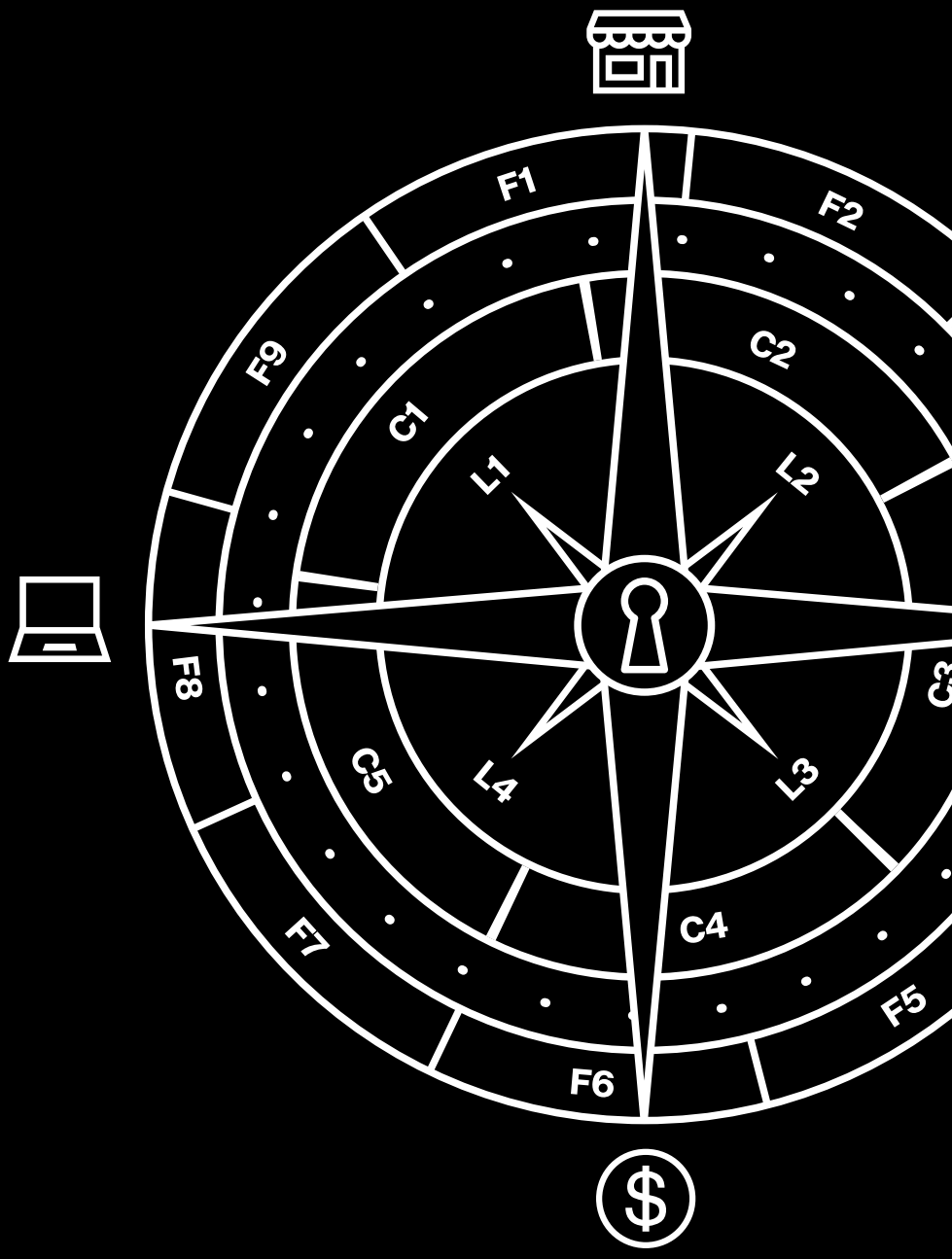
2019 Payment Security Report

Hospitality snapshot



verizon business ready

The hospitality industry is strongly invested in enhancing customer experience. Yet instead of showing customers the royal treatment, hospitality organizations are exposing customers to cyberthreats more than any other industry evaluated in the Verizon 2019 Payment Security Report (PSR).

In the 2019 PSR, we include more detailed data breach investigation correlations from our Verizon Threat Research Advisory Center (VTRAC) | Investigative Response team. The hospitality industry's compliance with the Payment Card Industry Data Security Standard (PCI DSS) slid from 42.9% in our 2017 report to 38.5% last year and 26.3% compliance in the 2019 PSR. Long-term trends show traveler accommodation, travel arrangement and reservation service organizations being breached most often. And with several major hotel data breaches in the news, it's a good time to assess and redress payment card security compliance practices.

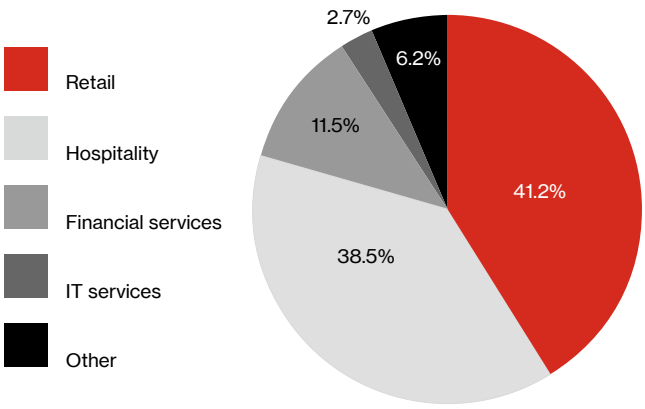


Figure 1. Confirmed data breaches by industry, six-year trend, Verizon PCI forensic investigations (PFI) global caseload 2010–2016

Payment card security is vital—but not all businesses are in full compliance.

In the nine years that Verizon has been producing the PSR, we've seen full PCI DSS compliance across industries improve annually until 2017, when our assessments measured a downturn two years in a row. Assessments from other Qualified Security Assessor (QSA) companies show a similar decline in full compliance with the PCI DSS. Hospitality suffered the biggest decline of the industries studied.

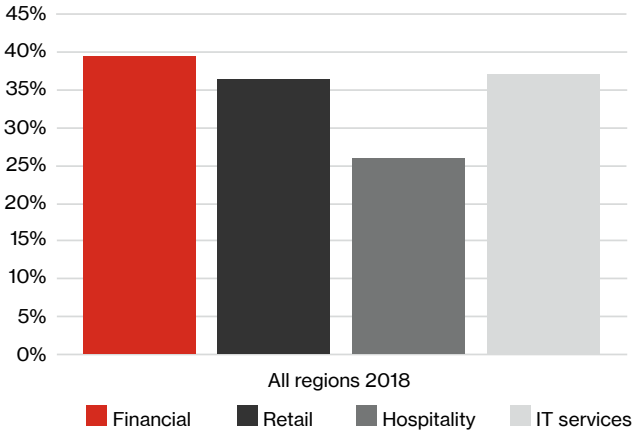


Figure 2. Global compliance by industry

What is PCI DSS?

Leading card brands set up the Payment Card Industry Data Security Standard to help businesses that take card payments reduce fraud. While the PCI DSS is focused on protecting card data, it's built on solid security principles that apply to all kinds of data. It covers topics like retention policies, encryption, physical security, authentication and access control. For more information, visit pcisecuritystandards.org.

While the 2019 PSR shows that overall compliance fell, the control gap—representing how far organizations were from fully complying with PCI DSS requirements—remained consistent with the previous year at 7.2%. Looking at only the organizations that failed their interim compliance validation, the control gap moved in a good direction by decreasing by 6.2 percentage points (pp) from last year to 10.2% in the 2019 PSR.

Organizations in the Asia-Pacific (APAC) region are showing a stronger ability to maintain full compliance at 69.6%. Europe, the Middle East and Africa (EMEA) scored a 48.4% on full compliance, while fewer than one-quarter of all organizations in the Americas (20.4%) maintained full compliance.

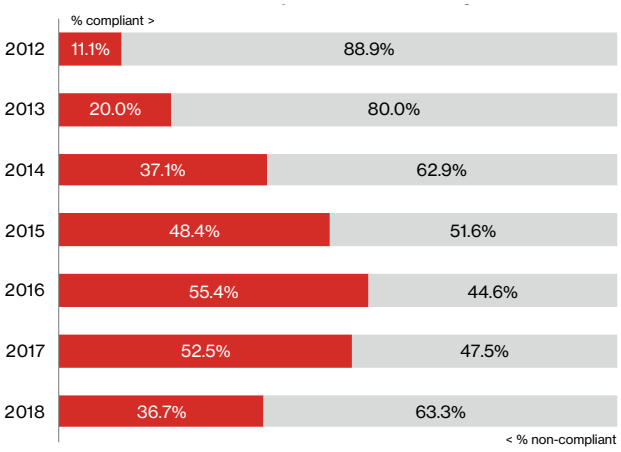


Figure 3. Full compliance by year

The overall drop in full compliance starkly reveals the importance of creating and maintaining a mature PCI DSS compliance program. To accomplish this, data protection and compliance programs (DPCPs) must evolve. According to the approximately 55 organizations we surveyed for the 2018 PSR, 18% of organizations across all industries have no defined DPCP. None rate their program maturity as optimized.

18%

of organizations across all industries have no defined data protection and compliance program. None rated their DPCP maturity as optimized.

Proactively reversing the trend

Protecting customer and cardholder data goes a long way toward creating a competitive advantage, and to do so, organizations need to be consciously proactive, rather than reactive. This is where our 2019 PSR can help.

The report reveals groundbreaking insights that help payment card professionals better understand their world. Our 2019 PSR explains how new navigational tools—such as the Verizon 9-5-4 Compliance Program Performance Evaluation Framework—can help organizations improve their PCI data protection and PCI DSS compliance.

How hospitality fared

The good

Hospitality's performance did show a few improvements.

While hospitality still had the lowest score for encrypting data in transit (PCI DSS Requirement 4), it was the only industry that improved in this category from the previous year. Hospitality also improved at protecting against malicious software (Requirement 5). It showed the most improvement of any industry in meeting this requirement, increasing its compliance to 84.2%.

Hospitality was the only sector we studied in the 2019 PSR that improved its ability to control physical access (Requirement 9) from the previous year, increasing its compliance score for this requirement 9.3 pp to 63.2%.

The bad

Hospitality ranked lowest out of the four industries (compared against financial services, retail and IT services) in accomplishing a number of major PCI DSS requirements:

- Maintain a firewall configuration (Requirement 1)
- Change vendor-supplied defaults (Requirement 2)
- Protect stored cardholder data (Requirement 3)
- Encrypt data in transit (Requirement 4)
- Develop and maintain secure systems (Requirement 6)
- Restrict access (Requirement 7)
- Test security systems and processes (Requirement 11)

Hospitality not only ranked low in compliance with those requirements, the industry also had the largest control gap for Requirements 1, 2, 6 and 11, and the largest increase in control gap for Requirements 3, 6, 7 and 11.

Particularly salient in hospitality's less-than-great performance this year are large drops in the ability to develop and maintain secure systems (a 21.9 pp drop), to restrict access (a 21.5 pp drop) and to authenticate access (Requirement 8, with a drop in full compliance of 11.7 pp to 42.1%).

The fact that hospitality succeeded in complying with these requirements before points to a challenge not with any one compliance task, but with designing and maintaining a mature PCI DSS program with consistent control performance.

The interesting

While hospitality lagged behind other industries at protecting stored cardholder data (Requirement 3), it also had some unique challenges to overcome, including a lack of mature solutions designed for hospitality environments.

Being able to respond to incidents can be as important as avoiding them. Hospitality struggled most with user identification and authentication (Control 10.2.5), reviewing and testing the incident response plan (Control 12.10.2), and training on breach responsibilities (Control 12.10.4), according to PSR data.

Why is it important to meet PCI DSS requirements?

We've correlated PCI DSS compliance with organizations that experienced payment card data breaches since 2008, and we have never seen a record of any organization suffering a confirmed payment card data breach and being compliant across all 12 PCI DSS key requirements at the time of the data compromise.

Recommendations

Control access.

Hospitality's big drops in compliance for restricting and authenticating access shouldn't go unaddressed, especially when so many vendors and solutions exist to help organizations. The Verizon 9-5-4 Compliance Program Performance Evaluation Framework can also help with controlling access.

Invest in maturity.

Hospitality's compliance with a number of the PCI DSS requirements is waning. This indicates the need to build more mature, consistent processes as payment security evolves, so that organizations aren't just reactive.

How to do that?

The next recommendation can get you started.

Figure 4. A relational model of the 9 Factors of Control Effectiveness and Sustainability

Develop program maturity.

Organizations don't deliberately fail to design good compliance programs. Developing program maturity is difficult. The right navigational guides, however, make it possible.

In the 2019 PSR, we provide the Verizon 9-5-4 Compliance Program Performance Evaluation Framework. It combines work from past PSR editions with additional guidance to create an integrated framework that can be the navigational aid that organizations need to enhance their data protection and compliance programs. The framework provides a new level of visibility and control to help businesses achieve repeatability, consistency and highly predictable outcomes for compliance success.

Make payment security feel at home.

Treating customers well is the definition of good hospitality. Handling customer payment card data with care and diligence is a part of that. For the security-minded hospitality organization, opportunity awaits. Building a consistent data protection and control program can help hospitality offer its customers—and their data—true comfort and relaxation.

Learn more:

To find out where to focus your security efforts and how to improve your compliance program, visit enterprise.verizon.com/resources/reports/payment-security/ or contact your Verizon representative.

verizon business ready