



VERIZON 2011 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

A Study Conducted By The Verizon PCI And RISK Intelligence Teams



2011 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

AUTHORS AND CONTRIBUTORS:

Listed in alphabetical order

- Wade Baker
- Andi Baritchi
- Tabitha Greiner
- C. David Hylender
- Jennifer Mack
- Martin McKeay
- Paul Mohl
- Aaron Reynolds
- Marc Spittler
- Ciske Van Oosten
- Other members of the Global PCI and RISK teams
- Special thanks to Carole Neal

TABLE OF CONTENTS

- Executive Summary2
- Introduction3
- Methodology4
- PCI DSS Assessment Results5
 - Overall Assessment Results.....7
 - Results by PCI DSS Requirement.....9
 - Detailed Results by PCI DSS Requirement..... 11
 - Requirement 1 (Firewall Configuration)..... 11
 - Requirement 2 (Vendor Defaults)..... 12
 - Requirement 3 (Stored Data)..... 12
 - Requirement 4 (Encrypted Transmissions)..... 13
 - Requirement 5 (Anti-Virus Software)..... 14
 - Requirement 6 (Development and Maintenance)..... 14
 - Requirement 7 (Logical Access) 14
 - Requirement 8 (Unique IDs) 15
 - Requirement 9 (Physical Access) 16
 - Requirement 10 (Tracking and Monitoring) 16
 - Requirement 11 (Regular Testing) 17
 - Requirement 12 (Security Policies)..... 17
 - PCI DSS Prioritized Approach..... 18
- Analysis of Investigative Response Data 20
 - Comparison to IR Assessments 21
 - Top Threat Actions..... 23
 - Backdoors 23
 - Physical Tampering 24
 - Authentication and Authorization Attacks..... 24
 - Data-capturing Malware 25
 - A Note on SQL Injection..... 26
 - In Summary 26
- What Contributes to a Better PCI Assessment? 27
- Conclusions and Recommendations 29

2011 PAYMENT CARD INDUSTRY COMPLIANCE REPORT

EXECUTIVE SUMMARY

This report analyzes findings from actual Payment Card Industry (PCI) Data Security Standard (DSS) assessments conducted by Verizon's team of Qualified Security Assessors (QSAs). The report describes where these organizations stand in terms of overall compliance with the DSS and presents analysis around which specific requirements are most and least often in place during the assessment process. Furthermore, we overlay this assessment-centric data with findings from Verizon's Investigative Response services to provide a unique risk-centric perspective on the compliance process. In a section new to this year's edition, significance tests are conducted to examine the relationship (or lack thereof) between various organizational practices and initial compliance scores.

- ✓ Essentially unchanged from last year, only 21 percent of organizations were fully compliant at the time of their Initial Report on Compliance (IROC). This is interesting, since most were validated to be in compliance during their prior assessment. What causes this erosion over the course of the year?
- ✓ Also similar to our prior report, organizations met an average of 78 percent of all test procedures at the IROC stage, with some variation in compliance scores. For instance, about 20 percent of organizations passed less than half of the DSS requirements, while 60 percent scored above the 80 percent mark.
- ✓ Organizations struggled most with the following PCI requirements: 3 (protect stored cardholder data), 10 (track and monitor access), 11 (regularly test systems and processes), and 12 (maintain security policies).
- ✓ PCI Requirements 4 (encrypt transmissions over public networks), 5 (use and update anti-virus), 7 (restrict access to need-to-know), and 9 (restrict physical access) showed the highest implementation levels
- ✓ Organizations do not appear to be prioritizing their compliance efforts based on the PCI DSS Prioritized Approach published by the PCI Security Standards Council—even less so than in the previous year.
- ✓ A mini-study comparing governance practices to the initial compliance score suggests that the way organizations approach compliance significantly factors into their success.
- ✓ Once again, organizations that suffered data breaches were much less likely to be compliant than a normal population of PCI clients.
- ✓ Analysis of the top threat actions leading to the compromise of payment card data continues to exhibit strong coverage within scope of the PCI DSS. For most of them, multiple layers of relevant controls exist across the standard.

INTRODUCTION

No field of human endeavor was ever born into a state of total maturity. From air flight to the construction of dwellings, human undertakings go through a long, often arduous process of evolution. One idea is placed slowly and carefully on top of another over a period of many years in an effort to arrive at that elusive point of ‘perfection’ or ‘completion.’ For instance, the medical practices that existed during Victorian England, while considered state of the art at the time, are not those we adhere to today. Practices experience a sort of ebb and flow as our understanding of how things work changes.

This concept is particularly applicable to the Information Security field. This profession as we know it today has not existed as long as some other, more established fields. While society has long been accustomed to the roles of doctors, lawyers, architects, etc., information security practitioners are relative newcomers. Barely ten years ago, the function of Chief Compliance Officer was largely unknown, and did not exist in the majority of organizations. However, while information security may not be enjoying the fullness of its maturity, it is certainly no longer in its infancy.

Information security exists for two distinct purposes: to enable an entity (a person, business, or government) to protect their own secrets, and to enable an entity to protect another entity’s secrets. The former will occur naturally—one is naturally incited to protect one’s own secrets. The latter, however, does not—it is an externality. As such, it is sometimes necessary to create regulatory bodies to ensure that these secrets are adequately protected.

Information security exists for two distinct purposes: to enable an entity (a person, business, or government) to protect their own secrets, and to enable an entity to protect another entity’s secrets.

Six years ago, to combat an increase of payment card breaches and associated fraud, the major payment card brands¹ joined forces to form the Payment Card Industry Security Standards Council (PCI SSC), and developed the Payment Card Industry Data Security Standard (PCI DSS). The PCI DSS was developed to encourage and enhance cardholder data security and facilitate the broad adoption of consistent data security measures globally. The Standard is managed by the PCI SSC and its founding members. All organizations that accept, acquire, transmit, process, and/or store cardholder data are obligated to continuously protect cardholder data to the minimum requirements set forth in the PCI DSS. They must prove compliance and report their compliance status annually.

In other words, compliance is a dynamic process and not a point-in-time event. The PCI SSC understood the fluid nature of both security and technology; in fact, its charter mandates that the standard continue to develop based on changes that occur within the industry. As our understanding of information assurance principles, risk management, and security governance grows and changes over time, the manner in which we go about protecting sensitive data will no doubt continue to evolve.

Of course, not everyone agrees on the relative value of PCI. Many feel that it’s a great leap forward in keeping sensitive data secure. Others, however, remain skeptical or downright critical of the standard. The latter camp contends that it’s a waste of resources, it’s too broad, the bar is set too high or too low, its effectiveness cannot be measured, and so on.

¹ The major payment card brands that formed the PCI SSC are: American Express, Discover Financial Services, JCB International, MasterCard Worldwide, Visa Europe and Visa Inc.

We can't conclusively confirm or refute these opposing points of view. What we believe we can do is provide actual data so that those who want to know the truth have something tangible by which to judge the standard. To that end, this report analyzes the findings of actual PCI DSS assessments performed by our Qualified Security Assessors (QSAs) over the past year. The report examines the progress of various organizations over a disparate geographic region as they struggle to achieve and maintain PCI compliance. The report also attempts to shed light on why some companies seem to be more successful than others, and which areas prove to be the most challenging.

We hope the findings and resultant discussion found in this document will be of assistance to organizations as they prepare their own compliance strategies. Whether beginning a compliance program, improving one that already exists, or successfully maintaining a currently compliant program, a realistic view of the current condition and common struggles of your peers should be beneficial to any organization. Lastly, we hope that in some degree this report will help to create a more secure payment card environment.

METHODOLOGY

The bulk of this report is based on actual PCI assessments conducted by Verizon's Qualified Security Assessors. The remainder comes from data gathered by Verizon's Investigative Response group while investigating real-world payment card data breaches. The primary focus is on over 100 Initial Reports on Compliance (IROC), Final Reports on Compliance (FROC) and, particularly in the case of foreign organizations, Gap Analyses conducted in 2010. This is a smaller pool of documents than in our last publication; where the previous effort covered a 24-month period, this represents a 12-month span. We frequently compare and refer to these 2008-2009 statistics throughout this report. All IROCs, FROCs, and Gap Analyses in 2010 were based on version 1.2 of the PCI DSS.

A wide variety of organizations are represented across these documents, including both merchants and service providers. While our previous report did include a small sample of reports from organizations outside the U.S., a more concerted effort was made across our regional teams this year to increase international representation and thereby illustrate the

global nature of the PCI guidelines. The resulting sample is approximately 60 percent American, 30 percent European, and five percent Asian, with the remainder distributed over other geographic regions.

While our previous report did include a small sample of reports from organizations outside the U.S., a more concerted effort was made across our regional teams this year to increase international representation and thereby illustrate the global nature of the PCI guidelines.

global nature of the PCI guidelines. The resulting sample is approximately 60 percent American, 30 percent European, and five percent Asian, with the remainder distributed over other geographic regions.

As for the assessment process itself, a QSA typically reviews current corporate policies, procedures, and diagrams of card dataflow before the initial site visit. Once on-site, the QSA interviews system administrators, programmers, security professionals, and other personnel to assess the overall level of compliance with relevant requirements. The QSA also determines whether systems and service maintenance procedures comply with PCI and company processes. Once the site visit is complete, the QSA delivers an IROC (or a gap analysis in parts of Europe and Asia). The time required to deliver this report typically ranges from two to six weeks; during this timeframe the client may focus on remediating issues found during the site visit. For most merchants and service providers, this represents a midway point toward achieving compliance. The FROC is issued when all requirements have been assessed and found compliant during the course of the engagement.

In order to create an additional dimension to this year's report, QSAs were asked to fill out a short survey assigning a subjective rating² for each organization's approach to several governance practices, which we recommended last year. We then compared these ratings to initial compliance scores (percent of test procedures met at the IROC) to test for a statistically significant relationship. A more detailed description of the testing methodology is provided later in this document.

Finally, Verizon values its clients' privacy and anonymity. During the creation of the analysis dataset used for this report, no identifying information was ever extracted from the Reports on Compliance (ROCs). The aggregated data includes only basic organizational characteristics (e.g., merchant type) and assessment results (e.g., in-place). Additionally, the data collection and analysis process was conducted in cooperation with Verizon's RISK team, which has years of experience handling sensitive, anonymous information for the Data Breach Investigation Report series. Furthermore, the findings in this report are presented in aggregate; we never call out results pertaining to particular organizations.

PCI DSS ASSESSMENT RESULTS

While there has always been a relationship between security, compliance, and validation, it's all too easy for people, even those in the security field, to conflate all three concepts as one and the same. This is probably because unless you're performing the work on a daily basis, you really don't have much need to understand the difference. Luckily though, a few years of people banging the drums with the refrain "Compliance doesn't equal security!" appears to have made all but a few holdouts realize that just because they're compliant with the PCI DSS requirements, they may not be secure from everything the Internet has to throw at them. Or perhaps recent headlines have made companies more aware that they're not as secure as they thought. Whatever the reason, we find the result encouraging.

In the interest of clarity, we will briefly outline how we define these concepts. Compliance is the continuous state of adhering to the regulatory standard. In the case of the PCI DSS there are daily (log review), weekly (file integrity monitoring), quarterly (vulnerability scanning), and annual (penetration testing) activities that an organization must perform in order to maintain this continuous state of compliance.

Validation, on the other hand, is a point-in-time event. It is a state of nature analysis that attempts to measure and describe the level of adherence to a standard at a given point. An organization may be able to pass validation in order to achieve compliance but then—once the QSA leaves—become lax about maintaining the degree of security the standard is designed to provide over time. As such, the goal of any organization should be to maintain its state of security at all times in adherence with the minimum baseline compliance requirements set by the standard.

In the end, the goal is security, and security is a continuum between 'I just put my new Windows 95 system directly on the Internet' and 'I unplugged my computer and buried it six feet under.' On the secure end, you have organizations that have made security a core value of their company. These may be companies that sell security as part of their service, which realize the value of making their data as secure as they possibly can, given the requirements of their business.

Compliance is the continuous state of adhering to the regulatory standard. In the case of the PCI DSS there are daily (log review), weekly (file integrity monitoring), quarterly (vulnerability scanning), and annual (penetration testing) activities that an organization must perform in order to maintain this continuous state of compliance.

² It is important to recognize that only the QSA survey was subjective; the remainder of the report is based on actual assessment data.

At the other end of the spectrum are businesses that just want to get on the Internet and don't care about or understand the risks associated with being online. In truth, most businesses are somewhere in the middle. It is often the visibility of security within an organization and the will of management to be secure that is more telling than the technologies or tools that a corporation has in place.

Payment card data breaches are an economic externality, and PCI's mission is to ensure that companies take better care of consumer payment card data. Just as an oil spill affects millions of people, so does a 'data spill.'

Payment card data breaches are an economic externality, and PCI's mission is to ensure that companies take better care of consumer payment card data. Just as an oil spill affects millions of people, so does a 'data spill.'

Compliance, especially the PCI DSS requirements mentioned above, aims at setting a baseline of security controls in the hope they'll be sufficient to keep organizations secure enough to continue doing business. The 12 primary requirements in the PCI DSS, when written, aimed at securing cardholder information, the cardholder data environment, and communications containing cardholder data; in other words, your credit card transactions. In order to be considered compliant, an organization must be in accordance with the requirements at all times. This is part of why the idea of 'compliance through security' works. An organization that has worked security into their daily process can more easily maintain these efforts than one that is performing them merely to meet a validation effort.

When a QSA or organization talks about validation, about having been assessed and having received a Report on Compliance, they mean a point-in-time snapshot of the organization's environment; i.e., the time that a QSA is reviewing

documentation, on-site performing assessments and interviews, as well as writing the resulting report. The PCI DSS validation strategy makes use of sampling in environments, so in most cases it is not all systems that are being reviewed, but enough to provide an expectation that the sample is representative of the systems as a whole. In other words, the QSA is looking at a relatively small number of systems over a relatively short period of time. There are enough PCI requirements and systems involved, however, that it is nearly impossible to go through a PCI assessment without finding some system or process that hasn't broken since the last time it was reviewed.

Unfortunately, the world is a messy place and there is no direct relationship between passing a point in time validation and being able to maintain compliance after the assessor has left. Nor is there any direct proof that either of these two actually led to a more secure environment. However, we still maintain the effort required to meet the PCI DSS guidelines for a very simple set of reasons. For one thing, we have to do something, and the bar set by the PCI guidelines is higher than the security of many businesses. Even if PCI isn't the perfect solution to this problem, in a large number of environments the security controls mandated by the PCI DSS provide a higher level of security than was previously in place. However, it also requires a much higher level of security expenditures.

Many organizations have a hard time sustaining the efforts required to be compliant year after year. Even the best organizations make mistakes, but all too many businesses simply put a band-aid over bullet holes in the hope that the effort will last until the assessor has left. This report discusses the level of compliance businesses had at the point of validation, and may allow us to make inferences about the continued compliance efforts of an organization and the security that results from those efforts.

Overall Assessment Results

In the pool of assessments performed by Verizon QSAs included in this report, 21 percent were found fully compliant at the completion of their IROC. This is just one percent less than in our last report, and effectively the same number. This lack of change is a bit disappointing, as many in the industry were hoping to see an increase in overall compliance as the PCI DSS became more familiar to an increasing number of organizations. Looked at from the other perspective, this means that 79 percent of organizations were not sufficiently prepared for their initial assessment.

Having established that only 21 percent “passed the test” (i.e., met all requirements by their IROC), the next question becomes “what was their score?” (i.e., percentage of all requirements met). On average, organizations met 78 percent of all test procedures defined in the DSS at the time of their IROC. This is down three percent from our last report; but again, the difference is nominal. Most of these organizations have had multiple chances to become familiar with the PCI assessment process and one would think they should become more able to meet requirements year after year. So why aren't they?

There is no clear and easy answer to this question, though we can draw several inferences from the statistics. The most obvious is that compliance is not a simple matter. PCI DSS is not a group of easy controls, and it is apparent that they aren't inherent in most security programs. Although a few of the companies can claim that it's their first rodeo, they haven't yet demonstrated mastery of PCI DSS. Therefore, the baseline set by the PCI DSS must not reflect the baseline set by the companies themselves. For most organizations, to achieve compliance they must do things they were not previously doing (or maintaining). Of course, whether or not these are the right things to be doing is a separate question and one that we touch upon later in the Analysis of Investigative Response Data section of this report.

Another common Achilles heel of merchants and service providers in the PCI assessment process is overconfidence. “It was painful, but we made it through last year, so this year should be a breeze,” is a typical sentiment with which many organizations approach the yearly assessment. That can be a costly mistake. When the QSA arrives on-site, a mere one-fifth of businesses are found to be compliant, even when given the extra time between the on-site visit and completion of the IROC.

Complacency and fatigue are two additional drags that make maintaining compliance year over year difficult. Too many businesses approach PCI from the point of view that “what was good enough last year will be good enough this year.” But unless someone's been babysitting a process, such as documenting and justifying all services allowed through the firewalls, things can easily be forgotten in the haste to get business done.

Figure 1. Percent of organizations found compliant at IROC.

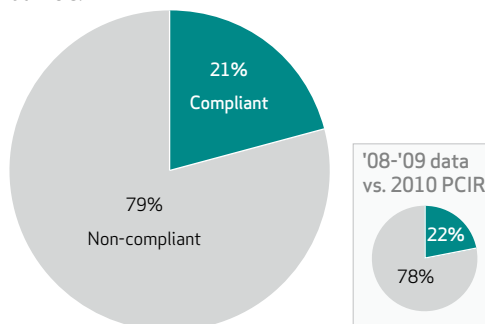
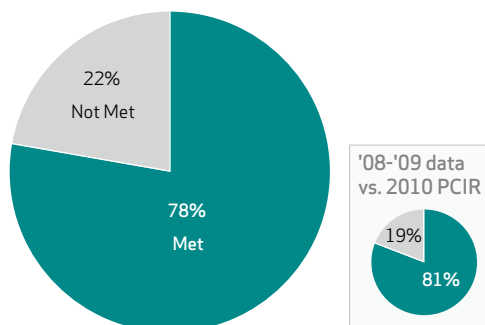


Figure 2. Percent of testing procedures met at IROC.



Fatigue will always be the enemy of security and compliance professionals, as it's a never-ending battle to protect the organization. When faced with a choice of where to place their energies, many people will choose to just get things done

When the complexity of PCI is added to the mix, with well over 200 requirements where failing even one means non-compliance—you have a genuinely formidable mix of circumstances.

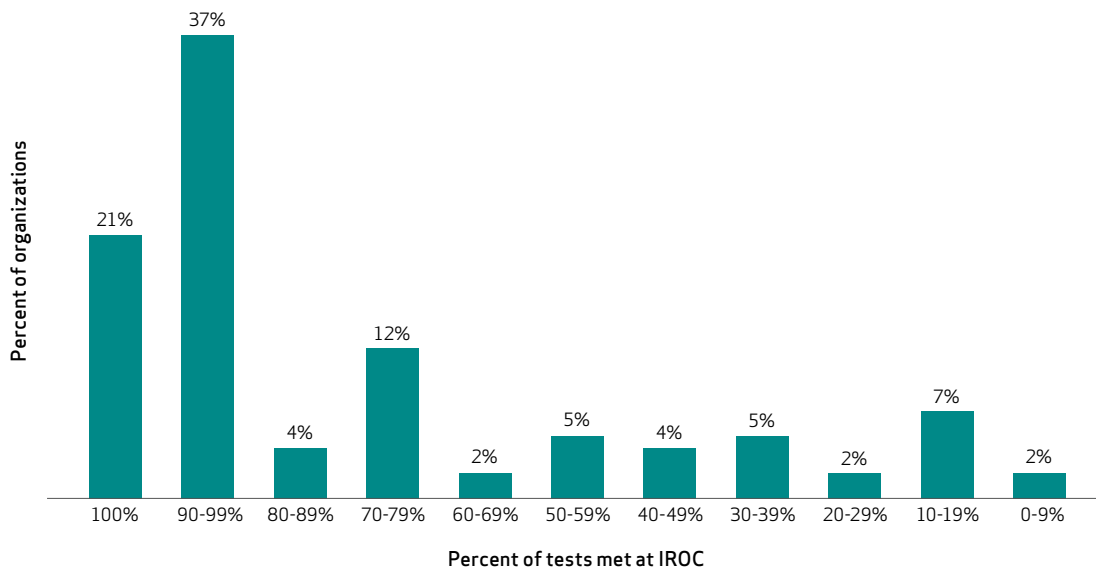
rather than worrying about the 'right way' or the 'compliant way'. The organization might take notice of PCI while the QSA is on-site, but afterwards allow a significant portion of the necessary practices to erode over time.

There are any number of other challenges including manpower, resources, corporate will, and complexity. Finding an IT or security department fully staffed to the level needed is rare; most organizations either may not have adequately accounted for the manpower resources required or have not found individuals with the right expertise to fill the positions they have. Security and, by extension, compliance, are still considered to be a drag on the economy by most businesses rather than an assumed part of the risk of doing business. This makes getting the resources needed to perform compliance

and security correctly difficult. Too few companies have a manager or director in charge of compliance efforts, and lack an informed sponsor at the senior or executive level within the corporation to provide support and guidance for projects. When the complexity of PCI is added to the mix, with well over 200 requirements where failing even one means non-compliance—you have a genuinely formidable mix of circumstances.

These findings are even more worrisome since, as time goes by, compliance with the assessment standards only gets harder, not easier. The PCI Council continues to give clarification and guidance on interpreting the standards, often narrowing and redefining acceptable practices. Performing that which was acceptable for one year's assessment is no guarantee of being compliant a second time if the guidance has changed. This will become increasingly true as the PCI DSS 2.0 requirements are used for all assessments starting in January 2012.

Figure 3. Distribution of testing procedures met at IROC.



All this hints at very different problems within these organizations, and very different solutions needed to address them. Understanding one's own particular stance and challenges with respect to compliance (or validation) is an important task. To offer additional help in that regard, we dig further into the state of compliance among the 12 requirements specified within the PCI DSS.

Results by PCI DSS Requirement

So far in this report we have illustrated that the majority of organizations do not meet their goal of 100 percent compliance upon initial assessment, which, considering there is no room for error, is not terribly surprising. We have also discussed at some length just how far off the path they may have wandered. While this data is certainly interesting and informative at a high level, it becomes both more valuable and actionable with increasing detail. Specifically, which requirements are readily achieved by organizations and which prove more difficult? There are two ways one can approach this question; either by identifying the percentage of organizations validated compliant with each of the 12 requirements or by identifying the average percentage of testing procedures (tests) within each requirement that were met at the time of the IROC. We attempt to look at the data from both points of view, and the results are depicted in Table 1.

When examining the percent of organizations passing each requirement at the IROC phase, one notices considerable variation. Some requirements show percentages dipping below 40 percent, while others exceed the 70 percent range. Six of the twelve show an increase over last year, and the average is up two points. However, the average number of test procedures met within each requirement is down four percent. None of these numbers is indicative of a clear change given the size and makeup of the dataset, but it certainly reinforces the notion that organizations continue to struggle (at varying degrees) in all areas of the DSS.

According to Table 1, Requirements 4 (encrypt transmissions), 5 (AV software), 7 (logical access), and 9 (physical access) once again proved the least difficult for organizations to pass in 2010. Requirement 10 (tracking and monitoring) boasted the highest gain (+13 percent), which we find perplexing given what we know from other studies about organizations' low awareness of network activity. If it continues to slide, Requirement 5 (AV software) may lose its place in the top three, which would be an odd development, since AV software has for so long been among the most basic and widespread of security controls. The improvement in compliance to Requirement 4 (encrypt transmissions) may indicate that administrators are deciding it's easier to direct all Internet traffic containing credit card data over SSL. Meanwhile, the small improvement in Requirement 7 (logical access)—if significant at all—could mean more strict attention is being paid to who is given access to cardholder data. (But we doubt this; a year is simply not enough time to measurably impact as pervasive an issue as over-privileging.)

Requirements 3 (stored data) and 11 (regular testing) are once again in the bottom tier, while Requirement 12 (security policies) ousted 10 (tracking and monitoring) from the bottom. This suggests that the encryption of data at rest continues to be a major headache for organizations, especially the more detailed portions, such as annual key rotations. Requirement 11's low showing reminds us why 'set and forget is a very bad bet' should be a core mantra of the security profession. The fact that security policies rank among the lowest of the low is not a good sign since policy drives practice.

The fact that security policies rank among the lowest of the low is not a good sign since policy drives practice. Without clear statement of what you want to do, how can you expect to reliably do it?

Table 1. Assessment findings at IROC by PCI DSS Requirement.

| PCI DSS Requirement | % of Organizations ^{**} | | % of Tests ^{***} | |
|---|----------------------------------|------------|---------------------------|------------|
| | '08-'09 | 2010 | '08-'09 | 2010 |
| 1: Install and maintain a firewall configuration to protect data | 46% | 44% | 82% | 78% |
| 2: Do not use vendor-supplied defaults for system passwords and other security parameters | 48% | 56% | 77% | 74% |
| 3: Protect Stored Data | 43% | 42% | 75% | 71% |
| 4: Encrypt transmission of cardholder data and sensitive information across public networks | 63% | 72% | 83% | 84% |
| 5: Use and regularly update anti-virus software | 70% | 64% | 86% | 80% |
| 6: Develop and maintain secure systems and applications | 48% | 53% | 83% | 77% |
| 7: Restrict access to data by business need-to-know | 69% | 75% | 87% | 87% |
| 8: Assign a unique ID to each person with computer access | 44% | 47% | 82% | 77% |
| 9: Restrict physical access to cardholder data | 59% | 55% | 91% | 84% |
| 10: Track and monitor all access to network resources and cardholder data | 39% | 52% | 75% | 70% |
| 11: Regularly test security systems and processes | 38% | 37% | 70% | 65% |
| 12: Maintain a policy that addresses information security | 44% | 39% | 83% | 79% |

Lowest three values denoted in red and highest three are in bold.

* i.e., 44% of organizations in 2010 fully met Requirement 1 at time of IROC.

** i.e., organizations in 2010 met an average of 78% of tests in Requirement 1 at time of IROC.

Without clear statement of what you want to do, how can you expect to reliably do it? Physical (Requirement 9) and application-level (Requirement 6) security also posted lower numbers, further proving struggles at all levels of the stack.

In the next section we'll delve deeper into each individual requirement, but before doing so, let's put these findings into perspective. Similar to most business processes, security can be broken down into a recurring plan-do-check-act (PDCA) cycle. The planning phase consists of assessing risk and establishing risk tolerance; creating and updating policies, procedures, and programs that reflect this tolerance; and otherwise identifying what the organization must do with respect to security. With this done, the organization will begin to do (implement) the things that turn the plan into practice. Next, smart organizations will check (validate) to make sure these practices are done well, according to plan, and functioning properly. If not (which is often the case), various actions will be required to remediate the discrepancy and maintain proper implementation of the plan. In relation to the PCI DSS, these phases can be viewed as follows:

- **Plan:** Requirement 12
- **Do:** Requirements 1, 2, 3, 4, 5, 6, 7, 8, 9
- **Check:** Requirements 10, 11 (though 1-9 contain checks too)
- **Act:** All requirements as needed, particularly those listed in the 'Do' phase

Examining this breakout against Table 1 shows that organizations are still better at Planning and Doing than at Checking in 2010. *Planning* got a little worse, the *do's* were a mixed bag, and *checking* improved for network activities, but was a little lower for systems and processes. The jury's still out on *acting*, since it's tough to get a bead on it within just one year. Knowing where others stand is helpful, but the really important question is how are YOU doing at PDCA? Answer that honestly, and you're likely to find your compliance and security efforts more manageable.

Detailed Results by PCI DSS Requirement

One of the highlights of working with data is that you are occasionally allowed to see trends emerging, whether an indicator is going up, down, or nowhere. However, since this is only the second year that we have published this report, we will not claim that advantage just yet. Nevertheless, it is interesting to see what the data tells us even over a relatively short time span of two or three years³. Overall, neither the ranking nor the compliance with the higher-level PCI requirements changed considerably from last year. However, when investigating the requirements individually, there are a few that demonstrate points of interest. In this section, we attempt to evaluate each specific requirement, with particular attention given to anything that may have helped or hindered the organization to meet and/or maintain compliance. As mentioned above, two reports covering three years of data is not enough to extrapolate real trending, but it does provide indicators that raise some interesting questions.

Requirement 1 (Firewall Configuration)

Requirement 1 remains virtually unchanged since last year, at 44 percent compliance, compared to the 46 percent who were found compliant at the time of the IROC in the previous report. This means that nearly half of all corporations are still failing to meet with some aspect of the documentation of their network, firewalls, and routers. It appears that the most difficult part of meeting this requirement is the documentation of network device configurations, with only 63 percent of companies meeting Requirement 1.1.5 regularly. As we mentioned last year with regard to this requirement, in many cases the traffic was being properly restricted but the corresponding paperwork was not up to par. Often companies possess the documentation; however, it's frequently outdated. In these cases what is actually in place doesn't meet with any of the standards written. In part, this is supported by the fact that only two-thirds of the ROCs found companies to have proof that bi-annual firewall reviews, Requirement 1.1.6b, actually took place.

Restricting inbound access (PCI Requirement 1.2.1) continues to be an issue for many being audited, with 23 percent of businesses found to be non-compliant at the time of the assessment. As in last year's report, most organizations still have limited outbound access controls, and the process of implementing them can be painful. Insecure traffic, such as FTP and Telnet, is still flowing through many networks. Web servers continue to host file and mailing list services. Most businesses don't have anyone with the time to dig into every rule in the firewalls to understand the complete rule sets. To be blunt, organizations often understand the big picture of how the network functions, but if the QSA points to a specific rule and asks why it's in place on a specific firewall segment, he or she will typically be met with a blank stare.

Let's face it—hackers are vigorously and repeatedly trying to penetrate your network and siphon out your secrets (and/or cardholder data). The firewall is the first line of defense, but only works if tuned and maintained properly.

³ The 2011 Payment Card Industry Compliance Report reflects 12 months of data. The 2010 report reflected 24 months of data.

Requirement 2 (Vendor Defaults)

Readers of the DBIR will recognize the familiar refrain that criminals go for the low-hanging fruit or targets of opportunity. Perhaps administrators are slowly beginning to appreciate the validity of this statement. This year the IROCs show Requirement 2 (Do not use vendor-supplied defaults for system passwords and other security standards) exhibited modest improvement, up to 56 percent in compliance from 48 percent the year before. This was despite the fact that the percentage of tests passed by organizations was down slightly. The most significant change within this group was the requirement to change vendor-supplied default passwords, which was up to 82 percent from 48 percent. Hopefully this means that in hindsight, systems administrators are learning that leaving the default username and password as 'admin' and 'admin' on the routers was probably not a good idea.

Unfortunately, Requirements 2.2.3b (secure system configuration) and 2.2.4 (remove unnecessary services) both remain low, at 74 percent and 67 percent respectively. Almost all systems administrators profess to know how to configure a system to be secure (Requirement 2.2.3a), but when it comes down to building and maintaining a system in a compliant manner (Requirement 2.2.3c), we're still failing in over a quarter of all cases. This is perhaps not surprising given that system configuration takes time, something that is always at a premium in most IT organizations. Additionally, new configuration guidelines are difficult to implement, but we remain hopeful that this requirement will continue to show an increase in the future.

Requirement 3 (Stored Data)

It is often the case that merchants who process and transmit data will also store that data. In many instances they store it unnecessarily; nevertheless no one will be floored by the finding that organizations continue to seriously struggle with meeting PCI Requirement 3 (Protect stored cardholder data). New technologies such as end-to-end encryption and tokenization are apparently having little effect, since at 42 percent, there has been no change from last year. Encryption

With the release of PCI 2.0 and the increased need to prove that a method exists to find all cardholder data stores and protect them appropriately, the encryption of data will become even more important to merchants.

of data at rest, as any security professional can tell you, is not an easy technology to implement even in the best of times. Finding a clear-cut solution that will work in all situations is even more difficult. With the release of PCI 2.0 and the increased need to prove that a method exists to find all cardholder data stores and protect them appropriately, the encryption of data will become even more important to merchants. In other words, you need to perform data discovery and make sure some developer isn't keeping a stash of copies of the live databases for testing purposes. Although this change is not contained in a specific PCI requirement, Requirement 3 will expose the problem during assessments.

As we allude to above, keeping stored cardholder data to a minimum seems to be a particularly difficult task for many companies. Not unlike most other scenarios in which a plan is required, you will seldom find an organization that does not have a clearly stated data retention plan specifying a time frame in which the data will be removed. However, finding one that can and actually does adhere to the plan is another matter altogether. The reasons for this can include a lack of resources, a simple failure to check to see if the task was carried out, a lack of knowledge regarding

where exactly the data resides, and even ongoing legal battles that require keeping data for extended lengths of time.

So it shouldn't be a huge surprise that 33 percent of businesses were unable to meet with Requirement 3.1 (keeping storage of cardholder data to a minimum). From discussions with merchants by our QSAs, it would appear that companies are slowly realizing the best way to secure cardholder data is to not have it, but this isn't showing up in our numbers yet. There remains a great deal more data gathering and storage going on by many merchants than there should be. Granted, 80 percent of merchants did not store sensitive authentication data, but that still means 20 percent of merchants were doing so at the time of the assessment. Card Verification Value CVV and PIN blocks were kept in similar amounts, with CVV retained in 23 percent of cases and PIN block data found in 18 percent of corporations. Given the large amount of data collected, it is alarming that Requirement 3.4, encrypt cardholder data, is met only 63 percent of the time. In other words, there's a lot of data being collected and not protected properly. This is evident when one considers the type and number of compromises within the last year.

Another problem area continues to be the annual key rotation, Requirement 3.6.4. This requirement is met in only 61 percent of cases, meaning that roughly a third of all businesses assessed continue to use encryption keys beyond their valid dates. Does this materially affect the security of the data if compromised? Probably not, but why does it continue to be an issue? Most implementations of encryption should provide a method for replacing keys, and key rotation is supposed to be in the annual schedule, so there's no understandable reason this number should continue to be so low.

Requirement 4 (Encrypted Transmissions)

Over time it has become much clearer to those involved with PCI exactly what Requirement 4 (Encrypt transmission of cardholder data across open, public networks) means, as evidenced by the rise in overall compliance with this requirement: from 63 percent to 72 percent. In general, organizations better understand exactly how to encrypt data in motion. Most businesses (83 percent) are making a concerted effort to comply with Requirement 4.2 by not taking payment information via e-mail. In many instances, they are going beyond simply making it a policy and are backing it up with automated filtering at the mail servers that deny any e-mails containing cardholder data. When the merchant is informed that accepting the occasional e-mail transaction will mean the entire mail system will be in scope, it becomes easier for them to justify these capabilities. Faxes still happen, but more often in a locked room to which only a few people have access.

Many businesses have segmented their wireless networks and no longer allow any PCI-regulated traffic containing sensitive cardholder data to flow over the airwaves.

Removing WEP (Wired Equivalent Privacy) from the list of allowable encryption for wireless traffic in June of 2010 seems to have helped companies comply with this requirement as well. We mentioned in last year's report that we expected this to be the result. Many businesses have segmented their wireless networks and no longer allow any PCI-regulated traffic containing sensitive cardholder data to flow over the airwaves. The rest have, for the most part, upgraded to systems using Wi-Fi Protected Access (WPA) and WPA2 to secure their wireless networks.

This is one of the larger increases in overall compliance with a set of requirements, and it is in part due to the narrow scope of Requirement 4. Dealing simply with the data in motion makes this requirement easy to understand and quantify, which leads to less miscommunication between the QSA and the company being assessed.

Requirement 5 (Anti-Virus Software)

Requirement 5 (Use and regularly update anti-virus software or programs) dropped from 70 percent last year to 64 percent this year. There is no single cause apparent in the sub-requirements and is likely simply related to the sample. The never-ending controversy of what systems are 'commonly affected by malware' is certainly not helping the situation.

The effectiveness of anti-virus (AV) remains contested in some circles, but there's no denying that AV is a required technology from a PCI standpoint.

The effectiveness of anti-virus (AV) remains contested in some circles, but there's no denying that AV is a required technology from a PCI standpoint. After all, although it may not be perfect, it is an additional layer of defense. Keep in mind that there may be other options and compensating controls that can be used to meet this requirement. For example, a whitelist approach, where only verified-trusted programs are allowed to be executed may satisfy this requirement using fewer CPU and Input/Output (I/O) resources and negating the need for periodic updates.

Requirement 6 (Development and Maintenance)

Requirement 6 (Develop and maintain secure systems and applications) is up from 48 percent overall compliance to 53 percent. Patching itself is still an issue, as only 74 percent of businesses were able to make certain that all systems were properly patched at the time of the IROC. Although patching Operating Systems is still an area in which organizations struggle, it's often the unpatched network equipment that is noticed by QSAs. This is mostly because network equipment is not always covered by an automated patching process. In fairness to the merchants, it should be noted that this requirement is especially difficult to comply with since any single system in the PCI environment not up to current patch level on the day of the assessment will result in a failure.

Secure coding practices also continue to be a problem. While 95 percent of all developers state they understand and utilize secure coding practices when interviewed (Requirement 6.5b), many do not actually have either the opportunity or know-how to do so in practice. Organizations seem to be coming to grips with change control processes; 91 percent met with the 6.4 Requirements. However, the numbers begin to slip into the 80 percent range when it comes to complying with separation of the testing and production environments (6.3.3), coding of internal applications (6.4), and websites (6.5).

Requirement 7 (Logical Access)

'Need to know' and 'Principle of least privilege' are fundamental security practices that have existed much longer than Requirement 7, and both seem rather straightforward: only those who need to know sensitive information are given access to it.

It could be perceived that this requirement is one of the easier ones to implement based on the compliance percentages from our past two reports. The percentage of organizations fully meeting Requirement 7 at time of IROC was 75 percent, an eight percent increase over the 2010 report results. Same as last year's results, organizations met an average of 87 percent of tests in Requirement 7 at time of IROC—the highest among all twelve key controls.

While the concept is simple, the ability to validate with a strong degree of certainty is not. PCI QSAs must rely on attestations from the client that they have identified (completely and correctly) the personnel requiring access to the information. Additional validation methods such as policy review and high-level demonstrations of access control rules can only uncover more binary gaps in compliance, as detailed below.

Organizations are required to have a policy and documented process in place to limit access to cardholder data, and must verify that their policies are up to date. Most organizations do have the technology to support this requirement but fail to meet it in full due to lack of a documented and enforced access control policy.

Another common pitfall is failure to automate the process of identifying and maintaining a list of authorized personnel. When people get promoted or transferred to another position and/or business unit, they should not accumulate privileges.

It is essential to maintain the systems that enforce the policy on access control, which include properly configuring directory services such as Active Directory or LDAP, and frequently reviewing the configurations. Most organizations can meet the challenge of deploying role-based access control systems, to ensure privileges are assigned to individuals based on job classification and function, and maintaining a default 'deny all' posture. When implementing access controls, several organizations are still focusing too much on the network perimeter. The policies and related procedures should include all the system components that are in scope. This must include clear procedures for maintaining access control at the application level as well.

Requirement 8 (Unique IDs)

PCI DSS Key Requirement 8 mandates that you assign a unique ID to each person with computer access to sensitive data. This requirement is applicable for all accounts, including point-of-sale accounts, those with administrative capabilities and all accounts used to view or access cardholder data or to access systems with cardholder data. Moreover, the sub-requirements address numerous account management controls, including password parameters, lockouts, and disabling inactive accounts.

More than half of organizations failed to meet Requirement 8 at time of the IROC. Of all the compliance validation tests for Requirement 8, organizations met an average of 77 percent at the time of IROC.

The results from our analysis of Requirement 8 indicate sub-requirement 8.3 (Ensure proper user authentication and password management for non-consumer users and administrators on all system components) and 8.5.7 (Communicate password procedures and policies to all users who have access to cardholder data) rate among the best implemented compliance test procedures within the main compliance requirements.

Sub-requirements 8.4 (Render all passwords unreadable during transmission and storage on all system components using strong cryptography) and 8.5.10 (Require a minimum password length of at least seven characters) were the *least* compliant at the time of IROC.

Most organizations do communicate their password policies and standards internally, but still experience difficulty enforcing them across all computing devices. It is essential that organizations use an enterprise-wide authentication framework that will enforce established password parameters. Decentralized enforcement of password policies and standards should be the exception (e.g., legacy systems), not the norm.

It is essential that organizations use an enterprise-wide authentication framework that will enforce established password parameters. Decentralized enforcement of password policies and standards should be the exception (e.g., legacy systems), not the norm.

Requirement 9 (Physical Access)

Five of the test procedures defined by Requirement 9 were passed in 95 percent or more of the assessments within our dataset. As we stated in the previous year's report, physical access controls are found by many to be more tangible than logical access controls.

Sub-requirements 9.3, 9.4 (employee/visitor controls), and 9.6 (secure physical delivery) rate among the best implemented compliance test procedures. Yet, for the second year, our research indicates that only about half (55 percent) of organizations fully met Requirement 9 at the time of IROC. On average, 84 percent of tests were fully met in Requirement 9 at the time of IROC, a seven percent reduction from our 2010 results.

The most challenging sub-control, at time of IROC, is 9.9.1: Properly maintain inventory logs of all media and conduct media inventories at least annually.

Several other controls in Requirement 9 remain challenging for some organizations—in part due to the interpretation of the intent of the controls. There is often confusion regarding treatment of onsite employees vs. visiting employees vs. third-party visitors. Literal interpretation of the standard by some has resulted in the substitution of the word 'employee' with 'onsite personnel' in PCI DSS 2.0. The specific definitions of onsite personnel and visitors should further clarify the requirements and intent of sub-requirements 9.2 and 9.3.

Despite widespread usage, some organizations are resistant to the implementation of some physical security controls, such as visibly displaying badges to distinguish employees from visitors. Policies to define and enforce the "what," combined with security awareness training to staff to educate them on the "why," are necessary for changes to be implemented in some environments used to a more open atmosphere.

Requirement 10 (Tracking and Monitoring)

Although the requirement calls for the tracking and monitoring of all access to network resources and cardholder data, the main objective is to maintain system logs and have procedures that ensure proper utilization, protection, and retention. The sub-requirements are designed to help ensure that logs are monitored for proactive detection of issues and archived in a secure manner to allow for use in forensic investigations as needed.

Requirement 10 is historically one of the most challenging key controls to meet. Organizations continue to find enterprise log management a challenge, most notably with generating (10.1 and 10.2), protecting (10.5), reviewing (10.6), and, to a lesser extent, archiving (10.7) logs. The sub-requirements within Requirement 10 feature many dependencies, and non-compliance with one can have a negative cascading effect on the remaining controls.

Compliance with Requirement 10 did realize an increase this year. 52 percent of organizations fully met Requirement 10 at the time of IROC, representing a 13 percent increase from last year's data set. On average, organizations met 70 percent of tests in Requirement 10 at time of IROC, a five percent decrease from 2010. Our assessments continue to reinforce our finding that organizations typically have fewer problems implementing logging on network devices and operating systems but are less successful with regards to application log management.

According to our analysis, the most challenging sub-control appears to be 10.5.5: Use file-integrity monitoring or change-detection software on logs to ensure that existing log data cannot be changed without generating alerts. File-integrity monitoring can be extremely complex and expensive to implement.

Other pitfalls towards compliance with Requirement 10 are the failure or inability to invest in a capable automated tool (log aggregator) to monitor logs on a daily basis, not maintaining security procedures to trigger a response to an exception report, and the inability to test implementations of log archival (e.g., the recovery and correlation of a full audit trail).

Requirement 11 (Regular Testing)

With only 37 percent of organizations fully meeting Requirement 11 at the time of IROC, it is the least compliant key control of the PCI DSS standard based on our compliance status assessments. Many organizations perform inadequate or no regular testing on the effectiveness of the security controls governing their cardholder data environments. Organizations met an average of 65 percent of tests in Requirement 11 at time of IROC, a five percent drop, from 2010. Organizations continue to have difficulty meeting the sub-requirements regarding network vulnerability scanning (11.2), penetration testing (11.3), and as mentioned in the previous section, file integrity monitoring (11.5).

At the time of the IROC, 67 percent of organizations met the testing requirements of 11.2. The lack of compliance with 11.2 is not necessarily as simple as failing to conduct network vulnerability scanning. The difficulties for some companies are the frequency (quarterly) combined with the expectation that findings defined as actionable are remediated and re-tested. Time and resource constraints hindered some in our sample from being able to present four 'passing' external and internal scans. Moreover, the new requirements for what is considered a passing external scan have had an effect on many organizations in our sample.

Requirement 11.3 specifies that an annual penetration test be performed by a qualified internal or external party, the idea being to check whether existing controls are able to repel a skilled and determined attacker. 53 percent of organizations perform external and internal penetration testing at least once a year and after any significant infrastructure or application upgrade or modification (Requirement 11.3).

Requirement 12 (Security Policies)

Organizations depend on the effectiveness of their information security policies, procedures, and capabilities to protect cardholder environments and the data that resides on, or are transmitted through, them. The principle that information security cannot be achieved by technical means alone is well established. Security tools such as firewalls, access control systems, and monitoring all contribute greatly to protecting cardholder data. However, the human element of information security management remains the weakest aspect. Failure to properly design, implement, and maintain the procedures and business processes quickly renders technology-based controls ineffective.

Failure to properly design, implement, and maintain the procedures and business processes quickly renders technology-based controls ineffective.

The findings for this study indicate that a mere 39 percent of organizations fully met Requirement 12 at the time of IROC. In line with several of the other key requirements, this is a five percent drop in comparison to the 2010 report findings.

PCI DSS requires that the security policies address all the requirements in the standard. Organizations met an average of 79 percent of tests in Requirement 12 at the time of IROC. It is evident that policies are written without completing prerequisite work; thus they lack critical content, and fail to identify the information assets that must be protected.

An often-ignored principle is that the security policies must directly address the protection of valuable corporate data/information assets, based on the findings of a risk assessment. It is risk-based security decisions, supported by properly executed risk assessments and the enforcement of security policies, that are the foundation of a well-designed information security program. With careful planning, they provide an essential guide for officers and employees in the implementation of effective and sustainable security and compliance programs.

Policies should be developed to manage risk. The only way to know what security measures are needed in a policy is to first discover the risks. Therefore, policy statements and related procedures should specifically address the threats and vulnerabilities identified in a risk assessment of both the organization and specifically the cardholder data environment (Requirement 12.1.2).

Security policy and supporting procedures provide no value if employees do not understand or know how to implement them.

Many security breaches can be traced back to weaknesses in security decision making, which results from poorly implemented risk management frameworks, and poorly written security policies and procedures. Policies that are lengthy and painfully detailed are often never read, and thus never followed. Alternatively, while policies are meant to be high-level documents (they are not detailed how-to procedures), some are unfocused, or written in vague terms that obscure the intent.

Surprisingly, the most compliant sub-control for Requirement 12 at the time of the IROC is 12.4: Ensure that the security policy and procedures clearly define information security responsibilities for all employees and contractors.

The most challenging sub-requirements under Requirement 12 are 12.8.2 and 12.8.4. For several organizations, Requirement 12.8.2, formally obtaining acknowledgement from service providers of their commitment to maintain proper security of cardholder data obtained from clients—and accepting accountability for the protection of that data—remains a taxing compliance issue. Lack of interpretation of sub-control 12.8.4 (*Maintain a program to monitor service providers' PCI DSS compliance status*) contributed towards its low compliance rating. Some organizations did not fully understand the real intent of this requirement—which applies only to those services delivered by the service provider to the organization, and only those services in scope of the organization's PCI DSS assessment.

Users who do not comply with the policy will likely face consequences. However, organizations should keep in mind that security is a learned behavior. Security policy and supporting procedures provide no value if employees do not understand or know how to implement them. For the protection of cardholder data to be effective and sustainable, it should include management actions for changing the behavior of personnel to voluntarily adhere to company policies. Companies can leverage seminars, awareness campaigns, and frequent communications to help provide this education.

PCI DSS Prioritized Approach

The Prioritized Approach was created in 2009 and defines a roadmap of activities around six ordered milestones that aim to help stakeholders reduce risk more quickly during the compliance process. The idea is that the earlier milestones address the most critical risks first. This process has been widely adopted globally by regional card brands and acquirers to provide guidance to organizations and reduce risk to cardholder data. Some global uses of the Prioritized Approach include:

- Acquirers asking for status reports in a Prioritized Approach format
- Non-compliant, as well as breached, entities being directed to focus on the Prioritized Approach
- Card brands tying the Prioritized Approach milestones to compliance validation initiatives.

A specific example of the Prioritized Approach changing the compliance validation landscape is the Visa Europe TIP program, which waives penalties for non-compliant entities that meet milestones 1-2 and grants “safe harbor” in the event of a data compromise if organizations meet milestones 1-4.

These milestones, which are listed in Table 2, are not organized around the 12 requirements; rather, sub-requirements are broken out and organized around the six milestones. In Table 2 we also show the percentage of PCI DSS requirements that were met/in place during recent years based on our 2011 data analysis when mapped against the prioritized approach.

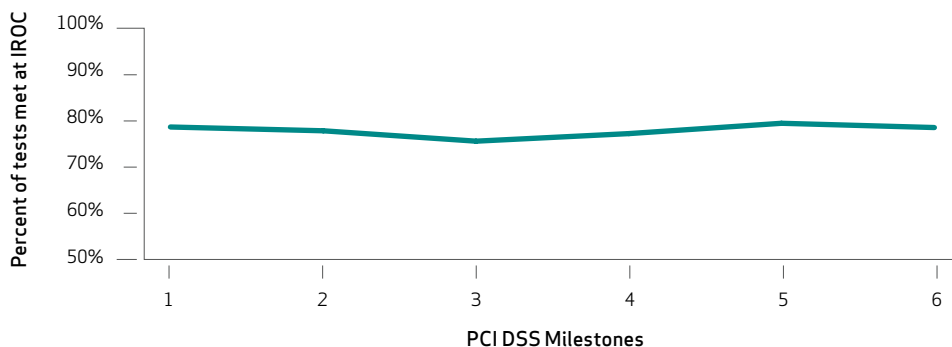
Table 2. Percent of test procedures met at IROC by priority milestone.*

| Milestone | Goal | In Place | |
|-----------|--|----------|------|
| | | '08-'09 | 2010 |
| 1 | Remove sensitive authentication data and limit data retention. | 88% | 78% |
| 2 | Protect the perimeter, internal, and wireless networks. | 81% | 78% |
| 3 | Secure payment card applications. | 81% | 76% |
| 4 | Monitor and control access to your systems. | 79% | 77% |
| 5 | Protect stored cardholder data. | 83% | 79% |
| 6 | Finalize remaining compliance efforts, and ensure all controls are in place. | 80% | 78% |

* Based on the PCI DSS Prioritized Approach from the PCI Security Standards Council.

Though Milestone 1 showed the highest in-place percentage in last year’s report, we found little real evidence that organizations were prioritizing their efforts around earlier milestones. We hoped another year might change things for the better, but this time around we found even less evidence of this. One would expect to see substantially higher adherence to the early milestones, but the nonexistent variation across all six milestones suggests a random or uniform approach to requirements within the DSS. The relatively flat line in Figure 4 depicts this interpretation well.

Figure 4. Percent of test procedures met at IROC by priority milestone.*



* Based on the PCI DSS Prioritized Approach from the PCI Security Standards Council.

Not only did the line flatten out even more in 2010, but it dropped several percentage points as well. Whereas the 2008/2009 numbers floated above 80 percent (Milestone 5 being the exception), all fall below that mark now. This is consistent with the small overall decline in initial compliance scores discussed earlier in this report.

When one considers that an organization undergoing an assessment is focused on receiving a fully compliant ROC, and therefore must meet all test procedures regardless of their milestone classification, this data makes more sense. These

The entire focus of the DSS is to protect the sensitive data; the fact that there is a drop in adherence to this protection at the time of an IROC is alarming.

organizations are focused on using the PCI DSS itself for guidance, and not the Prioritized Approach. However, since the Prioritized Approach emphasizes reducing risk to cardholder data, the apparent lack of adoption of the milestone analysis method may actually allow weaknesses in areas associated with higher threat likelihood and impact to exist longer than necessary. This is a case of the end goal of total compliance getting in the way of pragmatic security.

The data indicates that organizations are hitting every requirement with the same emphasis (or indiscriminately), as opposed to prioritizing them based on the risk to sensitive data. While it is true that they are required to meet all testing procedures, one would expect to see the requirements around the sensitive data (Milestone 1) more comprehensively addressed at the time of an IROC and throughout the year.

In reality, we saw a 10 percent drop of the in-place testing procedures under Milestone 1 as compared to last year's report. It is disturbing to see the requirements that avert the most risk were apparently not prioritized, particularly given the number of data breaches occurring. The entire focus of the DSS is to protect the sensitive data; the fact that there is a drop in adherence to this protection at the time of an IROC is alarming.

While adoption of the Prioritized Approach appears not to have gained traction with organizations, its prevalent use by acquirers and card brands to reduce risk to cardholder data of non-compliant organizations has increased, and we expect that an increasing number of organizations will be emphasizing the Prioritized Approach in their compliance efforts.

ANALYSIS OF INVESTIGATIVE RESPONSE DATA

Our industry-recognized Investigative Response (IR) team, which investigates about 30 percent of all publicly disclosed breaches, provides us unmatched intelligence into the current threat vectors and attacks against retailers, service providers, and other impacted organizations. Every year, Verizon publishes the acclaimed [Verizon Data Breach Investigations Report](http://www.verizonbusiness.com/Products/security/dbir/)⁴ (DBIR), which analyzes the breaches the IR team investigated. The series spans seven years of data, over 1,700 breaches, and more than 900 million compromised data records.

The majority of confirmed record losses involve payment card information, and this extensive dataset lets us identify the top security failures that contribute to card data breaches. In the sections below, we offer two interesting and unique lines of analysis with respect to PCI DSS. The first compares organizations assessed by our QSAs to payment card breach victims who engaged our IR team. The second lists the top threat actions used to compromise cardholder data in IR cases worked over the past year.

⁴ <http://www.verizonbusiness.com/Products/security/dbir/>

Comparison to IR Assessments

One of the common arguments made by skeptics of PCI DSS is that there is relatively little evidence supporting its effectiveness. We'd love to grow organizations in a lab and compare the breach likelihood of PCI-compliant organizations to those in the noncompliant control group. Instead, we did the next best thing.

Though neither exhaustive nor controlled, assessments conducted by Verizon's PCI and IR teams do allow comparison among organizations for which compliance and security results are at least partially known. At the culmination of a forensic engagement, the lead investigator performs a review of PCI DSS requirements and conveys these findings to the relevant payment card brands.

It is important to note here that the investigative response team is making a binary decision on each top-level PCI requirement. That is, rather than diving into the specifics of Requirements 1.1, 1.2, etc., like the QSA would do, the forensic investigator is simply making a top-level decision as to whether Requirement 1 was in place or not. In a sense, the forensic investigator plays the opposite role to a QSA in this scenario, as he or she answers the questions based on proving the negative rather than validating a positive. In other words, "I know this was not 'in place' at the time of the breach," rather than "I know this was 'in place' at the time of the audit." Since this PCI quasi-assessment is less intense, and more subjective, than a "normal" PCI assessment, there is a possibility that the IR data may actually show an optimistic picture of the breached entities' compliance by requirement.

Table 3. Percent of organizations meeting PCI DSS requirements.
IR data based on post-breach reviews; PCI data based on QSA assessments at IROC.

| PCI DSS Requirement | PCI Data | | IR Data | |
|---|------------|------------|------------|------------|
| | '08-'09 | 2010 | '08-'09 | 2010 |
| 1: Install and maintain a firewall configuration to protect data | 46% | 44% | 32% | 18% |
| 2: Do not use vendor-supplied defaults for system passwords and other security parameters | 48% | 56% | 41% | 33% |
| 3: Protect Stored Data | 43% | 42% | 19% | 21% |
| 4: Encrypt transmission of cardholder data and sensitive information across public networks | 63% | 72% | 77% | 89% |
| 5: Use and regularly update anti-virus software | 70% | 64% | 58% | 47% |
| 6: Develop and maintain secure systems and applications | 48% | 53% | 12% | 19% |
| 7: Restrict access to data by business need-to-know | 69% | 75% | 27% | 33% |
| 8: Assign a unique ID to each person with computer access | 44% | 47% | 26% | 26% |
| 9: Restrict physical access to cardholder data | 59% | 55% | 49% | 65% |
| 10: Track and monitor all access to network resources and cardholder data | 39% | 52% | 15% | 11% |
| 11: Regularly test security systems and processes | 38% | 37% | 19% | 19% |
| 12: Maintain a policy that addresses information security | 44% | 39% | 25% | 16% |

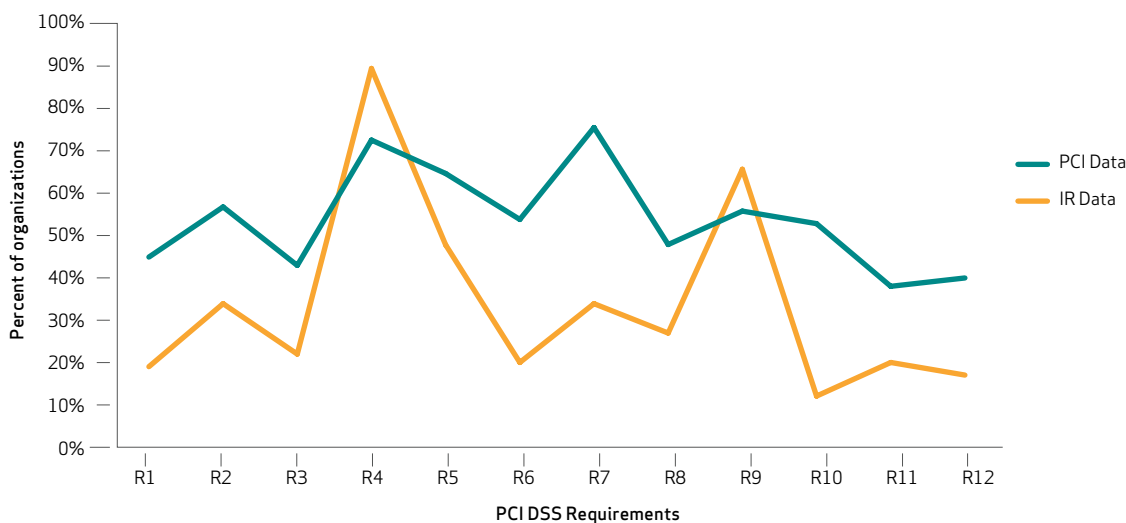
Lowest three values denoted in red and highest three are in bold.

Table 3 shows PCI DSS compliance results for two groups of organizations. The first includes the same sample of PCI clients discussed throughout this report (results mimic Table 1). The second group consists of organizations suffering a confirmed data breach investigated by our IR team in 2010.

Figure 5 presents the same data as Table 3 above, but the message is much more apparent: IR clients exhibit a lower likelihood of meeting PCI DSS requirements than do PCI clients. Said differently, breach victims are less compliant than a *normal*⁵ population of organizations. This is true across all requirements with the exception of Requirements 4 (encrypted transmissions) and 9 (physical security). As will be discussed in the next section, techniques attempting to compromise data traversing public networks were not a common threat action across our caseload. On the other hand, physical tampering was a common threat action in the compromise of cardholder data.

Though the disparity between the groups fluctuates per requirement, on average, PCI clients scored better than breach victims by a 50 percent margin⁶. So while ‘prove’ may be too strong a word to use in this case, the results do suggest that an organization wishing to avoid breaches is better off pursuing PCI DSS than shunning it altogether.

Figure 5. Percent of organizations meeting PCI DSS requirements.
IR data based on post-breach reviews; PCI data based on QSA assessments at IROC.



Though the disparity between the groups fluctuates per requirement, on average, PCI clients scored better than breach victims by a 50 percent margin⁵.

⁵ 'Normal' is not used here in the statistical sense. It simply refers to the fact that the group of PCI clients represents a set of organizations with no known atypical characteristics other than they all utilized our PCI assessment services.

⁶ It should also be considered that these results represent an IROC. Most of the organizations in the PCI dataset addressed the deficiencies shown here and were eventually validated fully compliant. In this respect, the difference between the IR and PCI datasets could be said to be even greater.

Top Threat Actions

All analysis prior to this point has been vulnerability-centric (or control-centric). Since the ultimate purpose of the PCI DSS is to reduce losses of cardholder data, a risk-centric perspective is relevant and useful to this study. For such a perspective, we analyze the threat actions identified in the breach investigations worked by Verizon's IR team. Threat actions describe what the threat agent did to cause or contribute to the incident. Table 4 lists the Top 15 threat actions⁷ leading to the compromise of payment card data in 2010. Any repeat performers are indicated along with their place on last year's Top 10 list.

The remainder of this section discusses these threat actions as well as the PCI DSS requirements that can deter, prevent, and detect them.

Table 4. Top threat actions based on 2010 payment card breaches investigated by or shared with the Verizon IR team.

| Category | Threat Actions | Percent of breaches |
|----------|---|---------------------|
| Malware | Send data to external site/entity | 44% |
| Malware | Backdoor (allows remote access/control) | 44% |
| Hacking | Exploitation of default or guessable credentials | 43% |
| Hacking | Exploitation of backdoor or command and control channel | 42% |
| Physical | Tampering | 36% |
| Malware | Keylogger/Spyware (capture data from user activity) | 31% |
| Hacking | Brute force and dictionary attacks | 30% |
| Malware | Disable or interfere with security controls | 28% |
| Hacking | Footprinting and Fingerprinting | 28% |
| Malware | RAM scraper (captures data from volatile memory) | 16% |
| Malware | System/network utilities (PsTools, Netcat) | 16% |
| Misuse | Embezzlement, skimming, and related fraud | 10% |
| Misuse | Use of unapproved hardware/devices | 8% |
| Physical | Surveillance | 6% |
| Hacking | SQL Injection | 5% |

A BRIEF PRIMER ON VERIS

The threat actions in Table 4 are based upon the Verizon Enterprise Risk and Incident Sharing (VERIS) framework. VERIS is designed to provide a common language for describing security incidents in a structured and repeatable manner. It takes the narrative of 'who did what to what or whom with what result' and translates it into the kind of data presented in the DBIR. The framework is available for free public use and can be accessed from the VERIS community [wiki](https://verisframework.wiki.zoho.com/).

Though VERIS recognizes seven categories of threat actions, only four are present in the Top 15 list (and one of those is mentioned only once). The percentages in Table 4 add up to more than 100 percent because most breaches involve more than one action in the event chain.

* <https://verisframework.wiki.zoho.com/>

Backdoors

In examining the threat actions from Table 4, it is convenient to organize the discussion around several logical groupings. Backdoors (malware) and the exploitation of them (hacking) are both in the top three and represent a good starting point⁸. Backdoors provide remote access to infected systems by bypassing normal authentication mechanisms and other security controls. With the backdoor established, an attacker can exploit it to access the system at will and engage in all manner of nefarious activities. Backdoors are popular tools because they facilitate the goals of concealment and persistence that cybercriminals crave.

⁷ The Top 15 are presented rather than Top 10 because there was a tie for 10th place.

⁸ It may seem odd to split these two actions, but there is a reason for it. VERIS classifies incidents as a series of discrete but related events. The introduction of malware to a system that opens a backdoor is viewed as a separate event from a threat agent using that backdoor to gain unauthorized access (the second is dependent upon the first but not certain to occur).

They are also the predominant means of exfiltrating payment card data from the victim's environment. In fact, malware that sends confidential data out over the Internet was this year's number one threat action, up from being a no-show on last year's Top 10 list. In terms of PCI DSS requirements relevant to data exiting an organization's network, Requirement 1 (firewall configuration) is the first to examine. While most organizations do a decent job at ingress filtering, egress filtering is often forgotten. Requirement 1 of the PCI DSS requires strong firewall rules in both directions, and as such, directly targets the number one threat action. Backdoors often operate via odd ports, protocols, and services, so ingress and egress filtering can be very effective in locking them down and aren't forced to rely on a known signature.

One would think Requirement 5 (AV software) would be a panacea for malware, and in spirit it should be. It seems counter-intuitive that one of the most implemented control areas relates to the most frequent threat actions. But as discussed in the DBIR, modern malware is highly customized (more than half according to the DBIR) and installed through vectors that evade AV software. A typical signature-based AV is outclassed by modern malware. That doesn't mean AV is useless—it provides a good layer of defense against 'classic' malware.

Requirement 2 (changing vendor defaults and hardening of systems) protects against many backdoors by disabling unnecessary and/or insecure services and changing default passwords. Since file integrity monitoring (in Requirement 11) is not signature-based, it holds promise as an effective measure against backdoors and other malware ('holds promise' is the operative phrase here; organizations struggle to get this right). Requirement 10 (tracking and monitoring) outlines controls that could be effective at detecting system changes and anomalous activity, but is, unfortunately, among the least implemented.

Physical Tampering

Physical tampering makes its debut this year as the number five threat action, accounting for 36 percent of the payment card breaches investigated in 2010. How could physical tampering have been responsible for so many payment card breaches if Table 3 tells us breached organizations and 'normal' organizations had similar levels of compliance with Requirement 9 (Physical Security)? Does that mean Requirement 9 isn't working?

While Requirement 9 has generally been successful at physically securing a data center and the network infrastructures, the endpoints have become the new weak link. Most instances of physical tampering occurred with automatic teller machines and gas pumps that had skimmers attached to, or inserted into, the device.

Requirement 12 (security policies) would help in efforts against physical skimmers by educating employees and customers to look for signs of tampering and fraud.

Authentication and Authorization Attacks

The next group of threat actions target authentication (who you are) and authorization (what you can do) mechanisms. Exploitation of default or guessable credentials, exploitation of backdoor or command and control channels, and brute force and dictionary attacks are consistently among the most prevalent and damaging attacks against cardholder data. Many systems and devices come preconfigured with standard usernames and passwords to allow initial setup. Because these are widely known by criminals (and because they're often simple), failure to change them often results in unauthorized access. This is especially prevalent in the hospitality and retail space where point-of-sale (POS) systems tend to be managed by third parties. If an attacker successfully steals or hacks valid user credentials, subsequent actions will appear to come from a legitimate user and are much less likely to be tagged as malicious by detection mechanisms. It also makes it easier for attackers to cover their tracks as they make off with their victims' data.

Access control lists (ACLs) are designed to specify which entities can access an object and what operations they can perform. If these authorization mechanisms are missing, weak, incorrectly scoped, or misconfigured, attackers can access resources and perform actions not intended by the victim.

Several requirements are designed to mitigate these threat actions. Eliminating default and guessable credentials is one of the main purposes of Requirement 2. Those that slip through the cracks should be found and remediated if an organization is regularly testing security systems and processes in line with Requirement 11. Since malware is commonly used to swipe credentials, Requirement 5 (AV software) can help prevent and detect known password-stealing malware. Restrictive firewall rules and network segmentation (Requirement 1) help shore up insufficient authorization at the network level, while restricting access by need-to-know (Requirement 7) works well at the application and system level. The large disparity between PCI clients and IR clients on Requirement 7 (see Table 3 or Figure 5) is interesting. Security professionals are intimately familiar with the concept of least-privilege 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, which gets our attention. While Requirements 8 (unique IDs) and 10 (logging and monitoring) might prevent some authentication and authorization attacks (though most will still look like legitimate activity), they do add accountability since specific actions against specific assets can be tied to specific agents. This, in turn, greatly aids the response, containment, and recovery process.

Exploitation of default or guessable credentials, exploitation of backdoor or command and control channels, and brute force and dictionary attacks are consistently among the most prevalent and damaging attacks against cardholder data.

Data-capturing Malware

From Table 4, we can see keyloggers/spyware moved up the list, while RAM scrapers moved down and packet sniffers dropped off. RAM scrapers, which have come into vogue over the last few years, are designed to capture data from volatile memory (RAM) within a system. Keyloggers and spyware, on the other hand, specialize in monitoring and logging the actions of a system user. They are typically used to collect usernames and passwords as part of a larger attack scenario, but can also be used on call center data-entry terminals to grab the actual card numbers and associated personal information of the victims.

The steep decline in the use of packet sniffers in breaches of cardholder data seems to indicate that Requirement 4 (encrypted transmissions) has been a successful countermeasure against data-capturing malware. Although, Requirement 4 only requires cardholder data transmissions be encrypted when traversing public networks.

Even for organizations that do encrypt all traffic internally, keyloggers, spyware, and RAM scrapers exploit soft spots in the armor by enabling criminals to capture data processed within systems.

This gives rise to the importance of controls within Requirement 11 (regular testing) such as file integrity monitoring. These applications observe system settings and monitor specific system and applications files. As is the case with IDS/IPS, tuning requires some effort and frequent false positives cause many to “dumb down” or ignore them altogether. In the event that malware evades the aforementioned defenses to infect systems, strict egress filtering (specified under Requirement 1) can contain it and Requirement 10 (logging and monitoring) stands a chance of detecting attempts to retrieve (e.g., via a backdoor) or send data out of the network.

A Note on SQL Injection

SQL injection, although not on this year's top list of threat actions, still deserves mention as significant due to the prevalence of e-commerce in today's economy. The raw numbers of SQL injection attacks were consistent with what we have seen in previous years, with the big difference this past year being the explosion of other types of attacks.

SQL injection is a technique that exploits how web pages communicate with back-end databases. At a very high level, the attacker inserts malicious statements into the web form and gets the answer to a query or the execution of other SQL statements. If the application trusts user input and does not validate it at the server, it is likely to be vulnerable to SQL injection, cross-site scripting, or one of the other input-validation vulnerabilities. In data breach scenarios, SQL injection has three main uses: 1) to query data from the database, 2) to modify data within the database, and 3) to deliver malware to the system. The versatility and effectiveness of SQL injection make it a multi-tool of choice among cybercriminals.

Since SQL injection is almost always an input validation failure, Requirement 6 (development and maintenance) is critical to thwarting it. Rather than waiting until the application is complete, baking security in throughout the development lifecycle is paramount to creating secure applications. Once developed, applications should be tested at regular intervals to verify controls are in place and up to par (Requirement 11). All the while, these applications should have logging enabled and be monitored (Requirement 10) to identify SQL injection attacks as they occur or shortly thereafter.

In Summary

None of the top threat actions listed above fall outside the scope of the 12 PCI DSS requirements. On the ominous side, the PCI requirements exhibiting the worst assessment scores (1, 3, 6, 10, 11, and 12) are also those most broadly applicable to the threat actions shown in Table 4.

While nobody has a lab to scientifically test for the relationship between PCI compliance and breach likelihood, this year's data reinforces the thesis from last year's Verizon PCI Compliance Report. As Figure 4 clearly shows, breach victims were less compliant across the board, with the exceptions of Requirements 4 and 9.

Is PCI perfect? Of course not; what regulation or standard is? But this study, now in its second year, continues to offer encouragement for organizations struggling to meet and/or maintain PCI compliance that their efforts are not for naught.

None of the top threat actions listed above fall outside the scope of the 12 PCI DSS requirements.

WHAT CONTRIBUTES TO A BETTER PCI ASSESSMENT?

In the security industry, we're great at giving recommendations, but often not so great at grading our recommendations, or for that matter, taking our own advice. So, before we launch into another set of recommended practices designed to improve the way you attain and maintain compliance, we probably ought to examine how we did last year. The Verizon RISK team was all too happy to put their "stat-jitsu" to work toward the purpose of keeping us honest.

To help test the merit of our counsel, we created an internal survey, based on our prior recommendations (refer to the 2010 PCICR), for QSAs to complete on behalf of each organization under audit. A simple ordinal scale from 1 to 4 was used for each question, with a short description provided for each extreme⁹. The questions are listed below.

1. Rate the organization's level of awareness and understanding of the PCI DSS requirements.
2. Rate the organization's level of preparedness going into the assessment.
3. Rate the organization's approach to maintaining compliance throughout the year.
4. Determine whether the security management and compliance functions within the organization are completely divorced or tightly coupled.
5. Rate the organization's level of understanding around cardholder dataflows.
6. Confirm whether the primary interest is to obtain a compliant ROC or truly improve security.

We took the ratings provided by the QSAs and compared them to each organization's assessment-derived compliance score (percentage of test procedures met) at the IROC stage. Table 5 presents these results¹⁰, which are well worth examining.

The most noticeable observation is the considerable difference between lowest and highest ratings for each item under study. On average, the highest-rated organizations met 20 percent more of the DSS requirements than their counterparts on the lowest end of the scoring spectrum. Whether this seems like a lot or a little is not important; the key point is that, in general, there appears to be a positive relationship between doing these things better and achieving better scores. Whether that turns out to be 10, 20, or 50 percent better, it's nice to see results falling in an expected direction, not to mention we avoid the embarrassment of a full retraction.

Table 5. Comparison of QSA-supplied survey ratings to initial compliance score.
Interpretation aid: Organizations with the lowest awareness of the DSS met 57% of test procedures at IROC/Gap report vs 96% for those that were most aware.

| | R1 | R2/3 | R4 |
|---------------------------------------|-----|------|-----|
| Awareness of the DSS | 57% | 88% | 96% |
| Preparedness for assessment | 79% | 88% | 93% |
| Maintenance throughout year | 77% | 89% | 94% |
| Integration of compliance & security | 72% | 87% | 97% |
| Understanding of data flows | 72% | 89% | 91% |
| Compliance-driven vs. security-driven | 87% | 83% | 94% |

⁹ While the QSA scoring is somewhat subjective, the ratings nevertheless provide a useful comparison of an organization's security with the resulting compliance results.

¹⁰ Organizations given level 2 and 3 ratings exhibited similar results, so we chose to present their combined average in this table to better contrast the lowest (R1) and highest (R4) from the middle (R2 and R3).

The largest delta between extremes (38 percent between R1 and R4) concerns the level of knowledge the organization has of the DSS. A shot in the dark rarely hits its mark, as they say¹¹. If these findings are valid, then having a competent compliance staff is probably not a bad investment.

We find it intriguing that the second-largest gap involves the level of integration between compliance and security. Organizations in which these functions were completely separate met, on average, 25 percent less at the IROC stage. So, a department dedicated and isolated to the purpose of compliance appears less able to meet that goal than hybrid and intermingled departments. If that's true, then it gives some real food for thought about the way we structure our organizations around these too-often competing notions of compliance and security.

The only item in Table 5 with negligible differences across the ratings scale compares the primary motivation of the organization in attaining compliance, whether to obtain a passing ROC, or truly improve security posture. Granted, discerning ulterior motives is not easy, but our QSAs made the call based on their intuition and the information available to them. The result is interesting and one that runs contrary to what we expected to find. Maybe our QSAs should brush up on their mind reading skills. Maybe this was not a very good question. Then again, maybe an organization's ultimate motivation in attaining compliance really doesn't matter; perhaps the doing matters more than the drive behind it.

Table 6. Results of significance tests comparing QSA-supplied survey ratings to initial compliance score.

| | R ² | p-value |
|---|----------------|--------------|
| Awareness of the DSS | 0.151 | 0.084 |
| Preparedness for assessment | 0.039 | 0.484 |
| Maintenance throughout year | 0.062 | 0.304 |
| Integration of compliance & security | 0.105 | 0.128 |
| Understanding of data flows | 0.056 | 0.324 |
| Compliance-driven vs security-driven | 0.059 | 0.324 |
| Average rating for all questions | 0.468 | 0.042 |

Statisticians will realize that even though differences like some of those shown in Table 6 appear substantial, they may not be statistically significant. That can only be determined through proper tests, which we ran and will discuss to conclude this section. Since the dependent variable (compliance score) is continuous and the independent variables (rating levels for the questions) are ordinal, we selected one-way ANOVA¹² as the method of testing the relationship among groups. To do this, we used a software package called JMP, and Table 6 shows the output of these tests.

The R² values¹³ show how well these organizational characteristics/practices (independent variables) explain the initial compliance score (the dependent variable). The values essentially answer “How

much of an organization's score can be attributed to these things?” That none of the values are very high seems to suggest the answer is, “Not much.” After glancing across these relatively low values, you might be thinking something similar to our initial reaction: “You folks need to get out of the recommendations business.” The p-values¹⁴ in Table 6—with the possible exception of ‘DSS understanding’—only serve to support this pronouncement.

11 Actually, we're not sure “they” ever really said that; it just sounds good to say that they did. You can cite us if you like it.

12 ANOVA (Analysis Of Variance) is a statistical method to test for significant differences between means of multiple groups. In this case, we are comparing the average compliance score across the rating levels for each question.

13 The coefficient of determination (R²) measures the proportion of variation explained by the model. The remaining proportion is attributed to random error. In this case, the results find that knowledge of the DSS accounts for about 15% of the initial compliance score.

14 The p-value is the probability that the null hypothesis (in this case, that there is no difference in compliance score across L1-4 organizations) is actually true. The lower the p-value, the less likely it is that the differences exhibited between group means are due to random chance alone. Values below .05 are often interpreted to signify a statistically significant relationship (though .1 or .01 are sometimes used as the threshold, depending on the situation).

However, if one takes the average rating for each organization across all of the characteristics/practices listed in Table 6, a different conclusion emerges. Taken together, an organization's approach to these things accounts for roughly half of the variation among compliance scores, which is a healthy sum (though it does beg the question of what contributes to the other half). It is also quite significant, with a p-value of less than 0.05.

This finding actually makes a lot of sense. Let's say we were studying the relationship between a person's physical characteristics and their likelihood of being a professional athlete. Suppose we hypothesize that speed, agility, strength, height, and body fat are our predictor variables. Testing each individually would probably show an insignificant relationship since there are, for instance, plenty of strong people in the world who don't get paid to play sports. On the other hand, if you are fast, agile, strong, tall, and trim, it's much more likely. In the same way, an organization that prepares well prior to an assessment, but is clueless about the DSS and their data flows is unlikely to score well on their IROC. Those that do all these things well exhibit more success.

The results of this simple side-study are not meant to be the final word in successfully navigating your next PCI assessment. They merely suggest that the way we run our organizations and approach compliance probably does factor into our success. And that should help give us a little direction and encouragement as we travel this (sometimes weary) road called compliance.

CONCLUSIONS AND RECOMMENDATIONS

Once again, it is our hope the data presented in this report provides the reader with a more accurate view of the current state of compliance in the payment card industry. Moreover, we believe it will help you to determine where your organization fits within that bigger picture and prove useful in helping you to reach your own compliance goals. After all is said and done, no magic formula exists to guarantee success in all your future PCI DSS assessments and endeavors, nor is there a single method or process to improved security. Nevertheless, we believe that this report has shown yet again that some common practices do exist, and are shared by highly successful organizations and serve to point one in the right direction with regard to both attaining and maintaining compliance. Not unlike most things in life, many of these practices are rooted in basic common sense, but, for a myriad of reasons, they often get lost among the everyday concerns and routine of running a business. As we have pointed out in other areas of this report, the problems our QSAs encountered during their assessments are, by and large, the same problems they encountered while compiling the data for last year's report. Therefore, we saw no need to reinvent the wheel with regard to our recommendations. Indeed, the previous section goes some way to suggest that they were quite near the mark. While we did provide new suggestions based on the data collected, we also included those previously offered since they are clearly as relevant today as they were before. They are enumerated below.

Name an internal champion for your PCI efforts.

As we have stated in many different ways, the secret to maintaining compliance lies largely in treating it as a daily part of conducting business. To achieve this, the correct mind-set must be instilled across the organization, and this type of integration must come from the top down. Furthermore, it is not likely to occur without the presence of a champion inside the organization. This individual must wield some amount of power, and use her or his influence to make certain not only that things get done properly, but also that everyone in the organization knows exactly which individual is responsible for what duty. In essence, most organizations require a culture shift to include security and compliance from the ground up, and for that daunting task a champion is indeed required.

| | |
|---|--|
| <p>Use caution when self-validating.</p> | <p>An emerging trend within the PCI space is that more level 1 and 2 merchants are choosing to self validate, or assess themselves. In order to utilize this option, the organization must send employees to an Internal Security Assessor (ISA) training course. Although this method of validation has been approved by the Council and is considered a legitimate practice, it has pitfalls that should be avoided. First, choose the team member who will act as ISA for your company carefully. Since the minimum set of knowledge, skills, and certification for the ISA is not as stringent as those for a QSA, there is a danger that the company could be deemed compliant by someone who really isn't qualified to do so. This could lead to security incidents and legal liability. With this in mind, the prudent organization will, at a minimum, have a disinterested party validate their scope. On the other side of the coin, the chosen employee might feel a certain degree of pressure from management to find that the program is compliant.</p> |
| <p>Be consistent with your interpretation/ implementation of penetration testing and vulnerability scanning.</p> | <p>The requirement for penetration testing has been around for more than three years, but many clients do not yet understand it or its implications. The requirement states that penetration testing must take place at least once annually or after any significant network or system change, e.g., OS upgrades, web application codes changes, and so on. However, many companies still neglect to follow these directives. For instance, the company will remember to do the test annually but forget to do so again after a change. Or, more typically, they do perform the test but do not validate the scope of the testing; consequently, they are required to perform the test again on in-scope systems, resulting in a loss of time and money. But perhaps the most frequent problem is that they will procrastinate and perform the test or scan at the last possible minute of an assessment. Invariably, the result is that they have between 100 – 200 findings to remediate and no hope of getting it done in time. This will cause the ROC to be delayed and the compliance deadline will be missed.</p> |
| <p>Beware, or at least prepare, for PCI DSS version 2.0.</p> | <p>This recommendation is slightly different than any others we have given, chiefly because the recommendations we typically make are based on the data we have analyzed, and since there are no 2.0 reports included in this data set this recommendation is a bit of a divergence from normal. However, given that the statistics have changed so little from last year's report, we feel that a word of warning is called for. While "beware" may be a bit melodramatic, "prepare" certainly describes how organizations should approach the version upgrade. 2.0 will be more stringent than any of its predecessors, largely in that it will require more evidence of compliance. Assertions that would have previously been accepted at face value will now require documented and detailed evidence as proof. In brief, the bar will be raised considerably with the new version and the wise CISO will begin to get their ducks in a row now rather than maintain the status quo.</p> |

--RECOMMENDATIONS FROM THE VERIZON 2010 PAYMENT CARD INDUSTRY COMPLIANCE REPORT --

| | |
|---|--|
| <p>Don't drive a wedge between compliance and security.</p> | <p>Whatever your stance on the "compliance vs. security" debate, hopefully we can all agree that intentionally keeping them apart doesn't make sense from either a compliance or a security perspective. Why force a false dichotomy between two concepts that should, in theory, be in alignment? After all, they both have the goal of protecting data. Sure, maybe you'll need to do some things for compliance that you wouldn't do for security (based on risk assessment or tolerance) or vice versa, but it's hardly an either-or situation across the board. The overall direction of managing compliance should be in line with the security strategy. Is your compliance management team the same as your security management team? If not, is there a concerted effort to collaborate when and where possible or do both sides govern their own private islands with no trade routes between them? If the latter situation is truer of your organization, perhaps you should ask why and whether it's best for it to remain that way.</p> |
| <p>Build security into your processes, not onto them.</p> | <p>By now, most organizations have learned the hard way that security applied as a band-aid is both costly and ineffective. What many do not seem to realize is that such an approach impacts compliance as well. While it is difficult to analyze through raw data, experience tells us that organizations that build security into their core processes generally spend less and achieve more when it comes to validating compliance. This probably has something to do with the previous recommendation; if an organization truly and consistently strives to be secure then it should not require a giant leap to be compliant.</p> |
| <p>Treat compliance as a continuous process, not an event.</p> | <p>The difference between process-driven and event-driven compliance programs is relatively simple to identify for an experienced assessor. Organizations that enjoy continued success in achieving and maintaining PCI compliance are those that have integrated the DSS activities into their daily operations. They work on an ongoing basis to review and meet requirements along with other external or internal compliance initiatives. They document security processes, maintain records, meet periodic internal checkpoints, and can quickly provide evidence of adhering to the designated controls. They create a roadmap for the next few years and consult it regularly to understand what challenges are on the horizon, what changes are necessary, and how best to integrate efforts into the short- and long-term strategy for protecting payment infrastructure and data. Put another way, achieving and maintaining PCI Compliance should not be considered an annual project but a daily process.</p> |

| | |
|--|---|
| <p>When preparing to validate, don't procrastinate.</p> | <p>This recommendation is related to and flows from the former. When organizations treat compliance like an event with a looming deadline, a great deal of rushing to and fro ensues. A tremendous amount of energy and resources will be spent in frantic preparation for the imminent arrival of the QSA. A year's backlog of changes are hastily made (those will come back to haunt you), the dust is blown off old documents (if they even exist and can be found), while duct tape and a good spit shine make everything else appear sturdy and tidy (move along, nothing to see here). This is the behavior of an organization that is almost certainly doomed to fail its assessment. It is also the behavior of an organization doomed to security failures, since—even if it manages to pass the assessment—will soon revert to normal behavior. The duct tape will wear off, the shiny stuff will tarnish, and the true state of things will be exposed. The organization will pay for compliance failures in wasted time and effort and for security failures in losses and penalties. The worst part, though, is that cardholders will pay for their behavior as well.</p> |
| <p>Avoid a failure to communicate.</p> | <p>As it relates to compliance initiatives, organizations often do not recognize the importance of communication. Those preparing for or undergoing an assessment should proactively communicate with all parties involved to avoid hindering the process through a lack of coordination. While this is certainly important among internal parties, it is especially critical when it comes to working with external parties. Open lines of communication to vendors that manage systems within the scope of the assessment will help make sure necessary information is available and ready for the QSA. If organizational changes make it impossible to meet a compliance deadline, the acquiring bank should be aware of the delay and the circumstances surrounding it. Keeping everyone in the loop is a rather obvious recommendation but it's also one that will help keep everyone happy—and a little more happiness to go around never hurts.</p> |
| <p>Understand how your decisions affect compliance.</p> | <p>A leopard can't change its spots and an organization can't (easily) change certain things about itself. Some of these unchangeables impact compliance. For example, the PCI DSS requires service providers to do some things differently than merchants, and there is nothing they can do to change that. This does not mean, of course, that organizations will never enact significant changes. It happens all the time, and it's important to understand how these decisions will affect the organization's ability to attain and/or maintain compliance. For instance, choosing to stick with legacy systems can make it more difficult to pass certain test procedures around access controls, audit logs, and encryption. Electing to outsource a function may result in it being more difficult to obtain information required for validation from the provider. Ultimately, such decisions will be made based on business needs and other related factors, but organizations do well to consider and prepare for the potential ramifications to the compliance process.</p> |

| | |
|---|---|
| <p>Keep it small and simple.</p> | <p>Continuing with the theme of decision-making, organizations often cannot fundamentally alter their IT environment. Business processes may necessitate certain infrastructure, applications, functions, and configurations. At times, however, a choice can be made between a more complex option and a simpler one. All else being equal, the simpler alternative will almost always be easier to manage in terms of both security and compliance. Based on our experience, ease of management correlates highly with successful management. Therefore, embrace this modified KISS rule whenever possible, and keep it small and simple.</p> |
| <p>Discover and track your data.</p> | <p>Nothing unnecessarily increases the scope of your PCI assessment like losing track of cardholder data. Make no doubt about it—those bits and bytes have an uncanny ability to multiply and migrate, and your IT infrastructure provides ample roosting places. Understanding data flows and stores is essential to establishing the scope of assessment. A poor understanding of this usually results in an overly large scope, which, in turn, usually results in more expense and difficulty. To overcome this, tight control over data is essential. This is a continuous process that begins with discovery. Thankfully, there are in-house tools and third-party services available that can help with this. We find they typically pay for themselves in the long run due to the difficulties and dangers of data run amuck.</p> |
| <p>Prioritize your approach to compliance.</p> | <p>On the road to “security,” organizations may set different destinations based on their individual risk tolerance. The road to “compliance” diverges from “security” in this regard (though they should be headed in the same general direction); the PCI DSS sets the destination (or at least a waypoint) for those governed by it. This does not mean that organizations must take the same route to get there or that all routes are equal. There is an optimal route and there are many sub-optimal routes. The PCI Security Standards Council recognizes this and published the Prioritized Approach as a guide on the road to compliance. Reliable data on which threats are most pertinent to the payment card industry can help adapt the route as well. Used properly, these resources will contribute to a safe, profitable, and successful journey.</p> |
| <p>Check yourself before you wreck yourself.</p> | <p>The phrase may smack of trite song lyrics, but it’s sage advice for security and compliance programs. Take the idea that everything will be alright as long as all the i’s are dotted and t’s are crossed and toss it out the window. It’s dangerous thinking. Healthy thinking understands that underneath it all, things are rarely what they seem. No organization is perfect. No security or compliance program is perfect. There are things right now that need to be acted upon and remediated but you will never know about them unless you check. If the dismal compliance scores in Requirement 10 and 11 aren’t enough to convince you of this, perhaps the findings we share about breach victims in this report (and in the DBIR) will. An organization that does not check cannot act. An organization that does not act cannot be successful in the long term. Don’t be one of them.</p> |

ABOUT VERIZON PCI SERVICES

Avoiding PCI compliance efforts, or not fully understanding how PCI applies to you, can be costly in more ways than you might think. You may face penalties and fines, litigation, and the costs of re-issuing compromised cards. And if a data breach occurs, you could lose money—and your well-earned reputation.

When you need assistance with implementing solutions and compensating controls to comply with the PCI DSS requirements, we can provide the right resources. The Verizon Business PCI Team performs hundreds of assessments each year and works with both local and global Fortune 500 companies. It is composed of QSAs and PA-QSAs in six global regions that support over 20 languages.

This dedicated team focuses on PCI DSS and PA-DSS Assessments as well as PCI readiness, advisory, and remediation services. In addition to professional services, Verizon Business assists PCI customers through a variety of product platforms including our Merchant Compliance Program (MCP), Online Compliance Program (OCP), and Partner Security Program (PSP).

Verizon PCI Services are becoming Terremark PCI Services

In April 2011, Verizon completed its acquisition of Terremark, a global provider of managed IT infrastructure and cloud services. Through the acquisition, Terremark, a Verizon Company, will deliver an expanded and enhanced solutions portfolio that combines the leading cloud, security and IT capabilities of Terremark and Verizon.

About Terremark, a Verizon Company

Terremark, a Verizon Company, is a leader in transforming and securing enterprise-class IT on a global scale. A subsidiary of Verizon Communications Inc. (NYSE, NASDAQ:VZ), Terremark sets the standard for IT deployments with advanced infrastructure and managed service offerings that deliver the scale, security, and reliability necessary to meet the demanding requirements of enterprises and governments around the world. With a global network of data centers and a comprehensive portfolio of secure solutions, Terremark is helping enterprise and government executives realize the power and promise of the cloud today. For more information, visit www.terremark.com.

VERIZONBUSINESS.COM

© 2011 Verizon. All Rights Reserved. The Verizon and Verizon Business names and logos and all other names, logos, and slogans identifying Verizon's products and services are trademarks and service marks or registered trademarks and service marks of Verizon Trademark Services LLC or its affiliates in the United States and/or other countries. Microsoft and Outlook are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries. All other trademarks and service marks are the property of their respective owners. MC15106 09/11

