendor service and support, a particular operating system that is not supported by a vendor, or lack of vendor support due to end-of-life.

BUSINESS CONSTRAINTS

Just over a third of all business constraints (36%) are due to internal operational limitations preventing the implementation of a required compliance procedure, and an equal amount is due to a financial or resource restrictions.

External business issues, such as third parties and vendors, account for 15% of the total business constraints. Only 6% of compensating control constraints are due to legal or contractual restrictions that prevent the implementation of the security control as specified in the standard.

Sustainability of compliance

Just 29% of the companies where we had a pairing of an FRoC followed by an IRoC were compliant at the interim assessment. This is nearly 50% higher than in the total dataset, but still quite low.

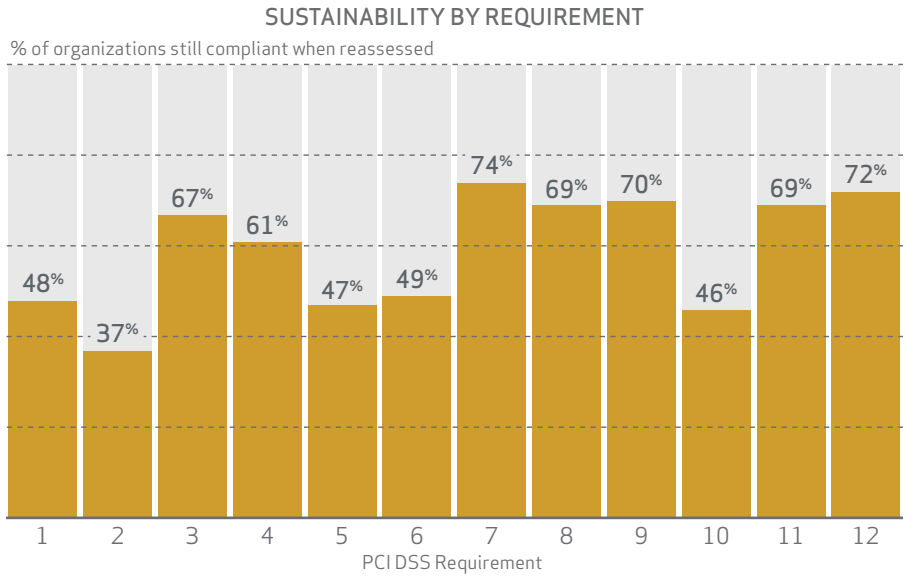


Figure 21: Number of companies compliant at interim assessment following successful FRoC, 2013-2014

For data protection and PCI DSS compliance to become business as usual, organizations must design and build sustainable control environments. This requires an organizational capability to maintain ongoing operation of all required security controls across a dynamic compliance environment, and a high potential (that is, organizational proficiency) to prevent or minimize any future deviation from the required standard of performance.

But many organizations rely on poorly designed and/or implemented controls, or manual operations that are both error-prone and costly to maintain. Controls that exist and are operated within poorly designed environments impede business efficiency and adversely affect security.

The extent to which compliance is sustainable is usually proportional to the investment an organization made to include sustainability as a compliance program objective, and part of project deliverables. Organizations achieve sustainability by design, building sustainability into the functional and operational specifications of the compliance program and reinforcing it through frequent education, training and awareness campaigns. Unfortunately, to date, controls appear to have been designed to focus more on their ability to withstand (inevitable) changes in the control environment; that is, to be robust, but not necessarily resilient.

Specifications should also factor in control resilience; i.e. the ability to recover from changes that negatively impact the functional and operational effectiveness of a control, or the control environment itself. Resilient controls improve the sustainability of a compliance environment. For example, specifying a procedure for how to recover from the introduction of a system component into the DSS scope which does not meet PCI DSS requirements. Or including a checklist on corporate change control worksheets to proactively detect planned changes that will lead to falling out of PCI DSS compliance before they are implemented, instead of reactively trying to correct such issues.

Organizations should be encouraged to implement and maintain risk-based compliance performance measurement (metrics) programs. The level of PCI DSS compliance sustainability can be monitored by tracking the amount of effort, resources (cost, people and time) required to maintain the required status of operation (that is, performance and effectiveness) and measuring the amount of deviations from the established standard of control operation and performance. Organizations that do not routinely monitor, report and evaluate the performance of their PCI DSS controls, fail to manage and maintain effective security controls. In fact, despite several years of PCI DSS compliance validation, many organizations are still not proficient at detecting and responding where controls dropped below established thresholds of functional or operational effectiveness, nor do they know when risk-tolerance levels are being exceeded.

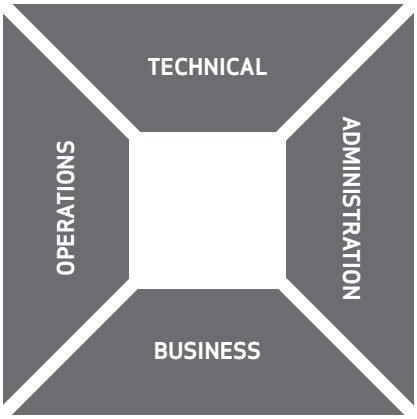
Evaluation of PCI DSS Requirements sustainability

The effort (existing resources, investment, and time) needed to maintain security controls breaks down into four areas:

- **Technical sustainability:** The complexity of the system components in an IT environment, the overall make-up (physical locations and architectural design) of the CDE and connected systems, and the number of parties involved (for example, third parties), can impact the level of investment needed to maintain the required configuration and functionality of system components.
- **Administrative sustainability:** All PCI DSS compliance programs require a substantial amount of operational documentation: such as policies, procedures, specifications, logs and written agreements. The effort required to maintain program documentation largely depends on the organization's level of the document management maturity and quality of the supporting IT systems to automate and streamline it. Administrative sustainability is also dependent on the organization's willingness to invest in continuous improvement through ongoing education, training, and awareness.
- **Operational sustainability:** The investment needed to operate, monitor, and maintain the performance of controls, to sustain the required ongoing level of effectiveness. This largely depends on the proficiency (IT, management, and security) of the staff and the operational culture of the organization regarding adherence to policies (formal and disciplined versus relaxed and "easygoing").
- **Business sustainability:** The alignment between strategic business objectives, data protection, and compliance objectives is one of the most important factors that influences the sustainability of PCI DSS compliance. It is not uncommon for executives to make strategic business decisions (like changes to sales channels and mergers) without considering the potential impact on information security and compliance, and how that might affect the business case. Later on, many companies find that a slightly different approach would have reduced the changes required to remain compliant significantly. Ensuring that strategic decision-makers are involved in the compliance process and consider the impact of decisions on compliance can save money and reduce disruption.

BEST PRACTICES FOR MAINTAINING COMPLIANCE

Section 4.6 of the PCI SSC's information supplement "Best Practices for Maintaining PCI DSS Compliance" recommends that organizations develop performance metrics to summarize the performance of DSS security controls, and as effective methods to measure the overall success of their compliance activities.



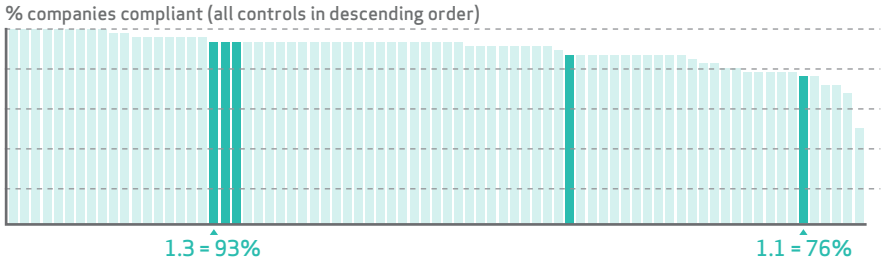
Compliance Maintenance Domains

Figure 22: Compliance maintenance domains

1

Install and maintain a firewall configuration to protect cardholder data

This Requirement covers the correct usage of a firewall to filter traffic as it passes between internal and external networks, as well as traffic to and from more sensitive areas within the company's internal networks.



WHY IS IT IMPORTANT FOR SECURITY?

A properly configured firewall is an essential part of the first line of defense. Firewall rules examine traffic and block any that doesn't meet security criteria, helping to prevent network intrusions. When ongoing management and maintenance of firewall and router configurations is neglected, it can significantly increase the organization's exposure and reduce security. Firewalls are not only essential to establishing the network perimeter, but also enforcing boundaries between security zones. Network partitioning (segmentation) alone is not sufficient, but it is a key preliminary step in securing any networked IT system.

Network segmentation and context-aware traffic filtering are key ways to limit exposure and reduce the likelihood of a successful breach.

Without effective access control in place, someone could access, modify or retrieve data from the CDE, either directly or through the use of malicious code. As well as making it possible to extract data, this could also be used to compromise the security management environment of the DSS scope — including administration consoles, Active Directory, patch management systems, and anti-virus consoles.

WHAT'S NEW?

Not traditional, stateful inspection, firewalls! Firewalls using dynamic packet filtering date back to CheckPoint's Firewall 1 in 1994, and 20 years is a long time in IT security. Network capacities have soared and the threats have become more complex, making traditional firewalls incapable of identifying all the unauthorized traffic.

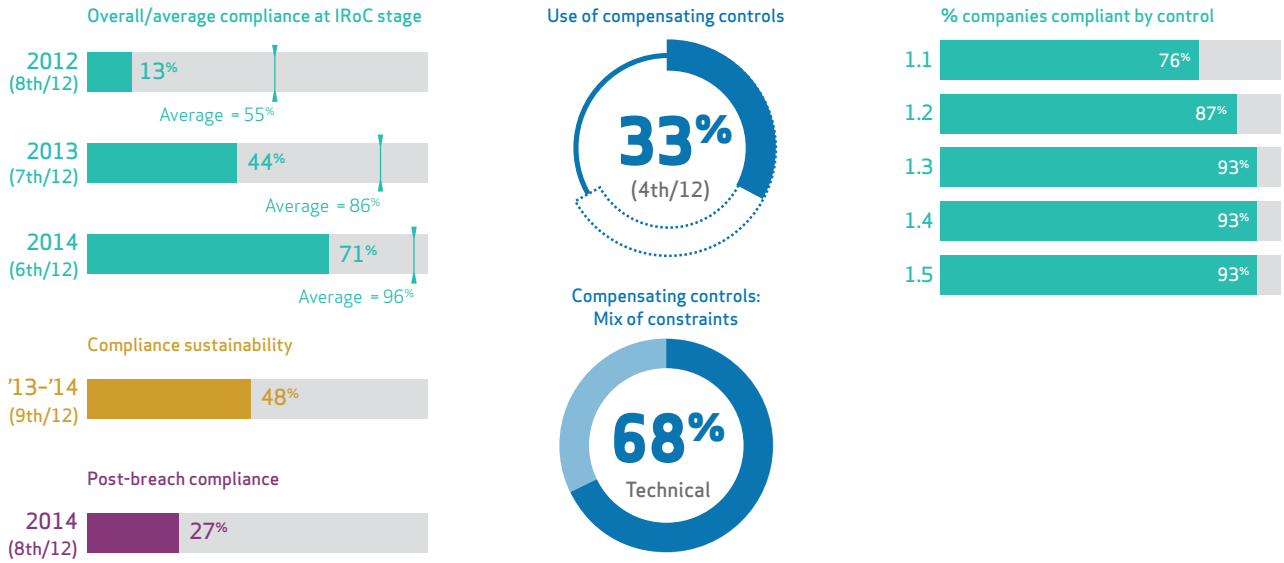
Next-generation firewalls are powerful devices that integrate full-stack (levels 2 to 7) protocol-based access control, email security, intrusion prevention, deep packet inspection, anti-malware, URL filtering, virtual private networks (VPNs), encrypted data and application control, and Active Directory in a single platform. This provides consolidated, multi-layer context-aware threat detection.

This integration means that potential threats detected in one component can be used to trigger changes in the behavior of the other components, providing multi-layer protection.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 1



Their manageability and ability to monitor activity at the application level, deal with the explosive growth in the number of devices, and block increasingly sophisticated threats make next-generation firewalls a must-have.

Most mobile platforms now support VPN clients at an OS level, and with the advent of "split tunneling", users can reduce the burden on VPN infrastructure by routing only sensitive traffic down the VPN tunnel. VPNs are still a recommended tool, but alternative solutions are emerging: for example, encrypted sessions to cloud applications already protect transport of data. VPN is also being replaced by containerization technologies and session border controllers (SBC), which instead of securing the device, secure the application and the connection it has back to the corporate network.

Updated control: 1.1 adds emphasis on implementing as well as documenting firewall and router standards. Several subcontrols have also been added to assist organizations in understanding the flow of data into and out of their environments. For example, 1.1.2 states that organizations must now produce a network map showing all the different hardware and software within the DSS scope. And subcontrol 1.1.3 states that organizations must produce a CHD flow map, which outlines where data originates in the network, how it is processed, and where it is sent out of the environment. Our QSAs are sometimes presented with a large number of diagrams, none of which show the right things. Most get the level of detail completely wrong: some border on the conceptual, others give far too much detail, distracting from their intended purpose. So the clarification of this control is very welcome. It should also help companies to understand the scope of the CDE and identify opportunities for reducing it.

Updated control: 1.4 clarifies the firewall control requirements for mobile devices — including those owned by employees — that can connect to both the internet and the cardholder environment. When connecting via the corporate environment, access to open public networks can be controlled — multiple layers of security can be applied that can block unauthorized traffic and identify malware and prevent it from reaching the device. However if a mobile device has unrestricted access to the internet or other public network, then there is a significant risk it could become infected. The malware would have bypassed the corporate network controls, and the whole DSS scope could be at risk when that device is reconnected to the internal company infrastructure.

Their ability to monitor activity at the application level, deal with the explosive growth in the number of devices, and block increasingly sophisticated threats make next-generation firewalls a must-have.

NOT ALL THAT IT SEEMS

We have seen instances of organizations having a next-generation firewall but not using its application-aware functionality, thereby exposing their network to threats exploiting social media applications and port hopping attacks. Organizations may not find all next-generation firewall features necessary, but they should enable functionality essential for detecting modern threats.

Next-generation firewalls have been widely available at a reasonable price for several years now, and while not required by the PCI DDS should be a part of every organization's security plan.

CAN A VIRTUALIZED FIREWALL BE PCI DSS COMPLIANT?

There's been some debate as to whether or not a virtual firewall can meet the requirements of 1.1.3. The DSS is rarely prescriptive about specific technologies; it focuses on the protection that must be in place. Hardware firewalls are not specified anywhere in the standard and so if a virtual firewall can perform the required functions then it should be considered PCI DSS compliant — as long as it meets the relevant controls on its configuration and use. If a virtual firewall is used, the whole virtualization stack it is running in should be considered as in scope for PCI DSS compliance.

THE STATE OF COMPLIANCE

Data from Verizon's RISK team shows that only 27% of organizations that suffered a data breach in 2014 were compliant with Requirement 1 at the time of their breach. By comparison, our QSAs found an average of 71% compliance with Requirement 1 in the same year. This shows a strong correlation between a badly configured firewall and the likelihood of a security breach.

Despite a substantial increase between 2013 and 2014, 51.1% to 75.6%, nearly a quarter of companies still failed to comply with control 1.1. Companies often interpret this control as simply requiring a dump of the firewall rules with an associated change ticket. They fail to document the security features enabled for each insecure service used, which requires mapping all the services in use.

COMPENSATING CONTROLS

A third of companies in our dataset used one or more compensating controls as part of their attempts to comply with Requirement 1.

Compliance with control 1.1.6 is often problematic, because organizations do not know which services, ports and protocols are open on systems within their organization, and in particular within their DSS scope. The testing procedures that most often necessitated the use of compensating controls, both by 31% of companies, were:

- 1.1.6.b [Identify insecure services, protocols, and ports allowed; and verify that security features are documented for each service].
- 1.1.6.c [Examine firewall and router configurations to verify that the documented security features are implemented for each insecure service, protocol, and port].

It is highly recommended that the management of system configuration is automated to provide ongoing visibility and active monitoring of system configurations, fully integrated into the corporate change control process.

SIMPLIFYING COMPLIANCE

Organizations typically have multiple security zones on their internal network — from about 4 in a small organization to 12 or more in most enterprises. Deploying traditional firewall architecture usually requires multiple firewalls or a combination of firewalls and VLANs with access control lists (ACLs) to establish these zones. This can result in high cost and complexity. A next-generation firewall can replace multiple traditional firewalls and other devices (such as intrusion detection and prevention systems) with a single device and management platform, significantly improving functionality and manageability. While DSS 3.0 does not require next-generation firewalls, adopting them can make complying with this Requirement significantly easier.

To comply with control 1.1 companies must have a thorough understanding of the flow of data, and few do. Often it's only the application's owner that knows what data is passed from one server to another, and it's very unlikely that a firewall administrator will know. It's important to change this. Firewall administrators should ensure that any request for a rule change includes details of what business process need justifies the change and what type of data will be affected.

You should also remember that merely comparing the current ruleset with the previous one looking for differences is not a proper firewall ruleset review.

Firewall teams can report on the current rules and provide guidance, but it should be the business and application owners that are ultimately responsible and who provide the business justification for firewall rules.

Configuration and change management isn't cool, but it's a highly effective way to simplify compliance and improve security. We strongly recommend that organizations automate the management of system configuration. Change is a constant in security and without automation it's impossible to keep abreast of the state of the whole DSS scope. No matter how many layers of security you have, if network devices are unpatched or incorrectly configured your chances of an attack turning into a breach are much higher. Automated configuration and change-management solutions provide visibility and active monitoring of system configurations, and can be fully integrated into the corporate change control process. As well as being able to run a baseline compliance report on an individual firewall, router or switch, the system should enable you to generate reports across the entire estate.

MAINTAINING SECURITY AND COMPLIANCE

We regularly see systems with unrestricted internet access to facilitate automatic OS and application updates, but this also offers a path for an attacker to exfiltrate data. Several recent high-profile data breaches involved the use of unrelated servers only intended for internal applications but with external connectivity. Servers like this can provide a staging point for a hacker attempting to steal information from other systems, like your POS systems. If external access is absolutely necessary, you should ensure that it is restricted to just the specific external resources that are required.

There's rarely a single factor to blame for a data breach, it's usually a combination of trivial issues — like overly broad permissions and failure to review configurations — that lead to a successful compromise. And firewall rules often feature in the list of contributing factors. Most people focus on inbound rules and pay insufficient attention to outbound rules. Inbound rules can help prevent the hacker getting in, outbound rules can prevent them — or a rogue employee — exfiltrating valuable data. Firewall restrictions should not just cover what data a system can receive, but also what it can send out.

Simplifying access control

Deployment of a traditional firewall architecture usually requires multiple firewalls and is often combined with VLANs and multiple other security devices to establish network zones and trusted internal boundaries. The use of multiple devices, each with its own ruleset and management console, not only results in high implementation and maintenance cost but also complexity. Many organizations already realized the need for consolidation and simplicity, and have replaced disparate security point products with next-generation firewalls that offer a single-vendor, consolidated architecture, and management interface.

The integration of application control, IPS, wireless and mobile security, deep packet inspection, encrypted data control, malware detection, and context-aware filtering in a consolidated unified threat management platform can significantly enhance the security capabilities of network access control. And as well as significantly enhancing functionality and network access control, next-generation firewalls also simplify manageability and so can provide considerable savings over the long haul.

Simplifying access control administration

Organizations that fail to govern security and network configurations to avoid the introduction and reintroduction of insecure configurations make maintaining compliance with Requirement 1 more difficult. Providing training to network and security administrators so that they have a consistent understanding and ability to identify features which would constitute an "insecure" services, ports, and protocols is critical.

Simplify documentation

There are still a significant number of organizations that produce poorly documented network and CHD flow diagrams. The latest applications can automate the discovery of all components within the DSS scope and significantly simplify the task of creating and maintaining up-to-date network diagrams, and system configuration documentation.

CALL TO THE PCI SSC

One of the criticisms that we made of DSS 3.0 in our 2014 report is that it still refers to stateful-inspection firewalls, a technology that most security professionals consider outdated. Malware and hacker attacks that can bypass stateful-inspection access controls have been common for nearly a decade. While other security standards have moved on, PCI DSS has not.

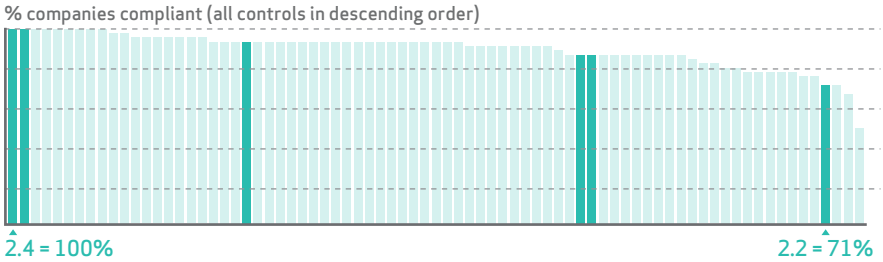
By failing to set a higher standard the PCI SSC is delaying the demise of this outdated technology, leaving the companies that still rely on it more vulnerable to attack.

In our opinion the failure to introduce this requirement in DSS 3.0 was a missed opportunity. We call upon the SSC to help raise the awareness around the firewall and anti-malware technology deficiencies and to update the DSS to reflect the latest widely accepted security practices. This will encourage more organizations to adopt up-to-date technology that is an order of magnitude more effective at detecting, preventing and responding to threats.

2

Do not use default passwords or security parameters

This requirement covers the controls that reduce the available attack surface on system components by removing unneeded services, functionality, and user accounts, and by changing insecure vendor default settings.



WHY IS IT IMPORTANT FOR SECURITY?

Vendors often ship products and services with default security settings. These defaults can be easily found on the internet and are included in many of the automated attack tools used by hackers. Not changing these settings offers attackers an easy way to gain administrative access to the device.

This is one of the simplest possible ways into a system — whether a laptop, server, or network appliance — but has been responsible for many data breaches in recent years. Once they've exploited this weakness to get in, attackers can gather data directly, deploy malware, or attack other systems. Changing settings at the time of installation is a simple and easy-to-implement process to harden systems.

Requirement 2 is one of the requirements most affected by the emergence of virtualization and cloud. These technologies simplify the way in which organizations run their IT infrastructure. However, with new technology always comes new challenges, like how to segment mixed environments (in-scope and out-of-scope systems hosted in the same physical server) to prevent attacks based on shared resources or other out-of-band channels. Hardening the virtualization stack can be quite a challenge.

WHAT'S NEW?

Updated control: 2.2.2 has been updated, but remains ambiguous. It refers to the services, protocols, and dæmons "necessary" for the functioning of the system. This can often get contentious: with sysadmins wanting to avoid changing systems and deviating from standard configurations, and QSAs insisting that common but insecure services like SNMP, FTP and Telnet are switched off.

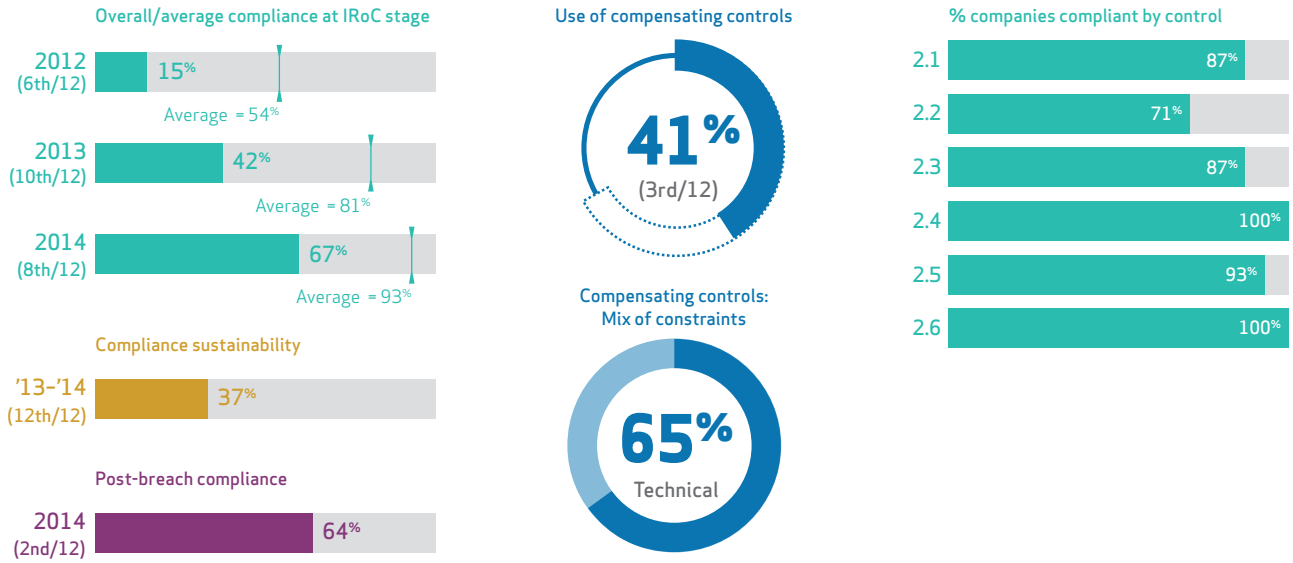
New control: 2.4 mandates the inventorying of all system components. This will help determine the DSS scope and help QSAs to select an appropriate sample size when validating compliance. This means every time a new piece of hardware or software is added, replaced, or removed, the inventory must be updated, including a description of the component and its function. Complying with this control will be challenging unless the maintenance of the inventory is automated, from task assignment through to completion, as part of the corporate change control process.

New control: 2.5 requires the policies and daily operational procedures associated with vendor defaults to be documented and communicated to responsible personnel.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 2



THE STATE OF COMPLIANCE

This year, 67% of organizations complied with Requirement 2, compared to 42% in last year's report. This shows changing defaults and systematically managing device configuration finally got the attention it deserves.

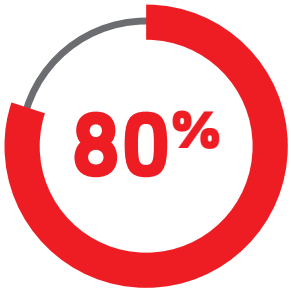
Between 2012 and 2014 just 40% of organizations that our RISK team investigated after they'd suffered a breach were found to be compliant with Requirement 2.

The only control within Requirement 2 where we saw a drop in compliance was control 2.1. In 2014 we reported that just 7% of companies that we looked at failed control 2.1 [Always change vendor-supplied defaults and remove or disable unnecessary default accounts before installing a system on the network] at IRoC. In our latest dataset that's almost doubled to 13%, indicating more companies are struggling to maintain the configuration of their system landscape.

Just 87% of organizations passed control 2.3 [Encrypt all non-console administrative access using strong cryptography] in 2014. There is no reason for so many companies to fail this control, and it simply shows a lack of process. Technologies such as SSH, VPN, and TLS are widespread and easy-to-use, and allow safe web-based access management to administrative functions.

The subcontrols in Requirement 2 that proved most problematic in 2014 were 2.2.4.c and 2.2.5.c, with just 84%, of companies passing. These concern the validation of a sample of systems meeting the documented configurations. The low compliance that we observed in this area shows how hard it is to keep the environment in line with its intended documented state and vice versa.

Vulnerabilities in obsolete technology are often blamed for data breaches, but misconfiguration of systems is actually much more likely to be the cause of a breach.



The 2014 DBIR found that four out of five breaches stemmed from authentication-based tactics, where attackers attempted to guess, crack, or reuse valid credentials.

Our forensics teams have found breached POS systems being used for other functions too, like web browsing and email. This dramatically increases the number and variety of possible attack vectors, putting the CDE at much greater risk.

CAN A VIRTUALIZED SERVER BE PCI DSS COMPLIANT?

Subcontrol 2.2.1 states that you must, "Implement only one primary function per server." This is often misinterpreted to mean that a virtualized system cannot be PCI DSS compliant. But the PCI SSC has made it clear that the intent of this requirement has nothing to do with server technologies, but is solely about limiting the impact if a specific function becomes vulnerable to attack.

The use of server virtualization is not a barrier to PCI DSS compliance as long as appropriate controls are in place to prevent a vulnerability in one virtual machine impacting the security of the others on the same server. In fact, some virtualization, especially desktop virtualization, can actually help increase security and simplify PCI DSS compliance.

COMPENSATING CONTROLS

Two-fifths of companies used one or more compensating controls as part of their attempts to comply with Requirement 2, the third highest in our study.

30% of companies were unable to pass testing procedure 2.2.2.b and used a compensating control. This is often a result of the absence of hardening options for exotic devices where unaddressed risks are mitigated through the use of additional measures. Another common justification is that business partners — even banks and card issuers — say that they can't support newer, more secure protocols.

SIMPLIFYING COMPLIANCE

Organizations tend to have hundreds or thousands of system components. Some are unique, but there will also be many very similar devices — like PCs. Any of these can have exploitable weaknesses, and securing them all individually would not be practicable. Standardization makes it possible to cost-effectively manage large numbers of devices by making it easy to spot deviations and quickly ascertain the potential impact of newly discovered weaknesses.

Without detailed hardening standards, an organization cannot possibly be sure that all components meet their standards. This baseline allows the use of tools or scripts to quickly assess if all components are configured correctly.

By defining and documenting the expected hardened configuration of each system, and adopting tools to automate, maintain and correct that configuration, organizations can validate that settings have been consistently applied and avoid exceptions caused by manual configuration. This should include a mandatory internal scan of any new system as part of the deployment process. This scan should ensure that only the bare minimum of services are enabled with only required ports open; it's easy to adjust this later if the system doesn't work. This can also help to reduce the workload involved in administering IT infrastructure, and can also reduce the cost of compliance assessments — the QSA can verify this automation and potentially reduce the size of the validation sampling.

MAINTAINING SECURITY AND COMPLIANCE

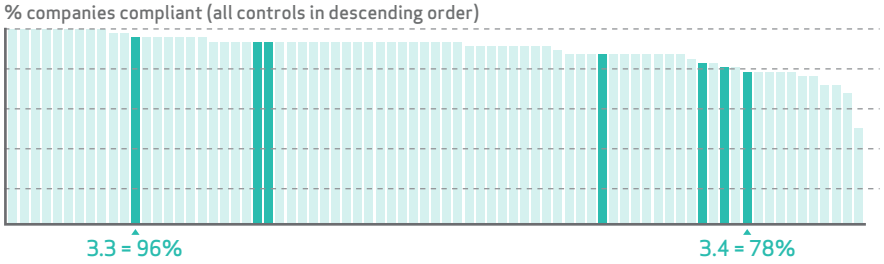
Maintaining compliance for Requirement 2 is not easy, and organizations should expect and be prepared to respond to unauthorized, unplanned and unintended changes to the configuration of systems. This requires standard configurations to be applied to every new device and continuous validation of all systems in the DSS scope. Developing robust procedures to achieve this will have a dramatic impact on the organization's security resiliency and the security of CHD within the organization.

Someone could change a firewall setting, unwittingly allowing traffic that would otherwise have been blocked. Incorrect file permissions on a server could also expose data to risk. Keeping up-to-date backups of network configurations enables the IT team to revert to a known secure configuration in the event of a problem, helping to shut down any potential vulnerability quickly and maintain compliance.

Keeping documented configurations up to date can be challenging. When a new security weakness that requires a change in the documented standard hardened system configuration is discovered, this change must be pushed out to all active systems and deployment templates. A common failing is missing systems that are not permanently online.

Protect stored cardholder data

3



This requirement covers the storage of CHD and SAD on system components, such as servers and databases. It states that all stored data must be protected using appropriate methods, no matter what type of system it is stored in. And it must be securely deleted once no longer needed.

WHY IS IT IMPORTANT FOR SECURITY?

The intent of Requirement 3 is to reduce the impact of any data breach. Sensitive authentication data (SAD), like track data, card verification values and PINs, must only be stored when absolutely necessary; and if it is stored, it be must be deleted and rendered unrecoverable as soon as the authorization process is completed.

Three simple rules:

- If you don't need it, don't store it.
- If you really need it, protect it when stored.
- If you do store it, securely delete it when you're done with it.

The loss of this sort of sensitive authentication data can be particularly damaging and costly, both in terms of remediation and reputation — this includes reissuance costs. As a result, 3.2 is one of the subcontrols that requires the most attention.

Where this sensitive data has to be stored — by those offering payment card issuing services for example — then encryption or strong hashing can dramatically reduce the risk. Should a system be compromised and data extracted, these techniques mean that without the cryptographic keys the haul will be unusable to the attacker.

Attackers often focus on compromising stored data. As reported in the 2014 DBIR, almost half (48%) of compromises involving payment card data breaches involved data that was stored unencrypted. We've also seen a shift to using RAM scrapers instead of file capturing or key loggers.

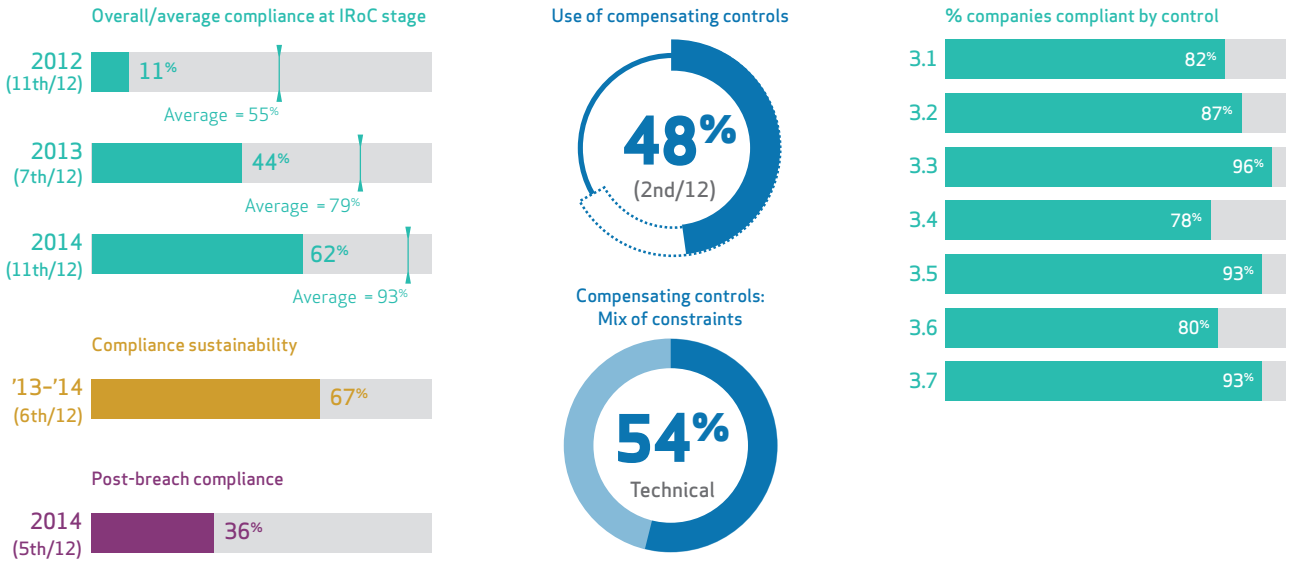
WHAT'S NEW?

The Verizon Investigative Response team has seen a significant increase in the use of RAM scrapers (see the 2014 DBIR for details). This is a form of malware that snatches data from volatile memory, that is, while it's being processed and before it has been encrypted and transmitted or stored to disk. This gets around encryption and lets attackers harvest the data in clear text. Several recent breaches in big-box retail companies have exploited this.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 3



> Don't forget to change keys if someone with knowledge of them leaves the organization.

DSS 3.0 clarifies the principles of split knowledge and dual control. Split knowledge is a method by which two or more people separately have key components, and each person knows only their own key component without any knowledge of the actual key itself. Dual control requires two or more people to perform a function, and no single person can access or use the authentication materials of another person.

Updated control: 3.2 has been updated to require that all SAD is rendered unrecoverable upon completion of the authorization process, clarifying the intent.

Updated control: 3.5 has been updated to provide additional guidance on key management, an area that organizations often struggle with. Enterprises are prone to cutting corners when it comes to properly managing encryption keys, and many encryption solutions do not include proper key management. 3.5.1 covers restricting access to keys to the minimum possible number of people, and 3.5.3 storing keys in as few places as possible.

Updated control: The subcontrols under 3.6 have been updated to ensure that best practices are followed when replacing keys at end-of-life or when compromised, and that those entrusted with managing keys understand and accept their responsibilities.

THE STATE OF COMPLIANCE

62% of the companies that we assessed were compliant with all the controls of Requirement 3 (versus 44% in 2013). This improvement is largely due to the better tools to search and find unauthorized data repositories (for example, production data found in development/quality assurance systems) that organizations have at their disposal.

However, despite this improvement Requirement 3 is the second-least well-complied with control in our study. The most common reasons for non-compliance include:

- Data held without a valid business need.
- Data stored beyond guidelines defined in official retention policies.
- Misconfigured systems unintentionally storing data.

Despite several attempts at clarification, control 3.4 remains confusing for many organizations — there are at least a dozen different variations on file encryption, database encryption, and encryption at the application layer to choose from. This is a large part of the reason for the low compliance with this control, at just 78%.

COMPENSATING CONTROLS

The use of compensating controls within Requirement 3 is very high — 48% of companies in our 2012–2014 dataset used at least one. The area where we saw a compensating control used most frequently was 3.4 [Render PAN unreadable anywhere it is stored]. The most common reasons for an organization to use a compensating control here were technical challenges with implementing encryption, such as performance degradation or incompatibility with other systems. We expect this to improve as encryption technologies have become more accessible and affordable.

SIMPLIFYING COMPLIANCE

Consider implementing P2PE solutions, tokenization, or outsourcing any processes involving CHD and/or SAD to either prevent the need to protect it, or to reduce the amount of data you need to protect.

More and more organizations are adopting tokenization as a superior alternative to traditional encryption, recognizing that it addresses the inherent vulnerability of cryptographic keys. Tokenization is based on converting sensitive data, such as PANs, into non-sensitive "tokens". It does so using a random factor, instead of encryption's repeatable formula, making it much harder to break. A hosted tokenization solution, delivered as a service, provides a flexible and comprehensive solution that protects data at rest, in use and in transit. This kind of solution is becoming more popular. Traditional tokenization is being replaced with new innovations such as vaultless tokenization and in-memory tokenization, which provides significant advantages in performance and reduced complexity. In the payment processing space, both Visa and MasterCard have tokenization platforms and services that they make available to issuers.

Database administrators (DBAs) should take ownership of the contents of all databases within the CDE. Too often this is left to the line of business owners who often lack understanding of security or the PCI DSS. DBAs should question what type of data is being placed into the database and ensure that it is secured appropriately. They should also build and maintain a comprehensive inventory of the files, tables, and other repositories that contain PAN. This would greatly simplify managing encryption and assessing compliance.

MAINTAINING SECURITY AND COMPLIANCE

Our data shows that three testing procedures within Requirement 3 are in the top 10% of those most likely to cause non-compliance during an IRoC assessment following a successful compliance assessment. These require special attention to avoid creating openings for attackers and falling out of compliance:

- 3.1.c: CHD that exceeds data retention policies must be deleted securely. For data stored in electronic form, all efforts should be made to automate the process. For data stored on other media, such as paper, a robust manual process must exist and someone must be responsible for making sure that at least every quarter any data exceeding retention policy limits is identified and securely destroyed.
- 3.6.4a and 3.6.4.b: Cryptographic keys used to encrypt CHD must be changed at the end of every defined cryptoperiod. All efforts should be made to automate this process. If this is not possible, a manual process must be in place and someone must be responsible for performing key rotations.

DISK ENCRYPTION

Full disk encryption is becoming more widely available and used — it's now built into OS X and Enterprise and Ultimate versions of Windows. It can encrypt entire disks/partitions almost transparently from users other than entering a password or token when booting the system or after a timeout. Encryption can help protect CHD held on portable devices in the event of the physical device (for example, laptop or external drive) being lost or stolen. But to be PCI DSS compliant "decryption keys must not be tied to user accounts" and it's this phrase that can cause confusion. Put simply, it means that the key used to decrypt the data cannot be connected to, or derived from, the authentication details used to access the system; the system's local user account database; or general network login credentials.

So, if a user logs in and the system automatically obtains the decryption key from a local repository — such as the keychain in OS X — then this encryption would not be DSS compliant. This setup can be compared to keeping your spare house keys under a plant pot by the door. The door may be secure, but the system is fundamentally weakened.

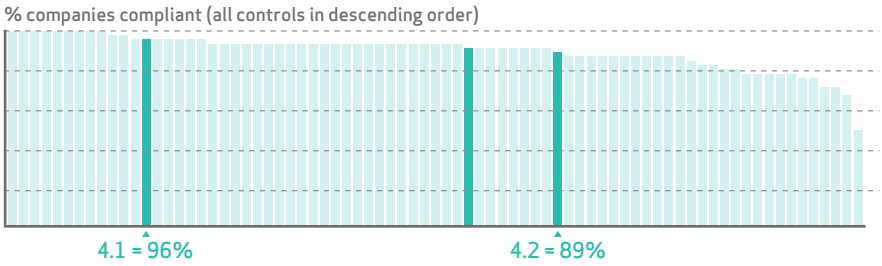
We would advise you to use:

- **Service accounts** that require additional credentials, such as a digital certificate, to access the key and decrypt the data. This simplifies account management and auditing.
- **Domain-level identity management** to reduce the likelihood of an attacker being able to exploit a misconfigured server or local administration rights.
- **Verify authorization rights** that reflect proper usage policies. Applications and databases may use domain access controls such as LDAP and Active Directory, but generally just to confirm identity. Access rights are stored locally, not inherited from the domain, and are mapped to the identity.

4

Encrypt transmission of sensitive information across public networks

This requirement is designed to protect cardholder data and sensitive authentication data transmitted over unprotected networks, such as the internet, where attackers could intercept it.



WHY IS IT IMPORTANT FOR SECURITY?

The encryption of data transmissions is a foundational information security practice, and most IT departments are familiar with how to protect common systems and applications. Requirement 4 covers communications over public/open networks, including email (whether to external parties, such as customers, or internally) and transactions made over the internet.

It is essential to use suitable data protection technology (such as secure TLS) to encrypt communications containing CHD that take place over any untrusted network, including internal ones. The term "untrusted network" includes any network outside of the organization's control, like the internet, and local "over the air" networks, like Wi-Fi and Bluetooth — even if they belong to the organization.

WHAT'S NEW?

Companies of all kinds are adopting cloud computing, and the merchants and service providers subject to PCI DSS are no exception. Cloud computing services offer many benefits, including increased agility and scalability, but as with any managed IT services, they alter the compliance landscape.

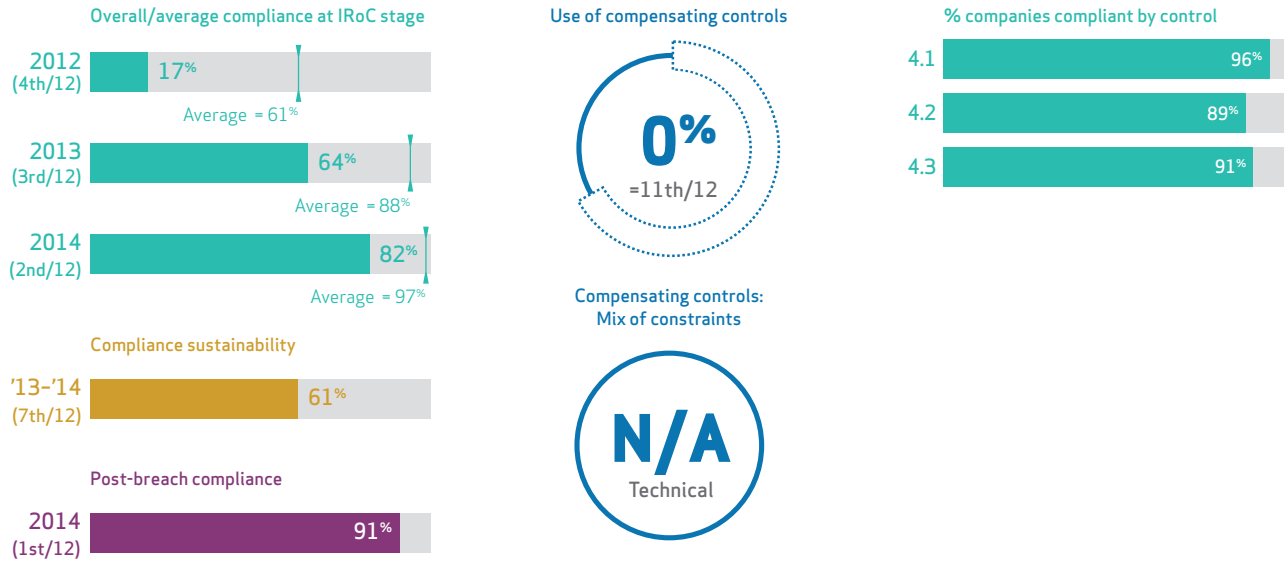
Providers can implement per-tenant, per-resource, and per-application security controls, keeping data secure despite the multi-tenant environment. Many on-premises environments rely on perimeter security as their only layer of defense and lack sufficient internal network access controls — so cloud environments can offer the same, or even better, security as their on-premises counterparts.

Organizations can protect transmitted card data in cloud environments in various ways; for example, verifying that the cloud providers segment the deployment into public-facing and private segments, and maintain encryption (or re-encrypt if necessary) until card data reaches an application server in a secure, private segment of the cloud environment.

Prior to 2013, lack of clarity caused uncertainty and concern around the requirements for protecting payment card data across cloud environments, in accordance with PCI DSS. In February 2013, the PCI SSC released the PCI DSS Cloud Computing Guidelines Information Supplement. This clarifies the security responsibilities of both the cloud provider and customer, and provides guidance for third-party cloud providers on how to secure payment data and maintain compliance with PCI DSS controls in a cloud environment.

Degree of change
Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 4



THE STATE OF COMPLIANCE

Protection of data transmitted via public networks is commonly understood and most organizations meet this requirement quite easily, for example using a strong version of TLS with sufficiently robust cipher suites and key lengths.

SSL (no matter what version) will no longer be accepted as of the upcoming DSS 3.1.

In 2014, 82% of companies were compliant with Requirement 4, versus 64% in 2013. The most common causes of non-compliance that we observed were:

- Using insecure cryptographic protocols (like SSL 2.0) or weak keys.
- Employees sending/receiving CHD in clear text via email.

COMPENSATING CONTROLS

None of the companies that we studied used a compensating control for Requirement 4.

SIMPLIFYING COMPLIANCE

Sometimes people do not realize that sending CHD in clear text via email, even just internally, not only puts the email server in scope but potentially every user's computer and all other connected systems too. Accepting payments by email makes it even more challenging, if possible at all, to comply with this Requirement. Both are bad practice and should be avoided in order to improve security and simplify compliance.

97.8% of organizations in our 2014 dataset complied with control 4.1.1 [Ensure wireless networks transmitting CHD or connected to the CDE, use industry best practices]. Setting up a secure VPN that your employees can use to connect to your organization's servers makes complying with this control very easy. This enables employees to work on the road without exposing your business or themselves to any of the risks commonly associated with public Wi-Fi connections.

Organizations can simplify DSS compliance using appropriate technology solutions to control, monitor and secure data and documents that contain CHD.

In February 2015, the SSC issued a worldwide notification that a revision to the PCI DSS and PA-DSS v3.0 standards will be released to address weaknesses that were identified in the Secure Socket Layer (SSL) v3.0 protocol.

CLOUD AND COMPLIANCE

Security and compliance concerns are commonly cited as the top barrier to adoption of cloud. While there are technical considerations, as we mentioned in last year's PCI Compliance Report, the main challenge is in dividing responsibilities for security and compliance clearly between the provider and the customer. Assumptions can be fatal, and ultimately customers should remember that they retain overall responsibility for compliance with data-related laws and regulations. The answer is rigorous governance that identifies the data that will be hosted in the cloud and which regulations affect it, protects it appropriately (for instance through encryption), and monitors security and compliance through detailed reporting.

MAINTAINING SECURITY AND COMPLIANCE

Most attackers know that most CHD that's now sent over open/public networks is usually well protected and so they go after softer targets. None of the breaches reported on in our 2014 Data Breach Investigations Report involved data "in transit". But complying with this Requirement is relatively simple and is important to maintaining data security.

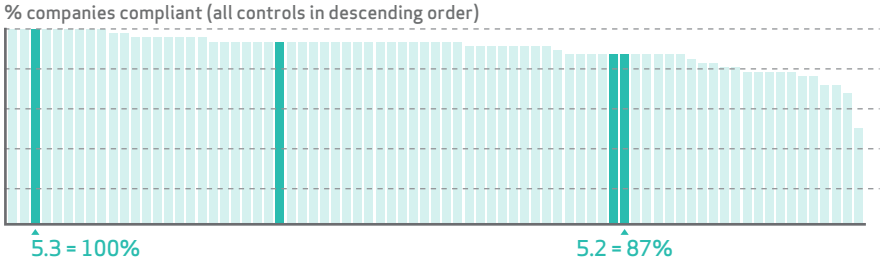
A common problem that we see is failing to keep up with encryption standards. The computing power available to hackers is constantly growing, making once secure passwords now easy to crack. We still often see companies using WPA2 with pre-shared keys (PSK) to protect their wireless networks, but this can now be broken in just a few minutes if the passphrases are not strong enough. If you're still using WPA2-PSK you should consider moving to WPA2 with enterprise mode (802.1X) for all wireless networks in scope as soon as possible.

Many organizations think that maintaining compliance with Requirement 4 is not much more than some patching and testing. This overlooks the complexity of continuously keeping webservers up to date with the latest certificates and encryption settings. The Heartbleed and POODLE incidents in 2014 highlighted the importance of not just updating encryption settings and key sizes, but also keeping webservers and libraries included in the webservers themselves up to date too.

Just keeping track of the updates can be a challenge. Administrators should monitor security newslists and be prepared to act quickly.

Use and regularly update anti-virus and malware protection

5



This requirement concerns protecting all systems commonly affected by malicious software against viruses, worms, and trojans.

WHY IS IT IMPORTANT FOR SECURITY?

Attackers can use malware — malicious code — to gain a foothold in the environment, capture CHD, and damage systems; so it's important for organizations to protect all systems in the DSS scope with anti-virus software.

Requirement 5 demands that anti-virus software is not only in place, but also that it is kept up to date; is capable of detecting, removing, and protecting against all known types of malware; generates audit logs; and that scans are performed regularly.

WHAT'S NEW?

DSS 3.0 requires organizations to use anti-virus and anti-malware software and keep it up to date. But traditional signature-based anti-virus technology is no longer effective, even when kept updated: thousands of new malware variants appear each day. Anti-virus vendors are adopting a layered approach that also draws on heuristics, cloud-based threat intelligence, sandboxing and other approaches to broaden the protection they offer. While client-based anti-virus installations are still important, organizations are increasingly relying on firewalls and other dedicated security infrastructure to block malware, and also to focus on mitigation — recognizing that some malware will always slip through, so the answer is to work to minimize the damage it causes.

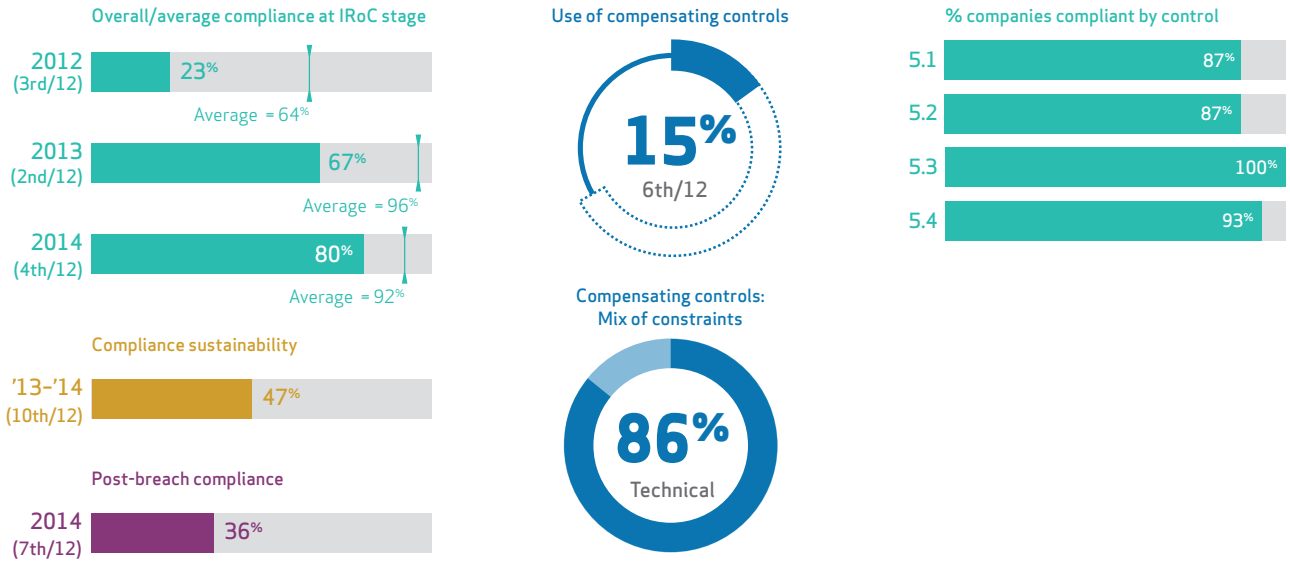
Anti-virus technology has evolved into endpoint security solutions that offer greater protection, including host IPS (HIPS), firewall, profiling based on network location, network access control (NAC), and file integrity monitoring.

The latest version of the standard clarifies where anti-virus must be used. The wording of the standard is that anti-virus solutions should be installed on all systems commonly affected by malware. In the past some companies have interpreted this to only apply to Windows-based systems. The standard now stipulates that organizations must have a process in place to "identify and evaluate evolving malware threats" for all systems that were excluded in this way. This should help to significantly reduce the risk of attackers targeting platforms that have been considered not to be at risk of malware in the past.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 5



Modern malware is polymorphic, constantly changing to evade detection — like a spy slipping on a disguise. Signature-based technologies — like traditional anti-virus, anti-malware and intrusion detection systems — which work by matching characteristics of threats, are largely reactive and do not provide adequate protection. Unfortunately, many companies — even large enterprises — still rely on these flawed technologies.

There have even been cases of malware being adapted to specifically target an individual organization.

New control: 5.3 stipulates that the anti-virus solution runs constantly and can't be disabled by users — with exceptions formally authorized on a case-by-case basis.

THE STATE OF COMPLIANCE

Requirement 5 was the only one of the 12 where we saw a drop in average compliance, from 96% to 92%. Only a small fall, but against the backdrop of a significant increase.

Control 5.1 addresses the coverage of the anti-virus solution and examining that it is doing what it is supposed to. Although still far higher than in 2012, compliance fell between 2013 and 2014. The first of the two testing procedures where an examination of the configuration is needed has the lowest passing score in Requirement 5, just 87%. The second, where only an interview is needed, has compliance of 100%.

Many organizations find complying with control 5.1.1 [Ensuring that anti-virus is capable of detecting, removing, and protecting against all known types of malicious software] challenging because it requires:

- Supporting multiple platforms — malware isn't just a Windows problem.
- Extending protection to systems and devices outside of the corporate network.
- Protecting data held in the cloud and on off-network devices.

Most organizations now realize the need to switch to unified platforms with next generation tools. These solutions enable organizations to take an integrated approach that can protect many kinds of devices, including desktops and mobile devices.

In 2014 we saw cross-platform malware in the wild for the first time. Typically written in Java, this can infect systems running Windows, Mac OS X, and Linux. It's no longer valid to think that malware is just a Windows problem.

Control 5.2 covers maintaining the anti-virus solution: installing updates, performing periodic scans, and generating and reviewing logs. Organizations have come a long way from 2012 when compliance was just 36%, though it fell slightly from 89% in 2013 to 87% this year.

COMPENSATING CONTROLS

Compensating controls are used for two parts of Requirement 5, controls 5.1 and 5.2. The main reason for using a compensating control for control 5.1 is a technical problem with the installation of the anti-virus affecting the operation of another application. A compensating control is used for control 5.2 just one-sixth as often as 5.1. Similarly, the main reason for using a compensating control is that the periodic scans adversely affect the performance of another application.

SIMPLIFYING COMPLIANCE

The malware threat has been on the horizon for a long time, and so have the solutions to address it. Previous versions of PCI DSS only specified that anti-virus software should be in place, that it be kept up to date, and that it generated logs. DSS 3.0 adds the stipulation that the user must not be able to disable it. To comply with this many organizations will have to update or even replace their anti-virus software and OS configurations. Rolling this sort of change out across a large estate of devices may prove challenging and should be planned for well in advance.

MAINTAINING SECURITY AND COMPLIANCE

If a suitable anti-virus solution is deployed properly — scheduled to run regularly, generates logs, and is set to update automatically — then nothing special needs to be done to maintain it other than to review logs at least once a day. Systems which are susceptible to malware that don't support anti-virus software must be protected by other security software that detects strange activity — examples include rootkit hunters and sudo alerts.

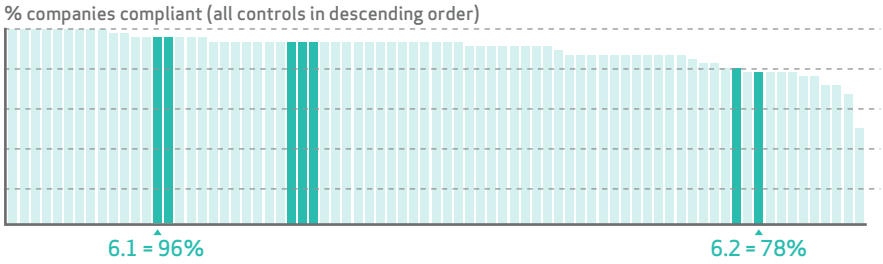
Ideally the use of advanced security solutions should be hassle-free, and transparent to end-users during normal operation. The integration of anti-virus and other endpoint protection solutions with next-generation firewalls provides enhanced enforcement capabilities at application level with inline protection. This eliminates the need to fit multiple endpoint solutions, reduces overall maintenance — with one integrated appliance replacing multiple standalone products for malware filtering, intrusion prevention, URL filtering, traffic decryption etc. — and cuts the number of times traffic needs to be inspected, resulting in increased performance.

To meet PCI DSS, anti-virus software must be configured to detect any known virus or malware and produce logs (network and system) that security teams can use to detect and investigate attacks.

6

Develop and maintain secure systems and applications

This requirement covers the security of applications, and particularly change management. It governs how systems and applications are developed and maintained, whether by the organization or third parties. It recognizes that the threat landscape is always changing, and compliance measures need to be adapted accordingly.



WHY IS IT IMPORTANT FOR SECURITY?

Requirement 6 plays an important part in helping maintain security posture by:

- Managing and documenting changes in the DSS scope.
- Using secure development practices for all applications in the DSS scope: whether traditional or web-based, and whether developed internally or by third-party developers.
- Preventing and testing for known weaknesses and common design or coding flaws.
- Identifying vulnerabilities and remediating against them by applying security patches.

Unless you know what's in the environment at any point, it's impossible to assess risk accurately. DSS 3.0 makes it clear that change management applies across the board. This ties back to the new control 2.4 that stipulates maintaining an inventory.

Investigations by our RISK team found that only 16.4% of organizations that had suffered a data breach were compliant with Requirement 6, compared to an average of 64% of organizations assessed by our QSAs in 2014.

Patch management can be a major headache for an enterprise, that's why they often delay updates and upgrades for as long as possible — some still run Windows XP!

WHAT'S NEW?

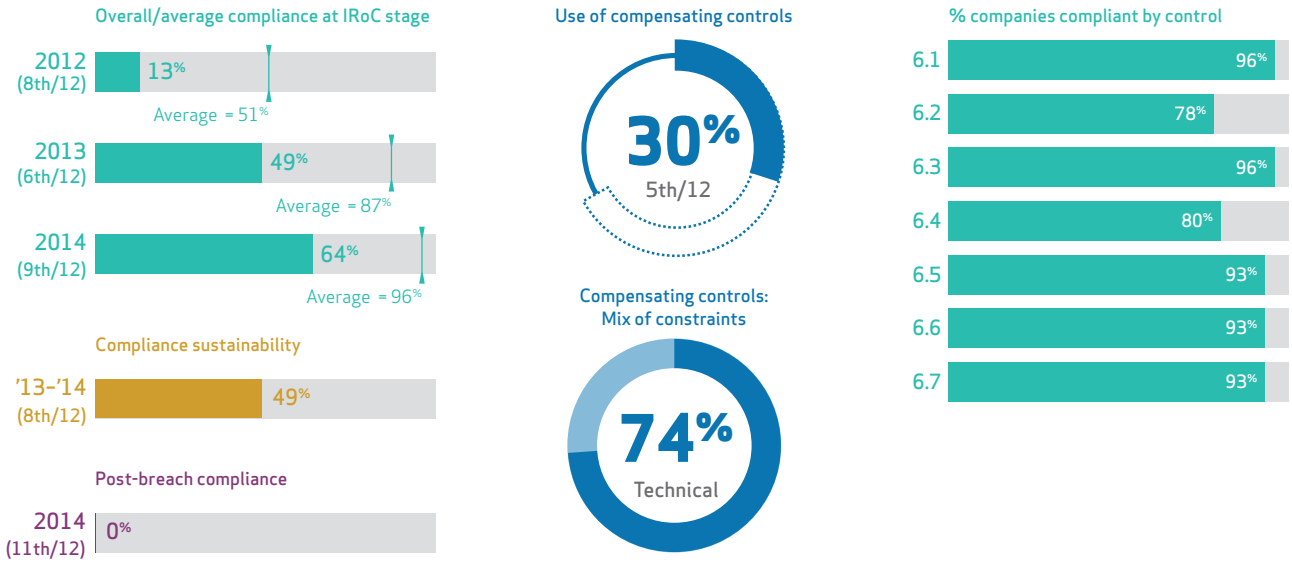
Requirement 6 was updated significantly in DSS 2.0 and again with the release of version 3.0. The overall wording of the Requirement changed to clarify that all applicable systems, not just critical ones, must have all appropriate patches applied — this will significantly increase the amount of effort required for organizations that did not understand this before. But requirement 6.2 also now includes a more risk-based approach allowing an organization to determine criticality in relation to their own specific environment.

Updated control: 6.1 has been updated to specify that organizations must establish a process to identify security vulnerabilities and then apply a risk and threat ranking to those vulnerabilities. To be effective, a vulnerability management solution should identify new software and infrastructure vulnerabilities in near "real time". Relying on static vulnerability data is not sufficiently effective.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 6



Updated control: 6.3 covering the secure handling of CHD in memory, reflecting the increasing number of attacks targeting data at the time of processing.

Updated control: 6.4 now makes it clear that change management applies to all changes to all system components, not only during software development and maintenance.

New subcontrol: 6.5.10 sets standards for web development practices, session control and timeouts, and testing of web applications that handle card data to reduce the probability of "man-in-the-middle" and client-side attacks.

Updated control: 6.6 has been rewritten to provide clarity on the two methods of complying with this requirement and more flexibility in choosing a technical solution to detect and prevent web-based attacks

THE STATE OF COMPLIANCE

Compliance with the controls within Requirement 6 has been rising since 2012, and this is really a good thing. Our RISK team found that less than one in 6 companies that suffered a breach were compliant with Requirement 6.

6.1, covering ranking new vulnerabilities using a consistent process, and 6.3, relating to secure development processes, have improved from under 50% in 2012 to 96% in 2014.

6.2, which addresses the need to implement patches and updates within specified timeframes, and 6.4, covering change management, have increased more than 2.5 fold, from 30% in 2012 to 78/80% in 2014. This shows that organizations have significantly improved their patching and change management processes. As the ability to consistently implement updates in a controlled manner implies having strong change-management processes, it makes sense that these are increasing together.

Compliance with 6.5 and 6.6 has also been increasing, reaching 93% in 2014. For 6.5, software developers should receive frequent training in secure coding techniques to know how to avoid common coding vulnerabilities — and in particular how sensitive data should be handled in memory. As for 6.6, fewer organizations are confusing their traditional network layer firewall, (which does not inspect traffic at the application layer) with Web Application Firewall (WAF) functionality — which can be a dedicated appliance, a device plug-in, or any other solution that detects and prevents web-based attacks.

> With customers expecting ever richer and more responsive websites and applications, and IT striving to deliver real-time insight, the use of in-memory technology is growing rapidly. As ever, hackers have been quick to spot the opening that this offers, and we've seen a significant increase in malware that can scrape data from memory.

SCORING VULNERABILITIES

The PCI DSS has included the need for using a documented risk rating process since 2012, it's now within 6.1.

It stipulates a process based on a "reputable outside source" — for example the Common Vulnerability Scoring System (CVSS) from the Forum of Incident Response Security Teams (FIRST). Is should also take into account the actual assessed risk of vulnerabilities as they apply to the specific environment. We believe that this contributed to the significant improvement in compliance with this requirement.

Some commentators have suggested that DSS 3.0 sets different expectations for internal and external scanning — as requirements for internal patching and vulnerability scanning talk about "High", "Medium" and "Low" risk (6.1 and 11.2.1), whereas external scanning needs to ensure that no CVSS scores of 4.0 or higher are detected (11.2.2).

In fact, the only difference is that the PCI SSC errs on the safe side for externally facing vulnerabilities — by setting the bar at anything rated as CVSS 4.0 or higher — while allowing organizations to address internal risks in line with their own specific situation. So if the internally documented and implemented processes shows a vulnerability with a CVSS of 4.0 is in fact only a medium or low risk in the specific situation, it can be addressed as such. But this also works the other way around. A vulnerability commonly regarded as a low risk, might be a high risk in an organization's specific internal environment.

COMPENSATING CONTROLS

Only two testing procedures forced the use of a compensating control, both concern the validation of the installation of patches. 6.2a (27.8%) deals with the policy and 6.2b (20.6%) the actual installation.

There are three main reasons for struggling to pass these procedures: technical constraints on installing patches in the stipulated time, business risks in installing patches, and limitations on installing patches caused by legacy systems.

SIMPLIFYING COMPLIANCE

Change control is one of the "gatekeeper" processes that helps maintain overall PCI DSS compliance. Both the DSS scope and threat landscape are in constant flux, with new implementations, processes, attack vectors, and vulnerabilities emerging.

To maintain the compliance status of the DSS scope, the organization must ensure that changes to systems or business processes do not impact existing DSS controls, and that any new systems integrate current security controls before going into production. These controls include incident response, log monitoring and reporting, access control, patch management, and malware management.

- Control 6.1 addresses identification and risk rating of security vulnerabilities and 6.2 the installation of patches. These controls should be considered in tandem. An organization needs to look into the identification and patching of vulnerabilities, and for such activity, a schedule based on Patch Tuesday could be considered.
- Control 6.3 covers the secure development of applications. The best way to maintain this control is a triggered approach, rather than a timed one. A checklist is a useful way to help make this control resilient.
- Control 6.4 addresses change management. A single mismanaged change request could make an entity non-compliant. Organizations should conduct internal audits to identify the current status, followed by corrective actions, if needed.
- Control 6.5 addresses common coding vulnerabilities. Regular training develops the potential to reduce such vulnerabilities.
- Control 6.6 covers addressing new threats and vulnerabilities on an ongoing basis for public-facing web applications. The associated reviews are to be conducted at least annually and after any change, unless WAF-type protection was chosen.
- Control 6.7 seeks dissemination of security policy. Surprise checks could be conducted to establish the current status, followed by ensuing corrective actions, if needed.

MAINTAINING SECURITY AND COMPLIANCE

The irony is that, as onerous as this patching requirement is, the effectiveness of Requirement 6 in terms of actually closing vulnerabilities depends largely on the responsiveness of third-party software and hardware vendors in releasing patches in the first place. An organization may be both compliant and still at risk if a vendor does not release a patch for a known vulnerability.

Organizations may find it challenging to maintain effective vulnerability management when an application or operating system reaches end-of-life and the vendor withdraws support. Relying on compensating controls to ensure effective data protection should only be a temporary solution, as the constraint will be invalidated once the upgrade has been installed. Updating to a more recent release or alternative software often offers a more robust and sustainable solution, and usually provides better ROI.

To protect all systems within the DSS scope, organizations must be proficient at obtaining the most recent relevant vulnerability information and scan their assets to uncover and address vulnerabilities. This requires organizations to actively maintain an inventory of system components and to identify and prioritize vulnerabilities. This can only be achieved by automating the process using an appropriate vulnerability management system.

Companies that do not have a comprehensive and highly automated vulnerability management program integrated with change control in place tend to find it more challenging to achieve success in maintaining compliance with Requirement 6.

DSS 3.0 states that all systems should have applicable vendor-supplied patches installed within an appropriate timescale according to prioritized risk, with critical patches installed within one month of release.

Complying with the patching requirements is not an easy task, doing so requires:

- Reading vendor security bulletins.
- Reviewing every reported patch and associated vulnerabilities.
- Analyzing the associated risks and deciding whether to patch or not.
- Testing implementation, reviewing results and considering potential impact.
- Making go/no-go decisions.
- Planning and implementing roll-out of a patch, or mitigation.
- Validating installation.
- Remediation in case of a problem.

And all within the usual constraints on time and money. Testing the impact of all patches to ensure they do not create new problems is labor intensive, and replicating the exact production environment so tests can be done without any risk to operations is usually also cost-prohibitive The trend to move applications into the cloud could help companies to implement patches more quickly and effectively, either by leveraging the expertise of their cloud provider or using the cloud to spin-up a test environment quickly and cheaply.

As always, reducing the size and complexity of the DSS scope should be the first step to reducing the patching workload.

Patch management and associated vulnerability management processes represent the biggest problem areas, because they're rarely well-documented and automated. Many weaknesses are only picked up during vulnerability scanning as part of Requirement 11, which means organizations are always playing catch-up.

Organizations must test patches for compatibility with systems and controls already in place before applying them to potentially thousands of devices, such as an estate of POS terminals across retail stores. This can be a significant challenge.

WEB APPLICATION FIREWALLS

There are many ways to corrupt the normal behavior of an application in order to access secure data or systems, including SQL injection, XSS attacks and LDAP injection. This sort of attack is invisible to traditional anti-virus software and simple stateful-inspection firewalls.

While vulnerabilities identified during a scan are not fixed, but are still known, management is accountable.

This makes the adoption of secure coding techniques critical. Web application firewalls (WAFs) can also help address this threat by detecting many of these common exploitation techniques. They help prevent the identified vulnerabilities from being exploited eliminating the accountability issue, giving the company time to fix the code.

IT TAKES TIME

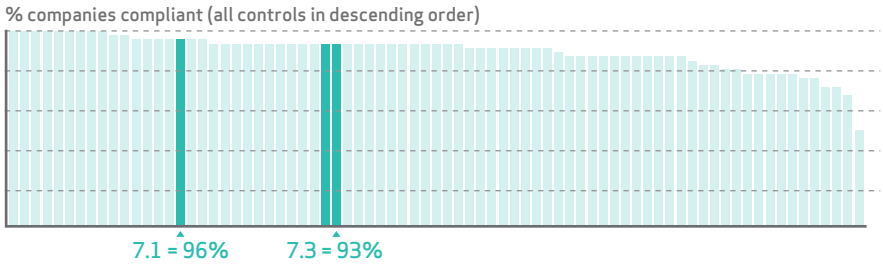
It can take months to fix vulnerabilities in applications:

- Identifying the issue can take time.
- The source code may not be readily available or understood.
- The original developers may no longer be available.
- Coming up with a workaround can take a lot of expertise.
- The languages used may no longer be in common use.
- Fixes can introduce new vulnerabilities.

7

Restrict access to data by need-to-know

This requirement specifies the processes and controls that should restrict each user's access rights to the minimum they need to perform their duties — a "need to know" basis.



WHY IS IT IMPORTANT FOR SECURITY?

User accounts are often a target for cybercriminals and employees with malicious intentions. Every user account with access to a system within the DSS scope is a potential security risk. The more people granted access, the bigger the target you offer to attackers, and the greater the risk of accidental or deliberate misuse by staff. Access should be limited on the basis of "need to know" or "least privilege," giving each individual the minimum privileges and access to data required to perform their role. PCI DSS stipulates an access control system for each element of infrastructure. This should include frequently overlooked systems managing physical security controls, like badge readers.

WHAT'S NEW?

Requirement 7 remained fairly static between DSS 1.2.1 and DSS 2.0, just two controls were updated. But this Requirement received a lot more attention in the move to DSS 3.0.

New control: 7.1.1 has been added to cover the definition of access needs for each user role, an important fundamental step.

Updated control: 7.1.2 has been updated to focus on the restriction of privileged user IDs to least privileges necessary and includes enhanced testing procedures.

Updated control: 7.1.3 has been refocused on assignment of access based on an individual's job classification and function.

THE STATE OF COMPLIANCE

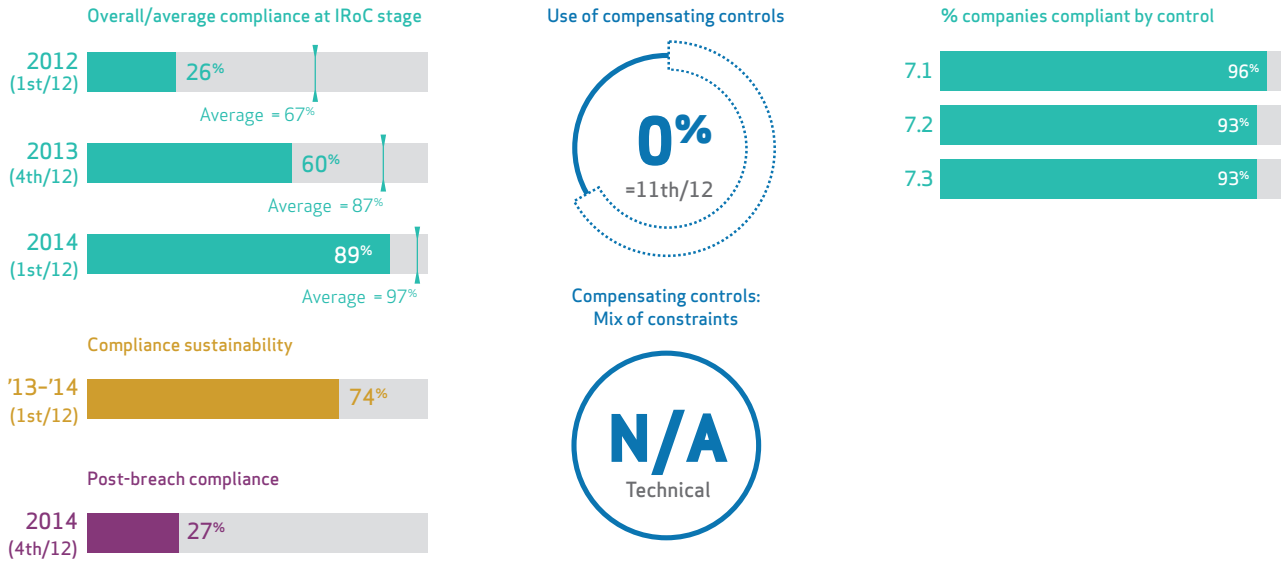
Compliance with Requirement 7 was already quite high, it was fourth in our report last year. Since then we've seen a significant increase to 89%, making it the most frequently complied-with Requirement in our 2014 dataset.

96% of companies were compliant with 7.1 [Limit access to system components and CHD to only those individuals whose job requires such access], an increase of 16pp on 2013.

Last year, 7.2 [Establish an access control system for systems components that restricts access based on a user's "need to know", and is set to "deny all" unless specifically allowed] was the best performing control within Requirement 7, perhaps partly explaining its relatively small improvement. In 2014, 93% of companies were compliant, an increase of 9pp on 2013.

Degree of change
Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 7



COMPENSATING CONTROLS

None of the companies that we assessed in 2014 used a compensating control for Requirement 7. It's hard to think of a justifiable reason why you can't implement an access control procedure to grant access depending on job role, as access control is built into most modern systems and it's quite easy to write policies.

SIMPLIFYING COMPLIANCE

The proliferation of mobile devices, bring-your-own-device (BYOD) policies, wireless networking, and cloud-based services have made enforcing access control much harder. These trends seem unlikely to abate, so companies must change how they manage access control; changing workflows and taking advantage of some of the new tools now available.

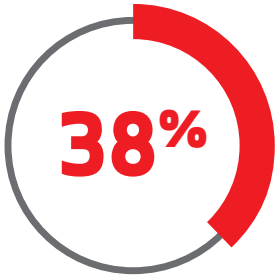
The latest network access control (NAC) solutions offer the ability to set granular policies around all users, devices, configurations and applications, and ensure that endpoints are in compliance before access is granted and can take remedial action if it is not. In our experience there's a clear correlation between using this sort of solution and being able to demonstrate the required visibility and reporting to comply with Requirement 7, especially in large organizations.

MAINTAINING SECURITY AND COMPLIANCE

In order to ensure consistency and deal with changes caused by recruitment and employee termination, it is essential that access management is automated, based on well-defined roles, and enforced across all components in the DSS scope. Roles themselves should be structured to ensure separation of duties.

Our QSAs often find many different access control procedures and policies for different platforms, despite significant overlap. We suggest that you use the same access control procedures and software across platforms wherever possible to simplify this task.

Another common mistake is treating a virtualized environment the same as a traditional one. Virtual machines and their related storage and networks often require unique security controls. Applying the same concepts of users, groups, roles, and permissions can lead to problems if perceived default separation of duties between infrastructure and system/application management are not reconsidered.



According to the 2014 Data Breach Investigations Report, 38% of POS hacking attacks involved stolen credentials.

There are four simple rules that make complying with Requirement 7, and maintaining security, easier:

- **Default to deny all:** wherever possible set the default access to none.
- **Grant access based on role:** implement a role-based access control (RBAC) model, as this is much easier to manage.
- **Grant least privilege:** give people the minimum possible access required to perform their job.
- **Enforce:** make sure that the process for managing identities and changes in authorization is consistent, well-documented and as simple as possible.

It is essential that organizations be proficient at identifying all users that access components in the DSS scope. All applications and their locations should be known, recorded, and maintained. You should periodically review effectiveness, for example, by reviewing logs to identify which users:

- Tried to log on to critical systems or CHD repositories, but were unsuccessful.
- Were able to successfully log on to a system within the DSS scope and access sensitive resources that they shouldn't have been able to.
- Were recently given increased authorization or direct access to CHD.

The accumulation of access privileges beyond what an end user needs to do his job is known as "privilege creep" and is a common problem in organizations of all sizes. It often occurs when an employee changes jobs within an organization and is granted new privileges. They may continue in their old role for several weeks, or even months and retain their former privileges.

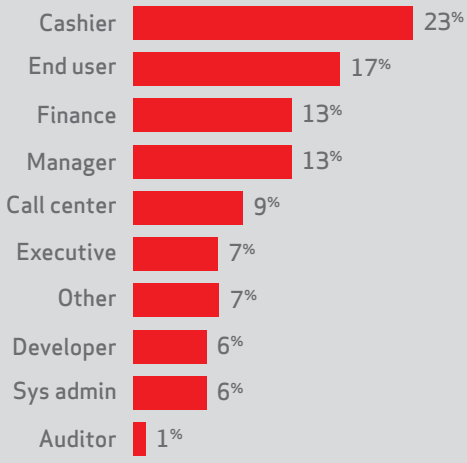
Unless security administration procedures are firmly monitored and controlled, it will result in an unnecessary accumulation of access privileges, including access to sensitive systems and components within the DSS scope. Organizations should maintain periodic access rights reviews to ensure privileges are revoked in a timely manner. The use of an identity and access management system can facilitate and simplify this process.

INSIGHT FROM THE VERIZON DATA BREACH INVESTIGATIONS REPORT

The 2014 Verizon Data Breaches Investigation Report (DBIR) stated that 88% of threat actions within the insider misuse category involved privilege abuse:

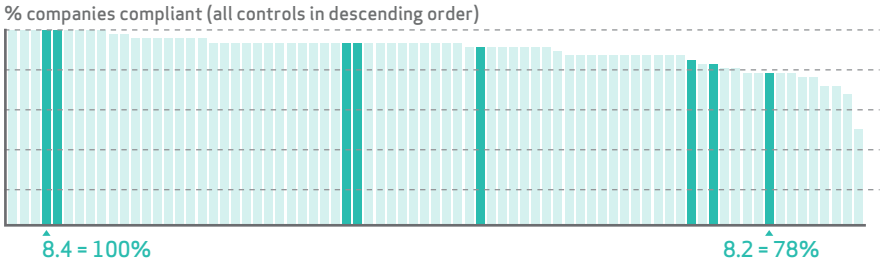
The DBIR found that very little insider misuse is through accounts which require high-level access. The RISK team saw more breaches exploiting the accounts of cashiers and call center operatives than developers or system administrators. There are a number of reasons for this, including:

- Higher turnover of staff.
- Lower security awareness, leading to poor security procedures and vulnerability to tactics like social engineering.
- Poor policies, such as shared accounts.



Identify and authenticate access to system components

8



This requirement sets standards for managing user identities and authentication methods, including passwords. Before DSS 3.0, it was called "Assign a unique ID to each person with computer access".

WHY IS IT IMPORTANT FOR SECURITY?

Assigning individual user identities is a vital part of ensuring that only the right people have access to sensitive data and systems, and that a clear audit trail can be established. Shared accounts make it very difficult to restrict and monitor access to individuals by "need to know". Organizations need accountability: only when each individual has a uniquely identifiable account can the organization determine exactly who has been accessing systems and data — a key first step in tracing how a breach happened.

Being held accountable increases users' awareness of the value of their credentials and privileged access, meaning they will be more likely to proactively act to protect it.

Authentication credentials, particularly passwords, are a prime target for attackers. Passwords can be lost or stolen, and weak ones can be cracked easily using brute-force methods. This Requirement sets standards for password strength, covers use of other authentication credentials such as two-factor authentication (particularly for remote access), and helps protect systems against password cracking attempts (for example, by limiting login attempts). It also governs how user credentials are protected at the time of use, during transmission, and in storage.

WHAT'S NEW?

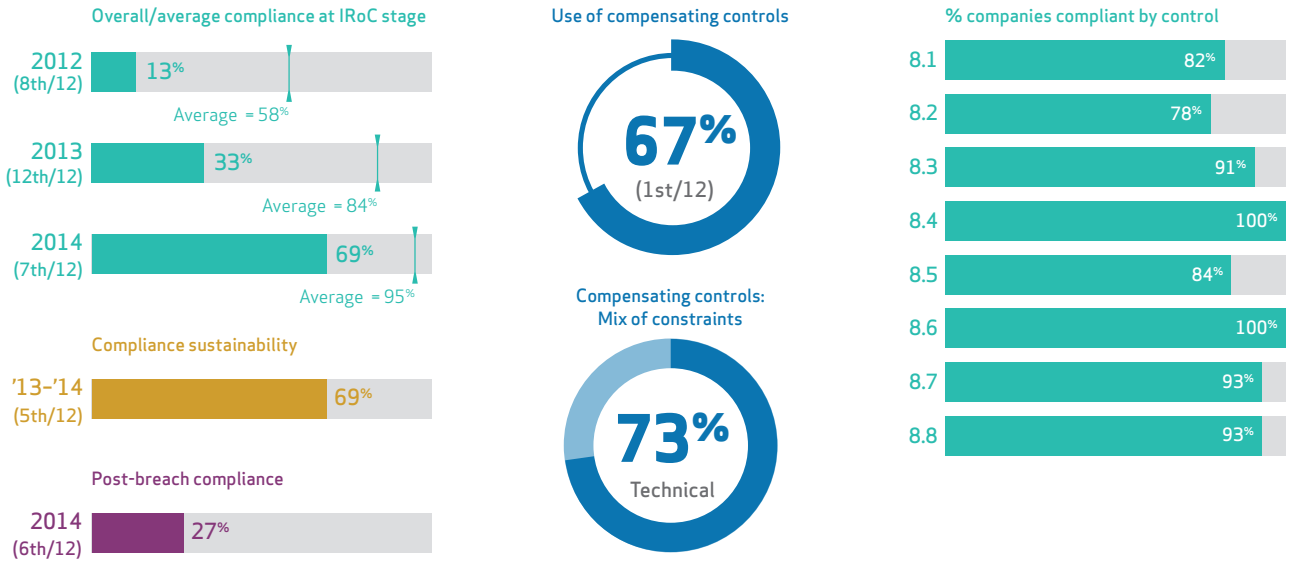
This Requirement changed significantly in DSS 2.0 and again in DSS 3.0. Most noticeably, it was renamed to reflect the full scope of identification and authentication management.

The changes to the Requirement 8 controls in DSS 3.0 align issues between control requirement and validation testing procedure. They provide much of the needed flexibility in authentication, and broaden the requirement to cover a wider range of scenarios to reflect the modern view that passwords are often an inadequate way of authenticating secure access. This will benefit organizations that have already moved, or are considering moving away from merely using passwords for authentication. Changes include:

- References to passwords have been changed to "authentication credentials" throughout.
- Identification and authentication have been split into separate controls.

Degree of change
Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 8



Updated control: The minimum password complexity and strength requirements have been combined into subcontrol 8.2.3, increasing the flexibility to use alternatives.

New control: 8.5.1 (a best practice until July 1, 2015) requires service providers to use unique credentials for each customer. In the past many third parties that employed remote access to provide services, like POS systems or IT support, used the same credentials for multiple customers. This control will reduce the risk that the compromise of one company will lead to many organizations being breached.

Updated control: 8.6 now includes other authentication mechanisms, such as certificates, physical security tokens, and smart cards. This control stipulates that where alternative authentication mechanisms are used, they must be linked to an individual account and ensure that only the intended user can gain access.

Regardless of the authentication mechanism(s) used, credentials must be linked to an individual account and only provide a single user with access.

THE STATE OF COMPLIANCE

Compliance with this Requirement has been growing steadily, rising from 13% in 2012 to 69% in 2014. The two controls where some companies still struggle are 8.2 and 8.5.

We saw significantly lower compliance with testing procedures for 8.2.4 [Change user passwords/passphrases at least every 90 days] that applies to all organizations, 88.9%, compared to the second part that only applies to service providers, 97.8%. Enforcing the changing of passwords every 90 days is unlikely to be a popular move, but it is an important way to prevent some of the most common forms of attack.

Security awareness, covered in control 12.6, will help and should be used to give employees tips for creating secure but easy to remember passwords. It will also help users to understand the value of their credentials and thus increase their willingness to comply.

Remote access vulnerabilities continue to be a primary cause of data breaches, especially for brick-and-mortar merchants.

The testing procedure that companies struggle with the most in Requirement 8 is 8.5.a [For a sample of system components, examine user ID lists for shared IDs/passwords]. Just 84.4% of companies passed this at IRoC stage in 2014, putting it just outside the bottom 20. Shared IDs and passwords are a major danger, letting hackers turn the compromise of a minor, and relatively unsecured system, into a major breach.

COMPENSATING CONTROLS

More companies used a compensating control for Requirement 8 than any other in our study. Within our full three-year dataset, the requirements that were most likely to lead to a compensating control being used were:

- Control 8.2.1 [Making passwords unreadable during storage and transmission] often required compensating controls due to technical constraints on the implementation of secure alternatives to Telnet and FTP on some systems. In most cases, it involved systems that did not support the implementation of secure protocols, which required the organizations to apply additional controls to meet the intent of security identification and authentication.
- Control 8.5 [Do not use group, shared, or generic IDs, passwords, or other authentication methods] is also compensated for fairly often by organizations that are unable to avoid using shared user IDs and share accounts for various operational reasons.

The remaining requirements in the mix of compensating controls under Requirement 8 include constraints around password and authentication requirements, such as minimum password length, limiting repeated access attempts, and system lock out durations, which were commonly compensated requirements under PCI DSS version 2.0. It is therefore not surprising that most of these controls have been revised under DSS 3.0.

SIMPLIFYING COMPLIANCE

Managing large estates of assets held by far-flung employees isn't easy. Then you've got the problems of outsourced IT, with vendors and service providers requiring access. Even enterprises with strong identity services struggle when storefront networks effectively prohibit central directory services, creating islands of devices beyond the reach of enterprise authentication services.

To simplify compliance with Requirement 8, organizations should implement a privileged identity and access management program (PAM), supported by appropriate solutions to automate and control the process — for example, using privileged identity vaults. Combining PAM with single sign-on and two-factor authentication solutions can simplify account administration and provide far greater oversight.

MAINTAINING SECURITY AND COMPLIANCE

Enforce password policies

Make absolutely sure that all passwords used for remote access to POS systems are strong. We often see factory defaults, the name of the POS vendor, a dictionary word and other weak credentials used. If a third party handles this, insist that a strong password is used, and verify it. And ensure that they don't use the same credentials for multiple customers. PCI DSS requires regular checks of IDs and passwords for remote access and database access —looking for passwords that aren't strong enough and shared credentials.

Implement identity access management (IAM)

Robust IAM policies are needed to ensure that users are given personal identification, strong passwords, and that controls and processes are in place for provisioning, decommissioning, and detecting unusual activity. The use of an IAM solution, although not specifically required for PCI DSS compliance, will help speed up the identification of compromised accounts and remediation.

WHY PASSWORDS ARE BROKEN

Back in 2004 Bill Gates exclaimed: "Passwords are dead." If only that were so. It's been well known since before computers even existed that human beings are not good at remembering long strings of random characters — most people struggle to remember how many m's there are in accommodation. Little wonder then that studies regularly show that the most common passwords — when users are given free rein — are things like "123456" and "password".

Some users think that they are being secure by doing things like replacing o's with 0's and I's with 1's; they aren't. Hackers are well aware of techniques like this, and many common hacking tools include an option to try these substitutions.

There are things that users can do, such as using the initial letters of a line from a song or poem, for example Iwsywilh4gl0n ("I want security, yeah; without it I had a great loss, oh now", "Security" by Otis Redding). But even this will only slow hackers down a little. Two-factor authentication with tough lockout policies [8.1.6] is a much better solution.

TWO (DIFFERENT) FACTOR AUTHENTICATION

You're probably very familiar with the different types of authentication:

- Something you know: like a password.
- Something you have: like a one-time password generator.
- Something you are: biometrics like fingerprint or retina scan.

Multi-factor authentication — two is common and specified by DSS 3.0 in control 8.3 — is the combination of more than one of these types. The most common is a password plus a one-time password, generated by a hardware token with a display, or increasingly an smartphone app.

Believe it or not, we have seen blogs that suggest that using two of the same factor — two passwords or two retina scans — counts as multi-factor authentication. It doesn't. Once you've scanned one of somebody's eyeballs there's unlikely to be very much to be gained from scanning the other. There's a pretty good chance that they are not far apart!

Use multi-factor authentication

Given the resources now available to even the most amateur hacker, single-factor, password-based authentication simply isn't good enough for anything internet-facing. Using multiple-factor authentication won't stop the theft of credentials, but will make it very difficult to reuse those credentials for fraudulent activity. Integrating two-factor authentication into a web-based application is now relatively simple using free or low-cost tools like Google Authenticator, Authy, or Duo.

When implementing two-factor authentication solutions you should be wary of SMS, telephone or email-based solutions. While these can offer a cost-effective way to roll-out two-factor authentication, many have known vulnerabilities and can be intercepted or even redirected.

Make maintenance part of business as usual

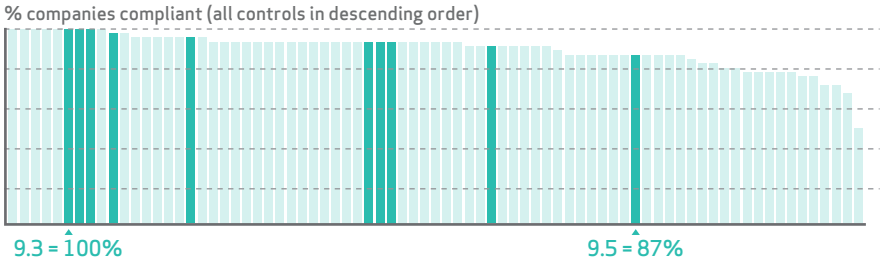
Some Requirement 8 controls have testing procedures that you might easily fail if routine care is not part of day-to-day business, including:

- 8.1.4 [Observe user accounts to verify that any inactive accounts over 90 days old are either removed or disabled].
- 8.2.4 [Change user passwords/passphrases at least every 90 days].

This is not hard to do, as long as system configurations are set appropriately and kept that way.

Restrict physical access to cardholder data

9



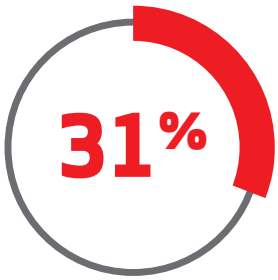
This Requirement stipulates that organizations must restrict physical access to all systems in the DSS scope and all hardcopies of CHD.

WHY IS IT IMPORTANT FOR SECURITY?

For organizations focusing on preventing hacking, viruses, and other types of electronic data breaches, physical weaknesses are easily overlooked. Without appropriate physical security in place, attackers — including rogue staff — can remove or copy CHD and SAD by tampering with POS devices, stealing paper receipts, or many other methods.

Physical access can greatly reduce the effort required to compromise a system. Even a well-secured server or laptop is much more likely to be compromised in a few minutes, if not seconds, if an attacker can gain physical access to it.

Requirement 9's controls demand that organizations use secure entry controls to prevent unauthorized physical access to systems and data within the DSS scope. It also states that organizations must secure media that carries CHD, restrict sharing, and protect POS devices against tampering and substitution.



According to the 2014 DBIR, 31% of confirmed data breaches over the last three years involved POS intrusion, but only 1% physical theft or loss.

WHAT'S NEW?

New control: 9.3 demands that organizations control physical access to sensitive areas for onsite personnel. Only authenticated access based on individual job function is permitted — and access must be revoked immediately when that person leaves the organization or changes role. This control works in conjunction with Requirement 7, which states that organizations must limit access to critical data on a "need to know" basis.

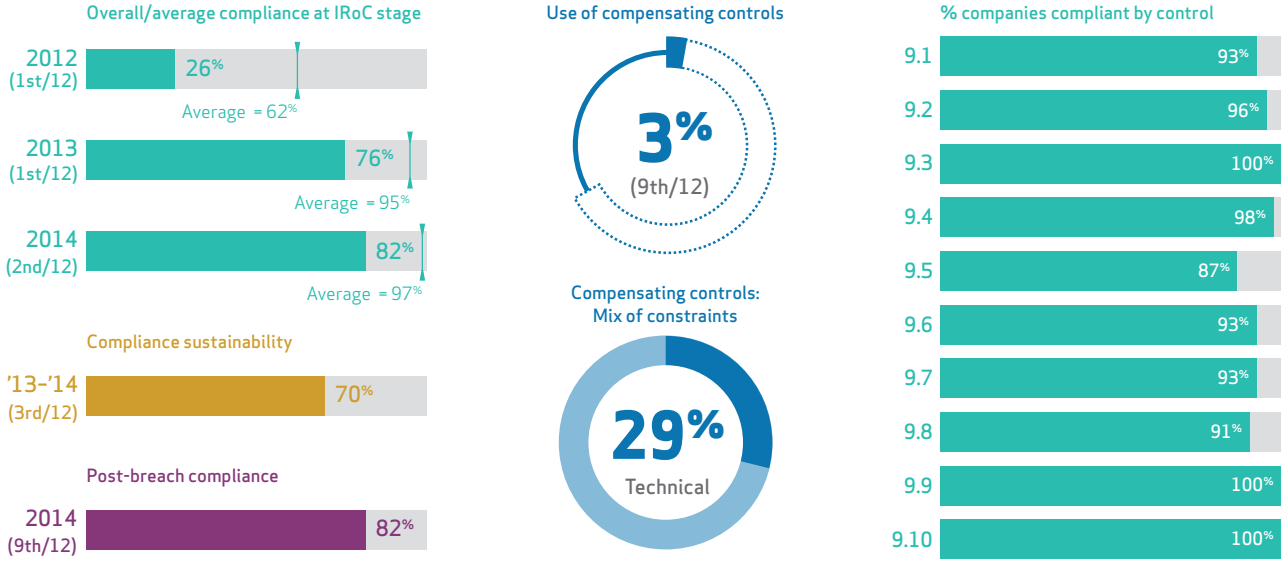
New control: One of the most interesting changes in DSS 3.0 is the inclusion of a specific control relating to the physical security of payment terminals, 9.9 [Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution]. The inclusion of this control reflects the increased number of skimming attacks on POS devices. This control requires:

- An up-to-date inventory of all devices, including details like serial numbers.
- Periodic surface inspections of all devices, and checks to ensure they were not substituted.
- Training to ensure that all staff are able to identify a suspicious card reader and know the proper procedure to follow in such cases.

We don't have enough data from DSS 3.0 assessments to confirm yet, but we expect companies to struggle with some of the new subcontrols under 9.9.

Degree of change
Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 9



MILITARY GRADE?

Subcontrol 9.8.2 requires organizations to "verify that cardholder data on electronic media is rendered unrecoverable… in accordance with industry-accepted standards…" Despite coming ninth out of the ten controls under Requirement 9, 91% of companies complied. But what exactly counts as "industry-accepted standards"? The most commonly cited one is NIST 800-88, from the US National Institute of Standards and Technology. And there are many secure wipe tools freely available that meet this standard.

In the past many security software vendors touted their product as being "military grade" and promised to obliterate data by overwriting it seven, or even more, times. Research has shown that, due to changes in storage mediums including track density, one overwrite is generally sufficient.

This control will be considered a "best practice" until July 1, 2015, after which it will be enforced. While it's good to see this added to DSS 3.0, many acquirers already place strict requirements on the control of payment devices as part of their contracts with merchants. And though often overlooked by the merchants, these acquirer requirements are often more demanding than control 9.9.

Organizations that were early adopters of P2PE solutions will recognize the objectives of this new control as it aligns with the self-assessment questionnaire for P2PE hardware solutions. This indicates that this requirement will not go away when moving to P2PE.

THE STATE OF COMPLIANCE

Few companies struggled with controls 9.3 and 9.4 that govern physical access and procedures to identify visitors, with 100% and 98% compliance respectively. This is partly because most companies now use external datacenters with established physical security procedures rather than onsite facilities.

The controls that companies had more problems with were those covering the management of all media used to hold CHD, including disk, tapes and paper. PCI DSS requires companies to:

- Physically secure all media.
- Maintain strict control over the distribution, internal or external, of any kind of media.
- Keep logs of all media and conduct an inventory at least once a year.
- Destroy media when it is no longer needed.

These demands can be more difficult to achieve because they are often outside of the control of IT and security staff. Complying with them requires everybody that handles media — including staff in small branches and seasonal staff in stores — to be aware of and follow the appropriate procedures.

Compliance with three out of four of these controls (9.5, 9.6, 9.7 and 9.8) fell between 2013 and 2014. The biggest drop was in 9.8, which fell 6.7 percentage points. This isn't a massive fall, but it's significant when you consider the general increase in compliance over the same period.

COMPENSATING CONTROLS

Companies with a large number of distributed sites, like retailers, can come up against technical constraints of security systems. That's why some need to use a compensating control for one or more of the testing procedures within control 9.1 [Use appropriate facility entry controls to limit and monitor physical access to systems in the CDE]. But generally the use of compensating controls with Requirement 9 was very low.

SIMPLIFYING COMPLIANCE

You can simplify compliance by including PCI DSS compliance in the contracts and service level agreements (SLAs) with in-scope third parties. In addition to this, by maintaining several other PCI DSS controls, organizations can increase the effectiveness and efficiency with which they maintain Requirement 9 controls.

For example, using:

- 1.1.3 [Current diagram that shows all CHD flows across systems and networks].
- 2.4 [Maintain an inventory of system components that are in scope for PCI DSS].
- 12.8.1 [Verify that a list of service providers is maintained].
- 12.8.5 [Maintain information about which PCI DSS requirements are managed by each service provider, and which are managed by the entity].

The output from these controls will make it easier to track and monitor the effectiveness of Requirement 9 controls.

MAINTAINING SECURITY AND COMPLIANCE

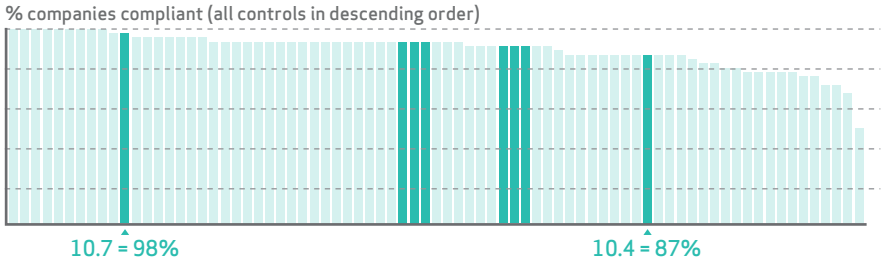
Requirement 9 has a number of controls, subcontrols and testing procedures that require "periodic" review to maintain continued PCI DSS compliance, including:

- 9.2, 9.7, 9.8, 9.9, which require organizations to conduct periodic media inventories, periodic destruction of media, and periodic inspections of devices to look for tampering or substitution.
- 9.1.1.c [Verify that video cameras and/or access-control mechanisms are monitored and that data from cameras or other mechanisms is stored for at least three months]. The area where most companies fail is monitoring this data. You need to have someone looking out for anything suspicious, for example reviewing visitor logs, badge access control logs, and even video from the server room.
- 9.5.1.b [Verify that the storage location security is reviewed at least annually]. Ideally, checking security should be made a "business as usual" process and performed regularly, plus any time that there's any suspicion that something may be wrong.
- 9.7.1 [Review media inventory logs to verify that logs are maintained and media inventories are performed at least annually]. Again, while an annual check is sufficient to be validated, we don't think that this is adequate to achieve good security.

10

Track and monitor access to networks and cardholder data

This requirement covers the creation and protection of information that can be used for tracking and monitoring of access to all systems in the DSS scope, including databases, network switches, firewalls, and clients.



WHY IS IT IMPORTANT FOR SECURITY?

This Requirement is designed to ensure that logs are monitored and securely archived, to proactively detect issues and facilitate forensic investigation in case of a breach.

Organizations must be able to track how users are accessing resources if they're to detect and prevent potential data compromises. The main mechanism for achieving this is system activity logs. Most applications, network appliances, and software packages can perform the level of logging required for PCI DSS compliance. Logs also enable organizations to analyze and determine the cause of a compromise during investigations after a breach.

Consistent and complete audit trails can also significantly reduce the cost of a breach. A large part of post-compromise cost is related to the number of cards thought to be exposed. Lack of conclusive log information reduces the forensic investigator's ability to determine whether the card data in the environment was exposed only partially or in full. Because the issuers usually push the full costs incurred in reissuing cards downstream, potentially all the way to the breached organization, knowing precisely which cards were actually exposed can directly affect the financial impact.

WHAT'S NEW?

The changes to Requirement 10 in DSS 3.0 include clarifying the meaning of several controls. For instance, the section on daily log reviews was revised to help organizations focus their log-review efforts on identifying suspicious activity, relaxing the need to review logs deemed to be less critical (according to the organization's risk-management assessment). However, the new standard also specifically mentions the need to detect anomalies so some current processes and policies may need to be adapted.

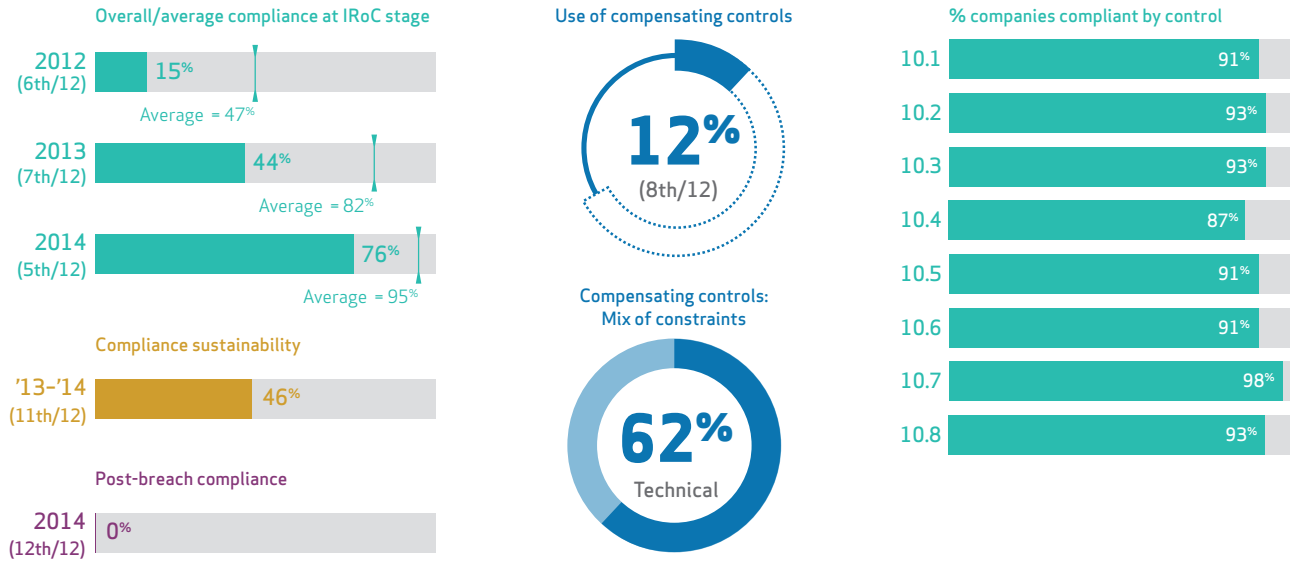
Updated subcontrol: 10.2.5 is an evolving requirement that requires the logging of the creation of new accounts and the elevation of privileges — and all changes, additions, or deletions of accounts with root or administrative privileges. This improves detection of tampering with authorization mechanisms. Organizations should verify if their existing logging solutions address these expanded requirements before their first DSS 3.0 assessment.

Updated subcontrol: 10.2.6 has been updated to prevent the stopping or pausing of audit logs, a common practice for malicious users trying to avoid detection.

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 10



Updated control: DSS 3.0 has clarified control 10.6. This now requires organizations to demonstrate the ability to detect anomalies through daily logs reviews. This will require companies to establish and maintain a baseline, and perform periodic review of logs from all other system components to "identify indications of potential issues or attempts to gain access to sensitive systems via less-sensitive systems". With DSS 3.0, this control now offers more flexibility to balance the effort required to perform log reviews with the different risk levels of the systems generating the logs.

THE STATE OF COMPLIANCE

Compliance with control 10.3 [Recording of audit trail entries for all system components] is actually quite high, at 93%, but it's long been one of the more challenging ones to meet.

A common problem is capacity. Auditing and logging can consume considerable resources (including CPU, memory, disk and network bandwidth). In the interests of performance, many organizations sacrifice security to maintain performance. Virtualized architectures are not immune from this challenge. Many organizations find themselves faced with adding additional capacity to their virtualization environments or turning off logging/auditing, accepting that they aren't PCI DSS compliant, and dealing with the additional risk.

Virtualization also presents its own unique challenges, including additional issues to consider as part of your incident response plan (to meet 12.10) and additional challenges performing post breach forensic examination.

13.3% of companies failed one or more of the subcontrols of 10.4. The most common area of failure was 10.4.1 [Critical systems have the correct and consistent time], which 8.9% of companies failed. Most administrators have configured their systems to be time synchronized and are surprised to learn that they are not. One of the common reasons is that a firewall is blocking the network time protocol (NTP). The next most frequent problem is with 10.4.2 [Time data is protected], which 6.7% of companies struggle with.

91.1% of the companies in our study complied with 10.5 [Secure audit trails so they cannot be altered]. Every company that failed 10.5 also failed testing procedure 10.5.3 [Current audit trail files are promptly backed up to a centralized log server or media that is difficult to alter]. This is important because frequently backing up logs makes it much harder for the bad guys to cover their tracks. Log data needs to be managed as a formally assigned

> It's a sad reality that most organizations that suffer a data breach don't detect it themselves, but only become aware of it when they receive notification from a law enforcement agency, the card brands, or another third party.

responsibility, with a task description that includes making backups of audit trail files. This task is usually automated, but organizations fail to implement procedures to monitor and maintain it.

Control 10.6 [Review logs and security events for all system components to identify anomalies or suspicious activity] also tripped up 8.9% of the companies that we looked at. Companies don't normally have a problem creating the logs, it's analyzing them automatically and efficiently that they find a challenge.

COMPENSATING CONTROLS

Across the board, 12% of companies we looked at used a compensating control within Requirement 10.

Merchants only used a compensating control for one subcontrol:

- 10.5.3 [Promptly back up audit trail files to a centralized log server or media that is difficult to alter].

Service providers turned to a compensating control to pass ten controls and testing procedures, the most common being:

- 10.2.2 [All actions taken by any individual with root or administrative privileges].
- 10.2.4 [Invalid logical access attempts].
- 10.2.5.a [Verify use of identification and authentication mechanisms is logged].

SIMPLIFYING COMPLIANCE

Even if a system is well-managed (well-coded with security patches deployed and anti-virus running, etc.) an intrusion can still occur. It's therefore essential that you make use of logs to detect any suspicious activity: in order to spot attacks while they are in progress, and investigate and remediate any breach. Of course many hackers will try and cover their traces, so securing logs is a must.

Log monitoring is one of the most frustrating but critically important daily tasks for IT security teams. Effectively monitoring logs is crucial to identifying breaches promptly and limiting the damage, but the volume of logs that most companies produce is overwhelming. Requirement 10 has been clarified in DSS 3.0 to specify that the frequency of log reviews should be determined by the organization's risk-management policy. This takes some of the pressure off, allowing companies to review logs from less critical systems less frequently.

Log management solutions have evolved significantly over the past six years. Several vendors now offer really good log management and SIEM solutions with out-of-the-box support for a broad range of devices. These systems automate and simplify log monitoring, and thus PCI DSS compliance. When buying a solution it's important to ensure that it fits the company's specific needs and covers all the types of platforms in use.

In order to meet PCI DSS Requirements, you need to ensure that:

- All systems within the DSS scope are time synchronized.
- Your logging solution archives logs in a manner that facilitates forensic investigation.
- Your log monitoring is capable of quickly detecting any attack.

DSS 3.0 is quite specific about mandatory logging settings, including the use of authentication mechanisms and possible changes to user account permissions and settings. While most enterprise-level operating systems support logging these events, it's rarely part of the default configuration. Custom applications and scripts may require development to include additional logging, triggers, and the blocking of pausing as required by 10.2.6.

Despite advances in solutions, log management still requires operators with advanced skills and experience to ensure that all relevant logs are centralized and available for review, compare them against an accumulated baseline, and respond to exceptions.

INDICATORS OF COMPROMISE

Aware that traditional methods of identifying attacks are no longer sufficient, the IT security industry has developed a new approach based on indicators of compromise (IOCs). RSA, the security division of EMC, defines an IOC as "a forensic artifact or remnant of an intrusion that can be identified on a host or network." By analyzing a large number of attacks, it's possible to create lists of signs that a breach may have happened, or is about to. In the quest to detect data breaches more quickly, these IOCs can provide vital early warning.

Typical IOCs include anomalies in traffic patterns, unusual patterns of requests (perhaps indicating a script rather than a human at work), activity from strange places and at strange times, and more advanced signs that are much harder for attackers to hide, like memory artifacts. Incorporating IOC intelligence into your security regime can help you spot malicious activity.

MAINTAINING SECURITY AND COMPLIANCE

Requirement 10 was never meant to be solely about using system logs to detect data breaches, organizations that focus on this as the sole objective often fail to design and implement a sustainable log management solution. Implementing effective log management has numerous other operational benefits and offers a proactive security layer.

It's essential that creating, monitoring and managing logs is automated, but even then a fair amount of manual work is required to ensure that the log management solution is working properly. It is not advisable to rely on default configurations.

Organizations must realize that it is impossible to effectively review log files manually, regardless of the number of system components in any particular DSS scope, be it one server or one hundred. The task must be automated to generate exception reports and alerts. And automation tools must be appropriately configured to avoid overwhelming smaller security teams with data, particularly when it comes to daily reviews. Even the best event alerting will fail to provide appropriate protection if security procedures aren't established to coordinate a quick and appropriate response to events.

The following must be checked at least daily to ensure continued compliance, but this can be automated:

- All security events.
- Logs of all system components that store, process, or transmit CHD and/or SAD, or that could impact the security of CHD and/or SAD.
- Logs from all critical system components.
- Logs of all servers and system components that perform security functions (for example, firewalls, intrusion-detection systems/intrusion-prevention systems (IDS/IPS), authentication servers, e-commerce redirection servers, etc.).

The power of logs is increased massively when they are combined intelligently and efficiently to provide detailed and actionable information.

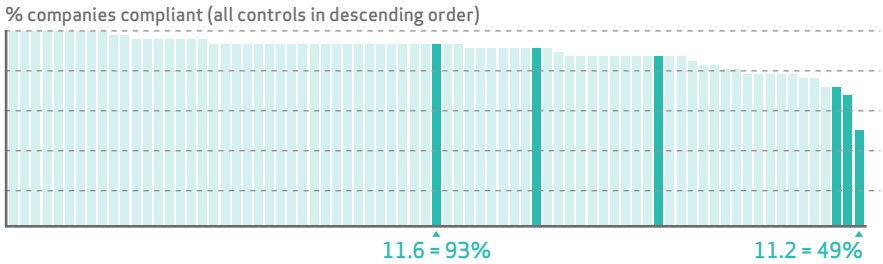
According to our DBIR 2014, audit logging is a key feature in detecting both POS intrusion and insider misuse.

IOCs enable companies to be more proactive in identifying attacks, and help spot more sophisticated attacks by considering multiple signs together. While it's not an explicit requirement of PCI DSS compliance, we recommend that you look at IOCs as a way to improve your defenses.

11

Regularly test security systems and processes

This requirement covers the use of vulnerability scanning, penetration testing, file integrity monitoring, and intrusion detection to ensure that weaknesses are identified and addressed.



WHY IS IT IMPORTANT FOR SECURITY?

Requirement 11 covers the need to regularly and frequently:

- Carry out vulnerability scans to identify unaddressed security issues.
- Scan for rogue wireless networks.
- Perform file integrity monitoring to spot unauthorized system changes.
- Use intrusion detection systems to spot signs of network compromise.

It also provides a crosscheck on the effects of other PCI DSS controls as it will identify many (but not all) missing security patches or insecure configurations.

Requirement 11 is fundamental to ensuring that the organization is prepared for the range of attack types reported in the 2014 DBIR. During post breach investigations we found that just 9% of organizations were compliant with this requirement.

WHAT'S NEW?

There have been significant changes to Requirement 11 over the years. In early versions of the DSS the focus was on a number of "testing activities" that needed to be performed by an external specialist organization, almost as a final check on the controls. The focus of the changes in DSS 3.0 is on moving penetration testing from "dark art" to a verifiable approach that covers both applications and infrastructure, and is consistent with industry standards. Testing is now seen as an integral part of the validation process for many of the other requirements: and a mandatory part of how organizations validate their compliance scope when network segmentation has been used to reduce it.

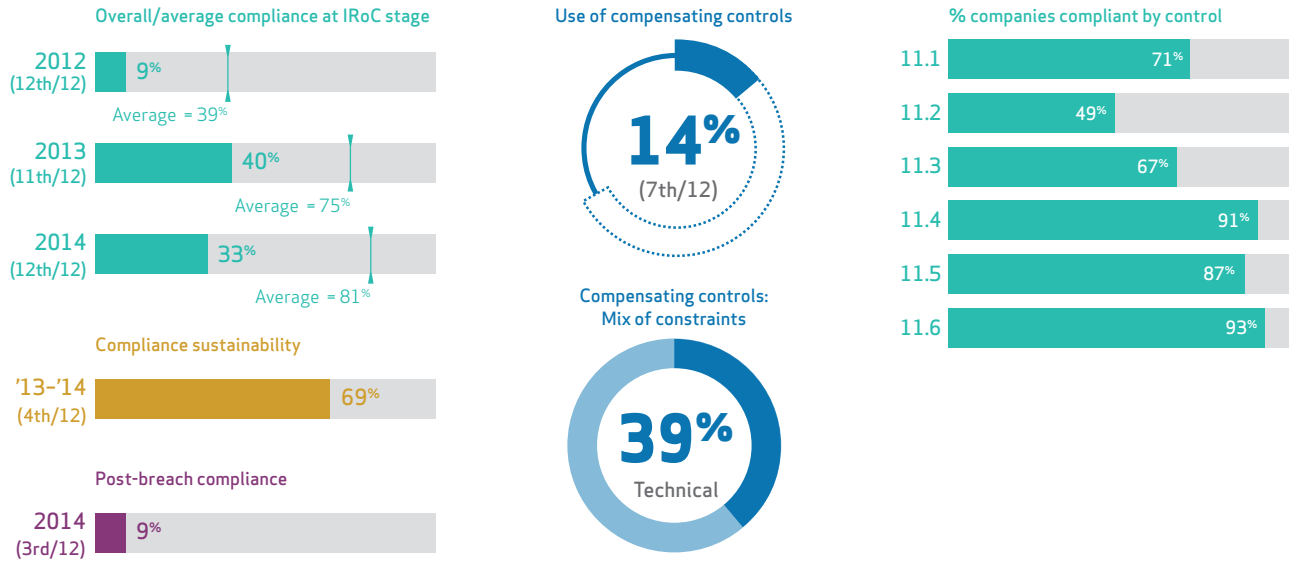
New subcontrols: In DSS 3.0 the guidance on wireless access point security has been extended to require an inventory of authorized wireless access points, each with a documented business justification (subcontrol 11.1.1). It also adds a new subcontrol (11.1.2) to align with the existing testing procedure for incident response procedures if unauthorized wireless access points are detected.

New control: 11.3 [Implement a methodology for penetration testing] specifies that organizations adopt a thorough, standards-based penetration-testing methodology — a

Degree of change

Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 11



best practice until July 1, 2015. Unlike Approved Scanning Vendors (ASV), which are assessed by and registered with the PCI SSC, there is no central registry, vetting, or control of companies offering penetration testing. Therefore the scope of the assessment and the quality of the report may significantly vary from one provider to another — whether performed in-house or by an external vendor. Having a defined methodology will help standardize penetration-testing activities and ensure that whatever approach the company chooses, the key points of the testing will be covered. The introduction of this control is long overdue, but while we welcome its addition we believe that it lacks sufficient rigor. There's still a danger that some companies will take a "bare minimum" approach to keep additional costs down.

New subcontrol: 11.3.4 requires that if segmentation is used to isolate the CDE that penetration tests are performed to validate that this segmentation is active and effective. This testing must be performed at least annually, but also after any changes to the segmentation controls and methods.

Unlike other parts of DSS 3.0 that dictate that testing should be performed after "significant changes", the standard stipulates that segmentation must be revalidated after any change to it.

THE STATE OF COMPLIANCE

Requirement 11 was the least-well complied-with requirement in our study. Just 33% of companies passed all the testing procedures in 2014, compared with 40% in 2013. It is the only Requirement where we saw compliance drop between 2013 and 2014.

Across this Requirement, nearly 40% of testing procedures scored 90% or higher, but two came in under 70% (11.2.1.a and 11.2.1.b). 14 of the 31 testing procedures were failed by one in five companies, or more.

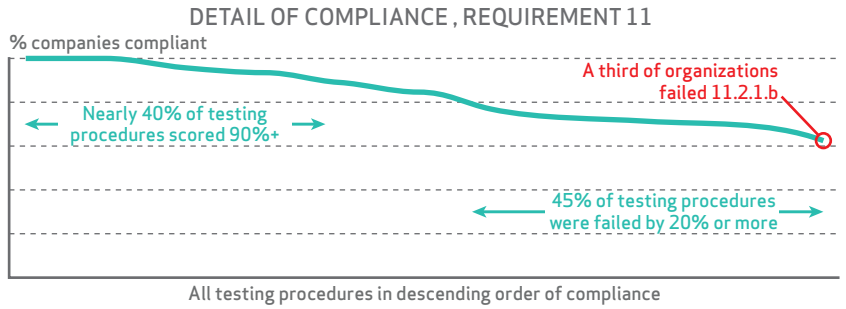


Figure 23: Companies compliant with Requirement 11 testing procedures, 2014

Compliance with control 11.1 fell from 80% in 2013 to 71% in 2014. Considering that the average compliance by control went from 80% to 90% in the same period, that's quite a significant fall. Companies that have chosen not to use wireless in their DSS scope often think that this excuses them from the need to perform rogue access point scans, and as a result they fail this control.

Control 11.2 [Perform quarterly internal vulnerability scans, and rescans as needed, until all "high-risk" vulnerabilities are resolved] has the lowest compliance rate of any in our study, and what's worse is that it's going down. In 2013, 56% of companies met the requirements of 11.2; in 2014 that figure was just 49%. Less than half of companies are regularly scanning for vulnerabilities and mitigating the ones that they find. We discuss the reasons for this and how to address them below.

COMPENSATING CONTROLS

14% of companies used a compensating control within Requirement 11, putting it in the midfield in our study. The three testing procedures they failed most often and used a compensating control were:

- 11.5.a (6.2%) and 11.5.b (4.1%). Change-detection mechanisms, such as file integrity monitoring, are an expense that companies don't typically budget for. Some paid-for tools are powerful, but can be difficult to configure to avoid getting lots of false positives. Cheaper alternatives exist, like open-source scripts, but require quite a lot of technical expertise to use.
- 11.1.a, 11.1.b, 11.1.c, and 11.1.d (3.1%). These testing procedures validate the detection and identification of all authorized and unauthorized wireless access points on a quarterly basis. Again this is a technical control that requires either an expensive tool that is difficult to configure, or an open-source tool that non-technical users will struggle with. Many companies are unaware that if the technical expertise isn't available to use wireless scanning tools, it is acceptable to perform physical walkthroughs. But whichever methods are used, they must be sufficient to detect and identify both authorized and unauthorized devices. So it might be hard to sell to an assessor or acquirer that a walkthrough is sufficient for a large environment.

VULNERABILITY SCANNING VERSUS PENETRATION TESTING

The terms "vulnerability scanning" and "penetration testing" are often misunderstood by organizations. A vulnerability assessment uses automated tools to look for known vulnerabilities across defined IP address ranges. The sorts of vulnerabilities found include unpatched or misconfigured systems. Penetration testing goes a step further. A penetration tester — such tests will always be carried out by a person, not automated — will scan systems to identify the IP addresses, device types, operating systems and software in use. This will enable the tester to identify likely vulnerabilities, which they will try to exploit to identify and evaluate weaknesses in networks and applications. A thorough penetration test may also include using physical and social engineering techniques.

SIMPLIFYING COMPLIANCE

The intent of Requirement 11 is to detect and correct known vulnerabilities. DSS 3.0 requires quarterly scanning, but more frequent scanning is advisable:

- Vulnerability scanning isn't an event, it's a process. You should scan, fix, and scan again until you achieve a "clean" result. The standard defines a clean scan as one that doesn't pick up any serious vulnerabilities: rated severe, high or critical. With new vulnerabilities — over 90% of which are severe, high or critical — emerging on an almost daily basis this can be a Sisyphean task. The PCI SSC has provided additional guidance in their frequently asked questions, providing some more flexibility.
- It often takes a while for vendors to issue patches; and even when they do, those patches often come with notes advising of circumstances in which installation could cause problems. In this case the QSA will look for evidence that the company has followed the vendor's guidance and taken appropriate steps to mitigate the threat.
- The standard also demands that a vulnerability scan is performed following any significant change to the DSS scope or systems within it. For example, adding a new web server, relocation, or a merger or acquisition.

While it's advisable to perform scans more than quarterly, it's only necessary to report four quarterly results to achieve compliance. As the results above show, we still see a lot of companies failing to meet even this minimum standard. Aside from the reasons listed above, we often see companies fail due to:

- **Lack of accountability:** Organizations lose track of scanning when people change roles or leave the company and the responsibility for managing scanning isn't handed over properly.
- **Ignoring the need to scan internally:** Organizations wrongly believe that passing an external scan is sufficient and their firewalls prevent any other form of threat.
- **Being unable to present reports:** We've seen many cases of organizations not able to produce scan results because they've lost access to a former ASV's online portal, or they've simply lost them. Consistent record keeping is an important part of PCI DSS compliance and being unable to produce documentation is just not acceptable.

SERVER-SIDE VULNERABILITIES

2014 will be remembered in the IT industry for the discovery of several notable server-side vulnerabilities.

In April, a serious flaw, known as Heartbleed, was exposed in the OpenSSL encryption code. This is widely used to protect website traffic and its discovery shook the industry. Almost a year later thousands of websites and devices remain vulnerable.

In September, multiple critical vulnerabilities were reported in Bash — a common command-line interface used in many UNIX-based operating systems, including Linux and OS X. These flaws could allow an attacker to remotely execute shell commands by placing malicious code in environment variables.

In October, Google researchers discovered a flaw in the design of SSL 3.0, christened POODLE, which could allow sensitive information, including secret session cookies, to be decrypted and used to take over accounts.

MAINTAINING SECURITY AND COMPLIANCE

Automate threat and vulnerability mitigation

It is not uncommon for organizations to identify vulnerabilities, even severe ones, within their compliance environment and then to leave them unmitigated for months. This is especially concerning for vulnerabilities that have been publicly disclosed, since it presents an opportunity for attackers to locate and exploit it, significantly increasing the likelihood of a security breach and data compromise.

While the identification of vulnerabilities is largely automated, the verification of false positives and their correction often requires more time than anticipated.

The majority of organizations have the necessary tools in place to automate and manage the vulnerability management process, but may regard an increase in the frequency of these tests to be an unnecessary burden on resources.

A Plan-Do-Check-Act approach to the vulnerability management process can improve quality and help streamline it, so that it functions in a consistent, repeatable and predictable manner.

It is essential that security testing process is sufficiently robust to maintain integrity despite environmental pressures (for example, requests to divert resources away from security testing, or to postpone critical security tests) and to be resilient — the ability to quickly recover from unexpected infrastructure or business changes that constrain or prevent security testing.

Increase frequency of security testing cycles

PCI DSS requires quarterly network and application vulnerability scanning, and conducting penetration tests once per year and after significant changes are made to systems within the DSS scope. When organizations attempt to meet only these minimum requirements, it often ends up complicating compliance management instead of simplifying it, particularly since such an approach lowers the organization's potential to maintain compliance with this requirement.

Include vulnerability testing as part of third-party onboarding process

Recent data breaches that resulted in significant CHD disclosures highlight the importance of managing connected third parties and the risk associated with third-party technology. Organizations can benefit from mandating in agreements, that third parties use independent verification services to provide assurance about meeting CHD and environment security requirements, as part of the procurement and deployment process.

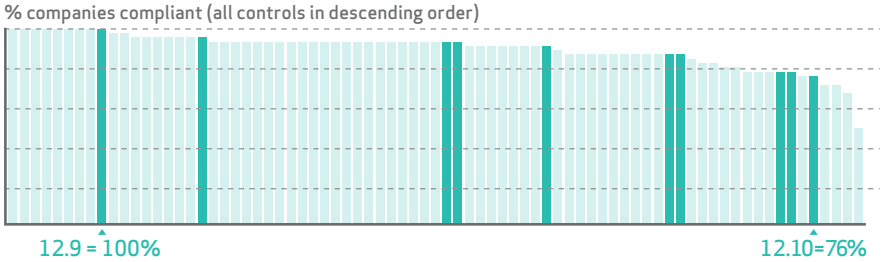
QUARTERLY SCANNING REQUIREMENT

The following steps are required to meet the quarterly scan requirement:

- All in-scope systems are covered by the organization's scan-remediate-rescan processes.
- All in-scope systems have been scanned, and rescanned as necessary, for each quarterly period.
- The organization has processes in place to remediate vulnerabilities and can present evidence to show that any vulnerabilities identified in previous scans have been addressed.
- Scan results show that previously identified vulnerabilities have been properly addressed, indicating that remediation practices are working.

Maintain an information security policy

12



This requirement demands that organizations actively manage their data protection responsibilities by establishing, updating, and communicating security policies and procedures aligned with results of regular risk assessments.

WHY IS IT IMPORTANT FOR SECURITY?

Deploying technologies such as encryption and firewalls can only go so far in protecting an organization and helping maintain compliance. Policies are needed to address the weak link in security — users. If people don't know or understand what's expected of them, they can put CHD at risk, no matter what other security measures you have in place. Policies play a very important role in securing data and must be kept up to date, documented, and formally approved. They are the foundation for everything else as they provide clarity, direction, and instruction and assign responsibility.

WHAT'S NEW?

Updated control: Clearly written policies and communication of those policies to all employees is critical to maintaining a secure environment. Control 12.1 [Establish, publish, maintain, and disseminate a security policy] stood out as a "catch all" requirement in DSS 2.0. In DSS 3.0 the need to document and communicate a security policy is covered in all the appropriate Requirements.

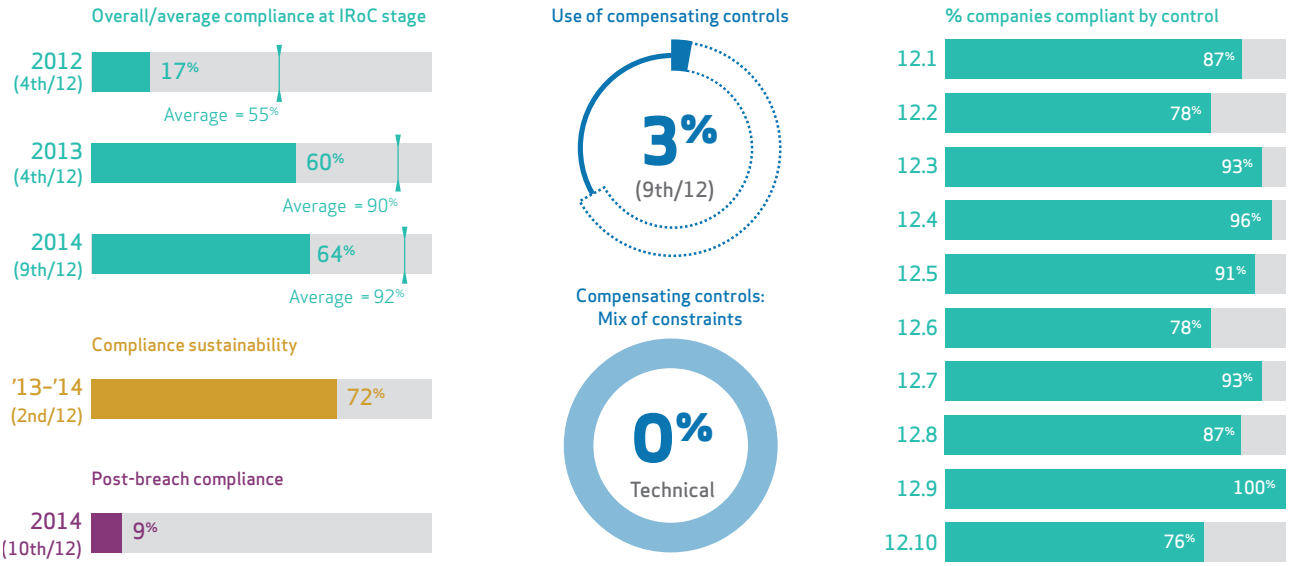
Updated control: 12.2 (was 12.1.2 in DSS 2.0) always required a "formal risk assessment" to be performed. Exactly what this meant was a topic of debate among practitioners. As well as clarifying the language in DSS 3.0, the SSC has released an information supplement, PCI DSS Risk Assessment Guidelines to provide more direction. This control has also been updated to require organizations to perform a risk assessment whenever there has been "significant change" to the environment, not just annually.

The management of third parties is a very important theme in DSS 3.0. This includes providers of hosting, hosted or managed firewalls, intrusion detection systems, payment gateways, customer service functions, and call center and sales functions. This list is not limited to organizations with which you share CHD, but includes any service provider that could affect the security of CHD. This is another example of where in DSS 3.0 it's more important than ever to understand and document the flow of CHD.

New subcontrol: 12.8.5 has been added to ensure there is exact agreement and clarity on which PCI DSS controls are handled by the service provider and which are handled by the customer (that is, the merchant). In the past there was the risk of the service provider not covering all applicable DSS requirements and that was difficult to determine upfront. This is should now be reflected in the service providers' Attestation of Compliance, thus simplifying due diligence for companies selecting a new third party.

Degree of change
Indicator of the scale of change between DSS 2.0 and 3.0

COMPLIANCE SNAPSHOT: REQUIREMENT 12



New control: 12.9 (service providers only) specifies that organizations must acknowledge their responsibility in a formal written statement. This means it will be totally clear that the service provider accepts and agrees to be responsible for all CHD activities under their control for their customer. This aligns with existing control 12.8.2 which stipulates that organizations make sure they have agreed on this subject with their service providers.

Updated control: 12.10 [Implement an incident response plan. Be prepared to respond immediately to a system breach] was renumbered from 12.9 in DSS 2.0 and includes clarification on the intent for including alerts in the incident response plan. For a fuller discussion of incident response, please see page 80.

THE STATE OF COMPLIANCE

Most organizations, even small businesses, have documented security policies to help employees understand data protection and behave accordingly. In DSS 3.0 the operational procedure and security policy components (12.1.1 and 12.2) have been split up and moved to be within the relevant Requirements.

Control 12.6 [Implement a formal security awareness program] showed a slight decrease, dropping from 80% in 2013 to 78% in 2014. This is an area where organizations should pay more attention. It's essential that employees are made aware of their responsibilities, and are proficient at detecting and responding to security incidents.

Compliance with control 12.10 [Implement an incident response plan] over the three years in our dataset was just 58% — the lowest for all controls within Requirement 12.

In 2014 control 12.10 showed the lowest compliance within Requirement 12 (as it did in 2013), just 76% of organizations passed it. This control is referenced in testing procedure 11.1.2.a [Examine the organization's incident response plan to verify it defines and requires a response in the event that an unauthorized wireless access point is detected]. Organizations should be much more proactive about training. In October 2014, the PCI SSC released an information supplement "Best Practices for Implementing a Security Awareness Program" to provide additional guidance.

DON'T ASSUME

We have had instances where a company claimed that they outsourced all hosting, including security, to a third party, but the contract with the hosting company only specified the delivery of datacenter space, power and light.

The new control 12.8.5 now enforces documenting this in the ROC and Attestation of Compliance.

COMPENSATING CONTROLS

Just 3% of companies used a compensating control with Requirement 12. This is too small a sample to allow any meaningful analysis.

SIMPLIFYING COMPLIANCE

Control 12.5 mandates assigning an individual or team within your organization with the responsibility for managing information security. This task can be simplified by providing them with the tools and procedures they need to measure and report on the actual performance of the compliance program, and the condition and effectiveness of security controls. The importance of automating measuring and reporting on compliance performance cannot be overstressed. It is key to simplifying compliance, improving performance, and achieving sustainability.

MAINTAINING SECURITY AND COMPLIANCE

As we mentioned in last year's report, we don't think that there is sufficient emphasis on determining and addressing residual risk — the need for organizations to document their examination and understanding of the risks that remain after implementing all required DSS controls. The special interest group that produced the information supplement mentioned above made it clear that the risk assessment should be used to determine what additional controls are needed. After all, PCI DSS compliance creates a firm baseline, but cannot cater to all the specifics of a company's situation.

We strongly recommend that the very first thing that you do when creating or revising a security program is to perform a risk assessment. It's essential to first understand the environment to enable you to design an effective security program. It should underpin every investment that you make in security, be it people, training, hardware or software.

The PCI SSC's information supplement doesn't specify which framework should be used, but lists a number of suitable options — including OCTAVE, ISO 27005, and NIST SP 800-30. This guidance suggests that a risk assessment framework should:

- Be defined and follow a documented process.
- Identify threats, vulnerabilities and controls that could impact the security of CHD, including risks posed by third parties.
- Rate the effectiveness of existing security controls.
- Identify organizational and technical vulnerabilities and score threats based on likelihood and potential impact.
- Cover any people, processes or technology that could impact the security of all systems within the DSS scope.
- Cover all payment channels and include any asset that directly or indirectly impacts the processing, storage, transmission or protection of CHD or the security of the CDE.
- Result in a prioritized risk mitigation plan.

This is one of the Requirements where we most clearly see the difference between companies whose goal is to comply — teaching to the test — and those which are focused on security. The former look at the findings of a vulnerability scan and identify what systems they need to fix; the latter look for the failings in their security processes as well, they don't just fix the issue but the underlying problem too.

Conclusion

Complying with PCI DSS is hard, and the majority of organizations that initiate a PCI DSS program for the first time fail to fully appreciate the impact it will have on their organization, in terms of its scope, the resources, and the time it takes.

Your company, the threats you face and the PCI DSS itself are evolving. The latest version of the standard includes hundreds of changes, but there are some clear themes that we've identified. We discuss these below, along with how we've seen compliance get better, and where we think that there's still room for improvement.

WHAT MAKES PCI DSS COMPLIANCE CHALLENGING?

There are several reasons why organizations have difficulty with PCI DSS compliance:

- **Scale and complexity of requirements**: PCI DSS covers a wide range of interconnected topics, most of which require attention at the same time. Many organizations don't even read and digest the contents of the entire standard and related program documentation.
- **Uncertainty about scope and impact**: Organizations may have difficulty predicting the effort and investment needed, the time compliance will take, and the impact it will have on business, operations, IT infrastructure, and business partners.
- **The compliance cycle**: Compliance is not a one-off activity, or even a simple yearly cycle. Compliance must be dynamic and be maintained even as the risk environment, IT infrastructure, regulatory and business landscape change from day to day.
- **Lack of resources**: Certain elements of achieving and maintaining compliance require not just an ongoing and unpredictable commitment of time and money, but specialist skills and knowledge that may not be readily available inside the business.
- **Lack of insight in existing business processes**: While planning large PCI DSS compliance programs, compliance teams often discover payment processes and sales channels that they were unaware of.
- **Misplaced confidence in existing information security maturity**: Many organizations discover a significant gap between what they agreed to do and what actually was implemented over the years when going through PCI DSS validation.

The following recommendations will help you to build a well-managed program that will help you to achieve overall success, avoid costly mistakes, increase ROI, and produce a real contribution to information security.

MAKING COMPLIANCE EASIER

Scoping and documenting data flows

Almost all the companies that we studied used some form of scope reduction. But many organizations still make PCI DSS compliance unnecessarily complex and expensive by not doing enough to exclude systems. There are three good reasons to strive to keep your DSS scope as small as possible:

- **Reducing risk.** If you store less cardholder data in fewer places, it reduces the opportunities for a breach to occur and limits the damage that a breach can cause.
- **Reducing workload.** Every system you can take out of scope is one less system that you have to validate for compliance. If a system is taken out of scope then it shouldn't pose any significant threat to CHD, reducing the attack surface.
- **Controlling costs.** While you're making changes to reduce scope, you may find that you can consolidate systems and restructure environments, saving money.

Two common critical mistakes with PCI DSS programs are not understanding the scope of compliance, and not knowing what, where and how CHD is stored, processed and

CALL TO THE PCI SSC

Lack of clarity on scope reduction, particularly the "full isolation" rule, means that organizations may be including more systems in their DSS scope than they need to, or adopting network architectures that are more complex than necessary in order to "play it safe". We call on the SSC to provide more clarity on approved scope-reduction techniques in upcoming versions of the DSS so that companies can be clear how they can exclude systems from their DSS scope and compliance workload.

transmitted. The reason for this is often not complexity of the infrastructure, but instead, failure to collaborate across internal departments to define the PCI DSS scope and CHD flows.

Ongoing interdepartmental communication and collaboration are crucial for achieving CHD protection and compliance success. The compliance organization should have cross-organization representation which includes all the relevant stakeholders (IT, security, HR, finance, legal, etc.).

Making network decisions without understanding the full context of compliance requirements, especially isolation and segmentation requirements and options, is another major pitfall that can have significant negative impact. Documenting data flows is an important part of scope reduction, and also helps to simplify achieving compliance.

Automation and leveraging the latest tools

It is just not practical to meet many parts of PCI DSS without some form of automation. But most organizations still have plenty of additional opportunities to increase automation and leverage the latest tools to reduce the burden of compliance and improve security. Many organizations are not yet utilizing the capabilities of next-generation firewalls and other application- and context-aware security systems. This is a missed opportunity. The maturity and sophistication of security technologies has improved greatly, and companies should reassess the tools that they use and whether a small investment might deliver a large ROI.

MAKING COMPLIANCE MORE EFFECTIVE

Logging, monitoring and testing

Security testing is still a big problem, as the results for Requirement 11 show — only a third of companies were compliant at IRoC stage. Testing that security systems are working as intended and monitoring logs to detect the early signs of breaches are critical steps in reducing the likelihood of a successful breach and minimizing the damage caused should one occur. This is an area where companies really must improve if they are to get ahead of the growing range of threats.

Setting metrics and measuring performance

PCI DSS does not cover the use of security metrics for measuring compliance performance, at all. There needs to be much more emphasis on the need to maintain a compliance performance measurement program, using risk-based metrics to measure and report on the effectiveness of security controls.

Defining responsibilities and managing third parties

One of the themes that we think runs through DSS 3.0 is an increased focus on ensuring that responsibilities are clearly identified and documented. This applies both within the organization and arrangements with third parties. It's frankly amazing that some companies have been prepared to trust parts of their PCI DSS compliance to a third party without having this in writing. We've seen many examples of companies assuming that a third party was looking after some element of security, and being quite shocked to find out that they weren't.

MAKING COMPLIANCE SUSTAINABLE

Environments aren't static, with both external factors and internal dynamics driving change — new threats, new technologies and organizational change to name just a few. Compliance at a point in time isn't sufficient to protect valuable data and their reputations, organizations must make being proficient at maintaining security controls in a dynamic environment a strategic imperative. Being able to say that you were compliant three months ago will be of little solace when dealing with the aftermath of a breach. But our data shows — whether you look at all IRoCs or pairings of FRoCs followed by an IRoC — less than a third of companies successfully maintain compliance between validations.

> The outcome of each activity should be to establish ongoing, sustainable protection of data, not just to meet periodic compliance requirements.

> Just one new uncontrolled Wi-Fi access point, unprotected admin account, or unencrypted drive could take you out of compliance.

> Instead of seeing PANs and other card data as just fields in a database, every employee should be taught to see them as valuable corporate assets worthy of protection and due care.

Many companies still treat compliance as a one-off tick-box exercise or fire drill that the security team owns and the rest of the organization begrudges. This is not only expensive and disruptive, but doing so leaves them more vulnerable to data breaches caused by changes to processes or infrastructure that happen between assessments. The answer is to fully integrate compliance into the context of your organization's larger governance, risk, and compliance (GRC) strategy, and make it part of day-to-day activities.

We advocate that compliance-mature organizations stop looking at PCI DSS compliance as a cost of doing business, and instead see it as an investment to be leveraged, both for improving your business performance and for managing risk.

Coordinated security programs can deliver quantifiable returns through:

- Greater employee awareness of security and a more active and alert security posture across the organization, helping reduce the risk of a breach and the damages it causes.
- More effective orchestration of security, data protection, risk reduction, governance and other compliance requirements — reducing duplication of investments and costs needed elsewhere in the organization.
- Improved business process and business process management — for instance as a result of greater transparency into data flows or through following best practices.

Our analysis of QSA vs PFI data has clearly shown a strong inverse relationship between PCI DSS compliance likelihood of breach. The biggest indicators of breach risk are Requirements 6 [Develop and maintain secure systems and applications] and 10 [Track and monitor all access to network resources and CHD]. This should serve as a wake up call that the days of set-it-and-forget-it are over. It's imperative to bake-in security as business-as-usual throughout the systems and process lifecycles.

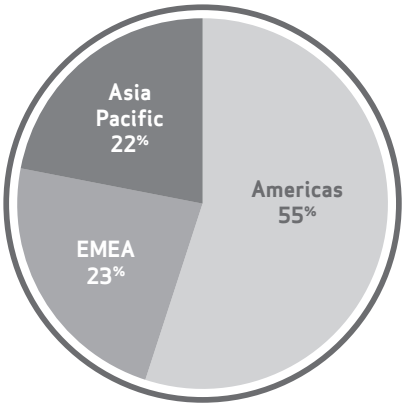
Questions? Comments?

We'd love to hear them. Email us at pcireport@verizon.com, find us on linkedin.com/company/verizonenterprise, or tweet @VZenterprise with the hashtag #pcireport.

Appendix A
Methodology

The companies that we assessed span many industries and countries. Our team of over 500 security professionals covers a wide range of expertise, including performing PCI security compliance assessments, investigating data breaches and advising clients on security and risk management. We believe that this give us a degree of insight into security and risk management that's hard to match.

BREAKDOWN OF DATASET BY REGION
SPLIT OF COMPANIES, 2012–14



BREAKDOWN OF DATASET BY SECTOR
SPLIT OF COMPANIES, 2012–14

Figures 24/25: Demographics of dataset, 2012–2014

A new feature this year is the analysis of final reports on compliance (FRoCs). These are the formal compliance assessment reports produced by QSAs for organizations that have achieved a successful PCI DSS validation. Looking at this additional data has given us a detailed insight into the use of scope-reduction techniques and compensating controls.

TERMINOLOGY

The assessments carried out covered both DSS 2.0 and 3.0. Unless explicitly stated otherwise, all the references to controls and subcontrols refer to DSS 3.0.

To achieve this, we performed a detailed mapping exercise between DSS 2.0 and 3.0 controls and testing procedures, looking at the intent of each — not just the wording.

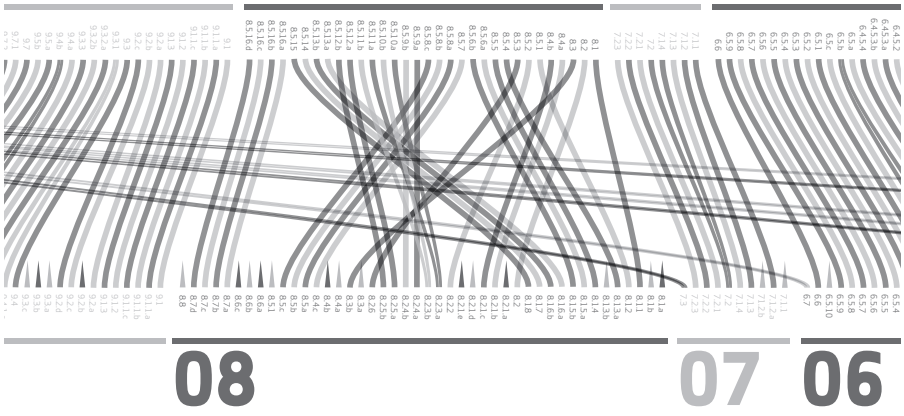


Figure 26 Extract of visualization of mapping of DSS 2.0 to DSS 3.0 used throughout this report

This research is based on quantitative data gathered by our qualified security assessors (QSAs) while performing assessments on PCI DSS compliance between 2012 and 2014. This data was augmented by analysis of forensic investigation reports by our security practice, the authors of the Verizon Data Breach Investigations Report (DBIR).

TYPES OF ASSESSOR

Throughout this report we use the term qualified security assessor (QSA). All the RoCs that we studied were written by Verizon QSAs, but PCI DSS compliance can also be assessed by an internal security assessor (ISA) or via a self-assessment questionnaire.

Types of analysis in this report

DEGREE OF CHANGE

We analyzed the number of controls and testing procedures that were entirely new and revised, and scored each Requirement accordingly. We then summed up all the scores to show the overall change by Requirement on a scale of 0 to 12. See page 16 for more details.

SCOPE-REDUCTION TECHNIQUES

We reviewed data flow diagrams, network diagrams and lists of in-scope system components for each organization within our 2012 to 2014 dataset. This provided interesting insight on the most used scope-reduction methods, and the extent to which organizations succeed in reducing the data, networks and infrastructure that are in scope.

COMPLIANCE AT INTERIM ASSESSMENT

As last year, we look at compliance by organization — the number of companies that passed all the validation testing requirements for all applicable controls that they were assessed on, divided by the total number of companies assessed. We look at this by requirement and for all requirements.

Where a required security control was failed, this failure is taken to cascade upwards (so failing 3.5.2.b would lead to failing subcontrol 3.5.2, control 3.5, Requirement 3 and the whole assessment).

COMPENSATING CONTROLS

This year we've extended our analysis to include the use of compensating controls. A compensating control should generally address only one PCI DSS requirement, but in some cases multiple requirements may be covered using a single compensating control. We therefore chose to do our analysis at the testing procedures level to provide a more granular view of what necessitated a compensating control. As well as looking at where compensating controls were used, we looked at whether the justification was a business reason or a technical constraint.

REVALIDATION AND SUSTAINABILITY

By looking at where we have pairs of a successful FRoC followed by an IRoC, we've been able to look at the compliance of companies undergoing revalidation (typically performed about nine months after the previous validation). This has enabled us to investigate where companies fall out of compliance.

Taking our IRoC datasheet as a base, we modeled what compliance we'd expect to see in our revalidation sample. We've then compared this to the actual level of compliance that we observed. The result is a sustainability index that indicates the Requirements where companies are least likely to be able to maintain compliance.

COMPLIANCE AT THE TIME OF A BREACH

Our PCI-approved forensic investigators study companies that have suffered a payment card data breach. By looking at their assessments over the past year we've been able to compare compliance in breached companies with the general population.

Appendix B
Definition of key terms

These terms and definitions are those used by the Verizon PCI Security practice. This includes our own internal terms and widely used industry terms. A comprehensive list of official PCI Council terminology is available on the PCI SSC website.

ACCOUNT DATA
Cardholder data plus sensitive authentication data.

ACL
Access control list, specifies which users and processes have access to system objects and what operations they are allowed to perform on those objects.

ASV
Approved scanning vendor: a company approved by the PCI SSC to conduct external vulnerability scanning services.

CDE
Cardholder data environment: all the people, processes, and technologies that store, process, or transmit CHD and/or SAD.

CHD
Cardholder data: comprises the full PAN or the full PAN plus any of the following: cardholder name, expiry date and service code

CHIP AND PIN/CHIP AND SIGNATURE
Colloquial names for EMV.

CISO
Chief information security officer.

COMPLIANCE ENVIRONMENT:
The entire in-scope environment consisting of the CDE and all in-scope system components.

COMPLIANT
See page 12.

CVSS
Common Vulnerability Scoring System.

CVV/CVV2
Card verification value. The number printed on a card to help secure "card not present" transactions — other terms include CVC, CID and CSC. To be precise, the code printed on the card is actually the CVV2 — and the CVV is integrity-check data encoded on the magnetic strip — but both terms are widely used online.

DBIR
The Verizon Data Breach Investigations Report, see verizonenterprise.com/dbir.

DLP
Data loss prevention solution — restricts the transmission of sensitive data, reducing the risk of suffering a breach.

DSS
PCI Data Security Standard.

DSS SCOPE
The CDE, all connected systems, plus any other systems that either support the security of the CDE or that if compromised could affect the security of the CDE.

EMV
Europay/MasterCard/Visa, the standard for credit and debit payment cards based on chip card technology — commonly known as "Chip and PIN" or "Chip and signature" in some regions.

FROC
Final Report on Compliance: a final PCI DSS compliance validation report documenting the annual compliance validation assessment results.

FULL ISOLATION
The elimination of all communication between the CDE and any non-CDE component, regardless of the security of the channel and the direction of initiation.

GRC
Governance, risk and compliance.

INTERIM ASSESSMENT
An initial compliance validation assessment performed by a QSA to determine the compliance status.

IOC
Indicator of compromise. RSA, the security division of EMC, defines an IOC as "a forensic artifact or remnant of an intrusion that can be identified on a host or network."

IDS
Intrusion detection system.

IPS
Intrusion prevention system.

IROC
Interim report on compliance, the output of an interim assessment, detailing the changes required to address identified deficiencies.

ISA
Internal security assessor.

LIABILITY SHIFT

Liability shifts are the transfer of the financial responsibility for fraudulent transactions or chargeback losses from one party to another, usually from a merchant to the issuing bank.

Several card brands have used liability shifts to encourage adoption of EMV.

After the specified shift date, the liability for counterfeit card present transactions falls on the party that does not support EMV. For example, payment processors (that is, either the issuer or the merchant's acquirer processor) that do not support EMV transactions would be liable instead of merchants, if the merchant is unable to accept EMV payments as result.

MASKING:

A method of protecting a piece of data, typically the PAN, by concealing a segment of it when it is displayed or printed (not when it is electronically stored). For example, replacing all but the last four digits of the PAN with asterisks (that is, displaying 1234567890123456 as **********3456).

NAC

Network access control. Brings together multiple endpoint security technologies (such as anti-virus, IPS, and vulnerability assessment) and privilege management together into an integrated solution.

NTP

Network Time Protocol, a protocol for synchronizing the clocks of computer systems, network devices, and other system components.

OWASP

Open Web Application Security Project.

P2PE

PCI point-to-point encryption standard.

PA-DSS

PCI payment application data security standard.

PAN

Primary account number.

PCI

Payment card industry.

PCI PIN

PCI SSC managed standard setting the requirements for protection and handling PIN information from POI up to the issuers. Enforced by the card brands, not the SSC.

PII

Personally identifiable information, information that can be used to identify an individual: such as full name, date of birth, place of birth, telephone number, credit card numbers, or biometrics like fingerprints.

PIN

Personal identification number, a secret numeric password known only to the user and a system to authenticate the user to the system. See also PCI PIN.

POI

Point of interaction: the initial point where data is read from a card (that is, where a cardholder swipes or dips their card).

PTS

PIN Transaction Security, a set of modular evaluation requirements for PIN acceptance POI terminals. PCI PTS is a standard managed by PCI SSC.

QIR

Qualified Integrators and Resellers, a PCI SSC program.

QSA

Qualified security assessor: qualified by PCI SSC to perform PCI DSS on-site assessments.

REASONABLE ASSURANCE

See page 12.

RESIDUAL RISK

The risk that remains after implementation of security controls. Organizations should actively measure residual risk through continuous monitoring of their environment to verify that actual data protection matches the planned performance, and take corrective action if needed.

RISK MANAGEMENT

Risk management is the identification, assessment, and prioritization of risks followed by coordinated and economical application of resources to minimize, monitor, and control the probability and/or impact of unfortunate events (such as data breaches).

PCI DSS security control selection, design, and implementation should be a product of ongoing risk management. See page 69.

ROC

Report on compliance. See IRoC and FRoC.

SAD

Sensitive Authentication Data: information used to authenticate cardholders and/or authorize payment card transactions. Includes, but is not limited to full track data (the magnetic stripe or equivalent on a chip), CVV, and PINs.

SAQ

PCI DSS self-assessment questionnaire.

SCOPE

See DSS scope.

SECURE

See page 12.

SEGMENTATION

Partitioning of networks at a logical layer, dividing one part of a network from another, typically using one or more of firewalls, routers, and VLANs.

SEGREGATION

System segregation is normally used to create divisions between devices, not networks. Effective system segregation can be achieved using a combination of host-level restrictions based on IP address or MAC address, application-level filtering, and whitelisting.

SIEM

Security information and event management.

SIG

PCI DSS special interest group.

SSC

The PCI Security Standards Council.

SSL
Secure sockets layer: all current versions are considered weak and do not meet "strong cryptography" requirements. In February the SSC announced that it would be issuing DSS 3.1 that would prohibit the use of SSL, regardless of implementation strength or key length.

TLS
Transport layer security.

TOKENIZATION
Replacement of a sensitive piece of data (such as a PAN) with a unique but different piece of data — the token — that has no reversible mathematical relationship to the original data.

TRUNCATION
A method of rendering the full PAN unreadable. For example, shortening a 16 digit PAN by removing the first 12 digits leaving only the last four digits.

VALIDATED COMPLIANT
See page 12.

ZERO TRUST MODEL

This model takes a data-centric point of view and promotes a healthy distrust of internal and external users, packets, interfaces, and networks.

Traditional segmentation focuses on network partitioning to control "trusted" versus "untrusted" or "semi-trusted" network segments. Zero trust assumes that there are no trusted networks, interfaces, applications, traffic, or users:

- All resources are accessed securely, regardless of location.
- The principle of least privilege is followed, with granular data access control.
- All traffic is logged and inspected.
- Access to all data is controlled.

This approach is particularly effective in the extended enterprise, where IT infrastructure changes frequently and there's a need to manage and secure new connections from business partners, contractors and employees using non-company-owned (or controlled) devices such as smartphones and tablets.

Appendix C

Compliance calendar

REQ	AREA	DSS 3.0	ACTIVITY	DAILY	WEEKLY	EVERY X MONTHS	ANNUALLY	PERIODICALLY	AFTER CHANGES
	SCOPE MANAGEMENT	All	Confirm all locations and flows of CHD and ensure that they are included in the PCI DSS scope.				A		
1	FIREWALLS AND ROUTERS	1.1.7	Review firewall and router rulesets at least every six months.			6			
2	NONE	-							
3	DATA RETENTION	3.1.b	Identify and securely delete any CHD that's exceeded the defined retention period.			3			
	CRYPTOGRAPHIC KEYS	3.6.4	Change cryptographic keys that have reached the end of their cryptoperiod.					P	
4	NONE	-							
5	MALWARE THREATS	5.1.2	Evaluate threats to systems not commonly affected by malware to confirm if they require anti-virus software.					P	
	AV AUTOMATIC UPDATES	5.2.b	Maintain anti-virus software.					P	
	AV SCANNING	5.2.c	Run anti-virus scan.					P	
6	VULNERABILITIES	6.1	Review of vulnerabilities.			1			
	PATCH MANAGEMENT	6.2	Install applicable vendor-supplied patches: critical within one month, non-critical within three months.					P	
	APPLICATION VULNERABILITIES	6.6	Perform vulnerability assessment on public-facing web apps. Not applicable if you use web app firewall.				A		
7	NONE	-							
8	ACCESS MANAGEMENT	8.1.3	Revoke access for any terminated users immediately.						C
		8.1.4	Review user accounts and remove/disable inactive ones.			3			
9	PHYSICAL SECURITY	9.5.1.b	Review the security of backup media storage locations.				A		
	MEDIA INVENTORIES	9.7.1	Review media inventories.				A		
	POS DEVICES	9.9.2	Inspect POS devices for signs of tampering or substitution — for example, broken seals or incorrect serial numbers.					P	

PERIODICALLY

The term "periodic" appears 20 times in DSS 3.0, compared to just eight times in DSS 2.0. Many organizations interpret this to mean annually, but the SSC's intention is that each organization defines its own frequency based on its risk assessment.

AFTER CHANGES

There are several controls that specify action to be taken after "significant changes". This would include anything that could materially affect the security of your CDE, including:

- Changing network devices like firewalls, routers, and servers.
- Changing payment applications.
- Changing operating systems, including applying patches.
- Granting access to the CDE to a new service provider — even if they don't have access to CHD.

REQ	AREA	DSS 3.0	ACTIVITY	DAILY	WEEKLY	EVERY X MONTHS	ANNUALLY	PERIODICALLY	AFTER CHANGES
10	LOGS	10.6.1	Review of logs and security events for all CDE components to identify suspicious activity.	D					
		10.6.2	Review logs from other components based on the organization's policies and risk-management strategy.					P	
11	WIRELESS ACCESS POINTS	11.1	Test for the presence of all authorized and unauthorized wireless access points.			3			
	VULNERABILITY SCANS	11.2.1	Perform internal vulnerability scans as needed, until all "high-risk" vulnerabilities [control 6.1] are resolved.			3			
		11.2.2	Perform external vulnerability scans, via an Approved Scanning Vendor. Rescan until a pass is achieved.			3			
		11.2.3	Scan the internal and external networks for vulnerabilities.						C
	PENETRATION TESTS	11.3	Conduct a penetration test that includes a review of threats and vulnerabilities experienced in the last year.				A		
	CRITICAL FILES	11.5	Compare critical files using change detection mechanisms, such as file integrity monitoring software.		W				
12	POLICIES	12.1.1	Review the organization's security policies.				A		
	RISK ASSESSMENT	12.2	Conduct a formal risk assessment.				A		
	REMOTE ACCESS	12.3.9	Deactivate remote access for vendors and business partners when no longer required.						C
	AWARENESS PROGRAMS	12.6.1	Run awareness program for existing employees. Confirm they've read and understand the policy/procedures.				A		
		12.6.2	Run awareness program for new employees. Confirm they've read and understand the policy/procedures.						C
	SERVICE PROVIDERS	12.8.4	Monitor the compliance status of service providers.				A		
	INCIDENT RESPONSE PLANS	12.10.2	Test the organization's incident response plans.				A		
		12.10.3	Designate personnel to be available on a 24/7 basis to respond to alerts.	D					
		12.10.4	Train all staff with a role in security breach response.						C

Appendix D
Incident response

PCI DSS compliance isn't just about proving that you are 'in control' but also that you can remain in control during a crisis. Incident response planning is fundamental to enabling an organization to remain in control of events should a breach happen.

Interruption to the availability of IT systems would have a massive disruptive effect on most modern organizations. To counter that risk, companies have extensive business continuity (BC) and disaster recovery (DR) plans, but unfortunately this rarely extends to the confidentiality of data. Organizations often give incident response little attention until a crisis occurs and they are forced to try to regain control.

The part of the information security triangle that PCI DSS pays little attention to is availability.

The main role of post-incident response in PCI DSS is establishing the risk to the payment system, and as such has a strong focus on determining exactly what cards were exposed. It's in your interests, as those cards will need to be re-issued and you will be liable for the costs incurred by issuers, to be able to accurately identify which cards have been exposed.

So how can incident response be approached with the organization's own wellbeing in mind, in such a way that it not only complies with PCI DSS, but also provides real risk mitigation?

KEY THINGS TO KEEP IN MIND

You will need to know about the incident — either by detecting it or being notified about it — before you can start to respond. This means you need to know your environment, what is normal and be on your toes all the time. One could say PCI DSS has at least one whole Requirement — 10 — about incident response, though we usually say this is about tracking and logging access. The same goes for controls 11.4 [intrusion detection] and 11.5 [file integrity monitoring] at least.

Keeping your incident response processes and documentation up to date requires continuous alignment and work, just like BC/DR plans. And finding out that they aren't maintained after the event is not something you want to be responsible for.

Incident response is dependent on the actions of individuals in what are usually very stressful circumstances, so training, both awareness and practical, is critical. A single misstep by a system administrator might destroy the vital evidence (to identify the culprit and identify which data was compromised) and/or cause unnecessary panic.

Make sure you think about communication strategies. Both from a pragmatic point of view (if you have a large incident, simple things like email or administrative access to systems might not be available), and from a legal and exposure point of view. Who will contact the government agencies, your forensics specialist, the card brands, your customers, your partners? When and how will this happen? What are you going to say? Anything that helps to keep the perception of the outside world in your favor will pay off later.

PREPARE

If things go wrong, there's unlikely to be enough time to find people, hire external parties, look for a legal person to review press statements or to define a strategy to handle the pressure from your acquirer, the card brands or the parties you provide services to.

The security triangle

Figure 27: The information security triangle

Make sure external forensic assistance is available when you need it. Having a certified PFI partner on retainer might be a good idea. It also means there is no need to get these teams up to speed during a crisis — they are already familiar with your environment — and their experience could be valuable in your incident response planning and drills.

DESIGN

Look at your PCI DSS scope and think what signals can be used to detect that something is wrong. This way you can both determine logging and monitoring items you need to include for Requirements 10 and 11, and design them from the ground up to detect key indicators of compromise. Although it might be counterintuitive, approaching logging 'backwards' based on the needs of incident response is a good exercise to spot what was overlooked, or what can be addressed more efficiently.

As the focus of PCI DSS on logging and monitoring is the detection of incidents and after-the-event fact finding, it's important to have a clear incident response process. If your logging and monitoring provides the visibility PCI DSS requires, it is much easier to demonstrate to a QSA that you have a thorough understanding of your environment and answer their questions — and remember, the assessor determines the sample size required for validation based on their confidence in your control over your DSS scope.

SUSTAIN

Rigorously link the maintenance of the incident response procedures to both development processes (technical and business) and change management. Just like for disaster recovery, during a crisis you do not want to discover that your contact lists or procedures to safeguard evidence are out of date because they refer to departments or servers that no longer exist.

It's important to keep up to date with the latest changes in payment fraud detection to keep abreast of new techniques for both fraud and its detection to understand the threat landscape. It is often not difficult to tune your monitoring and logging systems to cover new indicators of compromise. And you will discover during such exercises that either you have overlooked methods to detect problems by simply correlating data or information that you already possess, or that you have blind spots you never thought of.

TEST

Put your incident response readiness to the test. And not just once a year to please your QSA, but regularly and after any significant changes to your business processes or technical environments. This will also help you keep your contact lists up to date and those persons prepared. Do not just test your technical responses focusing on detection and containment, but also on how you will communicate.

Effective incident response planning requires looking at business processes and assets and performing thorough impact analysis to determine credible threats, and devising ways of detecting attacks as soon as possible.

About Verizon's PCI Security Practice

Verizon is a highly respected security consultancy and a trusted voice in the PCI community. We have one of the largest and most geographically distributed teams of QSAs in the world. This gives us unrivaled insight into what it takes to implement sustainable controls and achieve compliance.

In the world of information assurance, knowledge is power. The figures speak for themselves: since 2009 we've conducted more than 5,000 assessments, most for Fortune 500 and large multinationals. Verizon has provided other cardholder data security services since 2003. We also gain valuable insight from running one of the largest global IP networks and managing over 4,000 customer networks. On top of all this experience, we have invested in extensive research programs, publish several of the industry's preeminent ongoing research reports, and made targeted acquisitions of leading security companies, such as Cybertrust.

We put all this experience and expertise to work for our clients in four main areas:

- **Advisory consulting:** As a world leader in payment security and PCI DSS compliance, Verizon's security consultants can help organizations of all shapes and sizes solve their most complex information security and compliance challenges.
- **Assessment and maintenance services:** As well as reviewing and validating PCI DSS compliance, we help companies maintain security and compliance through our compliance maintenance program, data discovery, and vulnerability scanning and penetration testing services.
- **Remediation services:** We offer a range of targeted remediation solutions leveraging our broad portfolio of security products and services.
- **Outsourcing:** Our range of hosting, cloud, and managed security services can reduce the burden of running, maintaining, and securing key IT services, helping to make achieving and maintaining security compliance easier.

Verizon's PCI Security Practice has been approved by the PCI SSC as QSA, PA-QSA, QSA (P2PE), and PA-QSA (P2PE). Verizon is also an approved PFI company. As well as security certifications, many of Verizon's QSAs have deep industry knowledge, gained from years of experience working in the retail, hospitality, financial services, healthcare, and other sectors. Being able to draw on this experience helps all our security professionals to appreciate your challenges, and to put compliance in the context of your industry-specific security standards and regulations.

For additional resources on this research and to find out more about Verizon's PCI Security compliance services, please visit verizonenterprise.com/pcireport/2015.

REFERENCES

1. Managing cyber risks in an interconnected world, PwC, 2015
2. Radius Global Market Research, Quirk's Marketing Research Review, June 2014
3. The global cost of payment fraud, BI Intelligence, 2014
4. Payment Solutions News, PNC Financial Services, Spring 2014
5. The Nilson Report, Nilson, May 2014
6. Poll Shows Broad Impact of Cyberattacks, Wall Street Journal, December 2014
7. Card Fraud in Canada, Canadian Bankers Association, 2008-2013
8. 2013 Microsoft Vulnerabilities, Avecto, 2013

REPORT DETAILS

LEAD AUTHOR
Ciske van Oosten.

CO-AUTHORS
Andi Baritchi and Rein van Koten.

CONTRIBUTORS
Aaron Reynolds, Ajeet Singh, Allen Mahaffy, David van der Merwe, Doug Smith, Eric Jolent, Ferdinand T. Delos Santos, Franklin Tallah, Gabriel Leperlier, Ian White, Jaime Villegas, John Galt, Jyri Ryhanen, Kim Haverblad, Mark Stachowicz, Marko Perucica, Markus Feichtner, Pierre Aure, Pierre-Emmanuel Leriche, Priyanka Bhattacharya, Raul Dolado, Ronald Tosto, Sebastien Mazas, Will Lawson, and Xavier Michaud.

This report would not have been possible without contributions of data and insight from across Verizon's security practice, particularly the QSA and RISK teams.

DATE OF PUBLICATION
March 9, 2015.

PCI SECURITY PRACTICE

GLOBAL MANAGING PRINCIPAL
Andi Baritchi.

GLOBAL INTELLIGENCE MANAGER
Ciske van Oosten.

MANAGEMENT TEAM
Aaron Reynolds, Auro Gaudeni, Eric Jolent, Gabriel Leperlier, Ian White, Jaime Villegas, Luc Didier, and Sebastien Mazas.

GRC CONSULTING PRACTICES

GLOBAL MANAGING DIRECTOR
Rodolphe Simonetti.

verizonenterprise.com