PSR

2020 Payment Security Report

Retail

verizon

Retail sector: Data security becomes top priority as complexity increases.

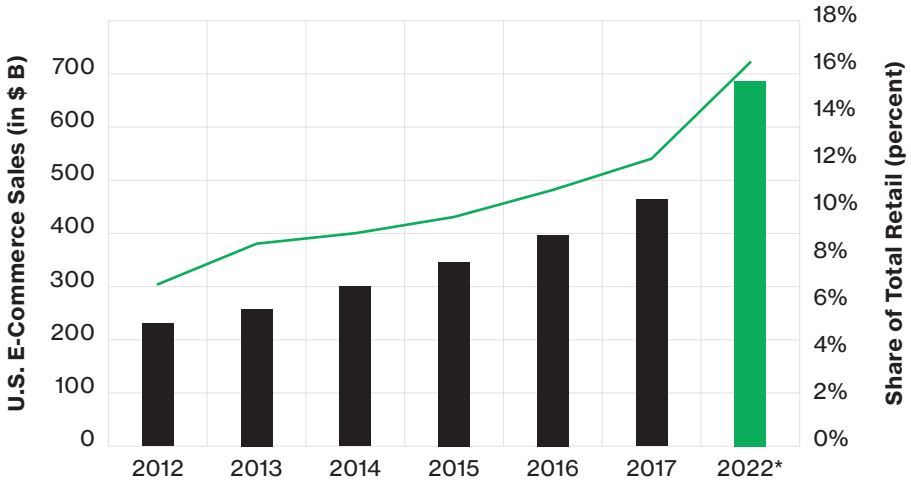
Get detailed recommendations in the Verizon 2020 Payment Security Report (PSR).

The retail sector has been struggling with the transition from brick-and-mortar sales to e-commerce for many years. In addition to the challenges of adapting to card-not-present transactions, mobile payments and other digital transformations, pressures imposed by COVID-19 have also significantly increased the disruption.

However, the greatest challenge of all is the industry's tendency to merely meet baseline security standards. The use of outdated security strategies, even during the worst possible conditions, is a straw that could result in a breach that might break the already-burdened camel's back.

Since 2010, Verizon's Payment Security Report (PSR) has been tracking the ups and downs of the retail sector's compliance with the Payment Card Industry Data Security Standard (PCI DSS). In 2019, the sector experienced a downward trend in its struggle to maintain sustainable and effective compliance. Even before COVID-19 was a concern, the industry had a mere 16.7% full compliance—a huge 19.7 percentage point (pp) drop from the PSR's 2018 findings, according to the 2020 PSR.[1]

Digital disruption in retail



Data: U.S. Census Bureau.[2] *Forecast

Retail industry data security risks

Financial gain continues to be a primary motivator for cybercrime and accounts for nearly 9 in 10 (86%) breaches. Within the retail industry, 99% of incidents were financially motivated in 2019, with payment data remaining the most sought-after and lucrative commodity, according to the 2020 Verizon Data Breach Investigations Report (DBIR).[3] The rapid transitions in retail have affected the behaviors of threat actors, who prey upon instability, lax compliance and change to exploit weaknesses in payment security.

A surge in online ordering has reduced the threat of skimmers and point-of-sale (POS) device hacking, as well as remote intrusion. In 2019, POS attacks made up only 0.8% of total data breaches, according to the 2020 Verizon DBIR.[4] The majority of these incidents include the use of RAM scrapers, which allow threat actors to scrape payment cards directly from the memory of the servers and endpoints that run payment systems.

Defending infrastructure and cloud platforms is now a greater concern. Threat actors can easily search for known vulnerabilities on payment platforms, looking for weak authentication, insecure access control and unpatched servers. When secure protocols are not in place and enforced, someone with even marginal attack skills can breach systems, according to the DBIR. Add to that challenge the recent significant shift to e-commerce by retail organizations scrambling to adapt, and payment security can be a secondary consideration to the need to quickly keep a challenged business viable. E-commerce in 2020 is accelerating at an unprecedented rate. From Q2 2019 to Q2 2020, e-commerce quarterly sales in the United States more than tripled from 13.9% to 44.4%, a 30.5 pp increase. From Q3 2019 to Q3 2020, the escalation continued with a jump from 18.0% to 37.1%, a 19.1 pp increase, according to estimates by the U.S. Department of Commerce.[5]

What is the PCI DSS?

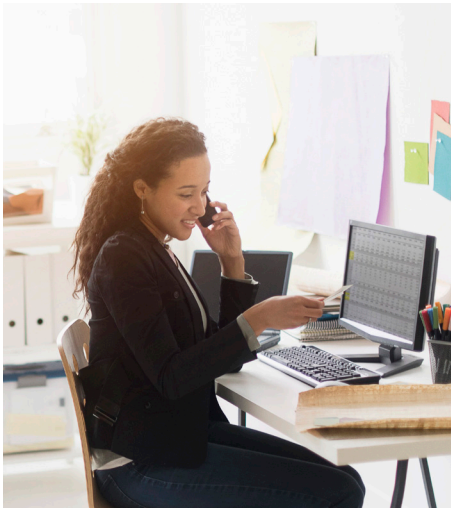
Leading card brands set up the Payment Card Industry Data Security Standard to help businesses protect stored, processed or transmitted payment card data. While the PCI DSS is focused on protecting card data, it is built on solid security principles that apply to all kinds of data. It covers topics such as retention policies, encryption, physical security, authentication and access control. We have correlated PCI DSS compliance with organizations that experienced payment card data breaches since 2008, and have never seen any organization suffering a confirmed payment card data breach while compliant across all 12 PCI DSS Key Requirements at the time of the data compromise. For more information, visit pcisecuritystandards.org

Meanwhile, the evolving and broad landscape of mobile devices is exposing users to a variety of security threats. Malicious actors leverage the passive attitude of mobile consumers accessing digital content and purchasing goods and services. Cybercriminals and nation-state hackers take advantage of disruptions resulting from COVID-19 and use mobile devices to spread malware, including spyware and ransomware. Workforce changes have exacerbated these problems, according to the 2020 PSR mobile security appendix.[6]

Verizon's PSR provides the kind of in-depth perspective the retail industry needs on the regulatory landscape of the payment card industry (PCI). It highlights risks associated with noncompliance with the PCI DSS in a range of industries worldwide. In the 2020 PSR, its 10-year anniversary edition, Verizon and several third-party contributors assessed four key industries on their level of compliance to the PCI DSS's 12 Key Requirements. The 2020 PSR reported that from the total population of organizations assessed on PCI DSS compliance in 2019, compliance fell to 27.9%, a drop of 8.8 pp from the previous year and a huge 27.5 pp decline (50.3%) from 2016, when compliance peaked at 55.4%.[7]

Is retail payment security built from straw or brick?

The retail sector lagged behind all other assessed industries, showing a mere 16.7% full compliance, a significant 19.7 pp drop from the 2018 findings. The sector also showed only a slight-to-moderate contraction of control gap. A reduction in control gap is a positive outcome: The smaller the control gap, the fewer controls are found to be not in place during validation, which narrows the noncompliance gap and exposure of the cardholder data environment to risks from threat actors.



Building compliance with straw

The industry's compliance performance in 2019 with the PCI DSS 12 Key Requirements was mixed, showing an overall decline from the previous year. In the case of five key requirements, it built a flimsy straw house, placing last among four assessed industries (retail, hospitality, finance, IT services).

Requirement 1: Install and maintain a firewall configuration, 66.7%: With only two-thirds of retailers in compliance on this critical requirement, the sector continues to put itself at significant risk of a breach.

Requirement 6: Develop and maintain secure systems, 58.3%: Retail reported just a 0.8 pp drop to 58.3% from 2018, but was still the lowest-performing sector for this requirement.

Requirement 9: Control physical access, 62.5%: Retail had the lowest rate of full compliance and second-highest control gap, at 5.3%.

Requirement 11: Test security systems and processes; and Requirement 12: Security management, 41.7% for both: Retail had the poorest showing for these two requirements, but also the smallest control gap. Thus, more retail companies are failing Requirements 11 and 12, but fewer controls are the sources of those failures.

Building compliance with brick

The retail sector built solidly with some key requirements, placing above the other three industries in four categories.

Requirement 2: Do not use vendor-supplied defaults, 83.3%: Retail ranked significantly higher in compliance than the other three industries, which trailed with 65.9% (finance), 64.3% (IT services) and 42.9% (hospitality).

Requirement 3: Protect stored cardholder data, 87.5%: Retail outperformed other sectors in 2019 at 87.5% full compliance, also noting an 8.0 pp improvement compared to the previous year.

Magecart malware infrastructure breaches

Skimmers are not just found on physical payment terminals. They show up online too, using different attack vectors. Typically, they are grouped under "Magecart malware," a nod to the first such attacks, which were found on Magento shopping cart platforms. Magecart attacks inject malicious JavaScript code on merchant-managed e-commerce sites and third-party payment pages. They can target the supply chain, as occurred in the Volusion e-commerce platform data breach, or they can appear directly on a merchant's payment page as injected iFrames, for example. The malicious code can be found in third-party libraries, steganographic images or third-party add-ons. The commonality among the variations is the siphoning of payment card data as online transactions are occurring. With so many possible attack vectors and an increase in the number and creativity of attacks, what can merchants and service providers do to protect themselves and their customers? Reinforce the basics of patching (Control 6.2), file integrity monitoring (Control 11.5) and logging (Control 10). Bolster detection capabilities by scanning, assessing and testing web applications and critical system components for vulnerabilities (Controls 6.5, 6.6, 11.2, 11.3). Strengthen prevention through applying hardening standards (Control 2.2), anti-malware software (Control 5), identity and access management (Controls 7 and 8), intrusion detection system/intrusion prevention system (IDS/IPS) (Control 11.4), and service provider management (Control 12).[8]

Requirement 7: Restrict access, 95.8%: This requirement remains the most well-maintained, retaining the top requirement position for the fourth consecutive year. With retail's full compliance at 95.8%, it outperformed even finance, which came in at 89.4%.

Requirement 8: Authenticate access, 83.3%: Merchants reported significant growth in compliance of 17.1 pp to 82.4%. Retail noted the smallest control gap, reducing 1.2 pp to 3.0%. Retail also reported the highest use of compensating controls at 16.7%.

Industry best practices

The speed and scope of change taking place in the retail industry is requiring strategic thinking and agility coupled with sound security practices. As with any organism, sound security is key to survival. Organisms that spend less time defending themselves have more time to grow.

The rapid shift to e-commerce is creating an approach to payment security that is increasingly about defending infrastructure and connections to the cloud. Data security is required by the PCI DSS to be a 24/7 ongoing activity. To be effective, multiple components of the control environment must work together in a series of control systems in order to achieve sustainable compliance. Organizations should not allow any third-party service involved with payment security data storage, transmission or processing, or any services that affect the security of card data, to be in noncompliance with the PCI DSS, as specified in Requirement 12. Devices can connect to hundreds of services a day, and organizations cannot allow any significant weaknesses to persist within their environment if they expect sensitive data to be effectively protected. All systems need to consistently meet their control objectives.

Common data security mistakes

Chief information security officers (CISOs) need to deal with unproductive practices in their organizations that don't promote effective and sustainable data protection, such as:

- Lacking an effective security strategy, continuing to operate in a reactive mode
- Not understanding the scope of their risks, operating with poor risk assessment and management practices
- Viewing data protection as a technology problem, not managing data protection as an operational business process and cultural problem
- Failing to get real buy-in from board members and senior business management, not communicating a compelling narrative about the need for security investments
- Not knowing what to address first, being unable to balance quick wins with long-term strategic initiatives
- Being unaware of data and IT assets and operating with many blind spots, not knowing where data exists and its sensitivity level, and failing to map data flow and stopping shadow IT channels
- Security functioning as an island, not addressing security as a cross-functional issue that affects other parts of the organization
- Not testing their security, failing to test whether controls are effective (process and capability) and continuously testing for vulnerabilities
- Inadequate education of the workforces, having inadequate security awareness, training and education
- Denying that they're a target, with people and departments not believing they're at risk or thinking they are too insignificant to become a target[9]

Organizations need to be familiar with their cloud service providers' track records and reputations in the provisioning of secure services. Retailers need to consider all of the different connections and where the potential breach entry points exist. (See page 30 of the Verizon Mobile Security Index 2020 for additional information on device breach points.)[10]

Many organizations are implementing zero trust models for cloud security management. Zero trust is a set of security measures intended to make sure that organizations do not automatically trust anything inside or outside of defined perimeters designed to protect sensitive data. In a zero trust environment, an organization must continuously verify users and devices while providing conditional access on an as-needed basis to digital resources such as email, applications, documents and information. Creating a zero trust environment around the mobile workforce requires integrating unified endpoint management (UEM), identity access management (IAM) and mobile threat defense (MTD) tools. (For more details on zero trust, see the 2020 Payment Security Report's "Mobile security" appendix on page 123.)[11]

The impact of COVID-19 on work-from-home practices has increased the challenges faced by the retail industry. Contact centers responsible for payment data adjusted their security protocols when workers moved from offices to their homes. Retail establishments and organizations need to make sure that bring-your-own-device (BYOD) policies effectively maintain control over employee devices in their homes and include updated acceptable-use policies. Employee devices should not be allowed to connect to unauthorized applications. Home work spaces also need to be out of range from potential listening devices, such as "smart speakers." These are just a few of the many considerations organizations need to think about in this new work dynamic.

The Payment Security Report: An exceptional guide

The Verizon 2020 PSR provides a wellspring of ideas on security practices for practitioners, CISOs and organizational leaders. The challenges CISOs face in designing, implementing and executing a sound data security compliance program requires strategic thinking. A lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational design and execution. That's why the 2020 PSR includes clear guidance on five elements of a high-performance data security environment, as well as how to avoid these seven strategic data security management traps:[12]

1. Inadequate leadership
2. Failing to secure strategic support
3. Lack of resourcing capabilities
4. Falling short on sound strategic design
5. Deficient strategy execution
6. Low capability and process maturity with a lack of continuous improvement
7. Communication and culture constraints

In previous editions of the PSR, we reviewed in detail the concepts of control effectiveness and sustainability. We introduced the 9-5-4 Compliance Program Performance Evaluation Framework (the 9 Factors of Control Effectiveness and Sustainability, the 5 Constraints of Organizational Proficiency and the 4 Lines of Assurance)—valuable tools to help implement, maintain and measure control effectiveness. We covered how organizations can address constraints and develop data security compliance management proficiencies to become more efficient. We also discussed the application of metrics and maturity models for improving the sustainability and effectiveness of the control environment.

In addition to maintaining compliance efforts in line with the PCI DSS 12 Key Requirements, what next steps should your organization take during these disruptive times in the retail industry?

Retail and mobile device security

Data compiled for the Verizon Mobile Security Index (MSI) 2020 found that:

Thirty percent of retailers were compromised.

1.5x

Retail establishments are 1.5 times as likely to be compromised if they sacrificed security.

Retail, travel and hospitality companies are using mobile platforms to appeal to modern consumers and keep physical stores relevant. Mobile is also helping to cut costs and waste from the supply chain. But there's also a lot at stake: 87% of retailers said they are concerned that a mobile security breach could have a lasting impact on their brand and customer loyalty. Retailers are worried about a wide range of mobile security threats, from emerging ones like cryptojacking to more established threats like ransomware and phishing. But they're also concerned about "insider threats," rating their employees as the greatest risk when it comes to mobile devices. Employee actions, even if inadvertent, can expose retailers to greater risk. While 88% of retailers said their frontline staff use mobile devices, only 37% said that these employees have a high level of cybersecurity awareness. And despite the risks, 40% of retailers had knowingly sacrificed mobile security. Our latest data shows that 30% had suffered a compromise—no improvement over the finding in the Verizon Mobile Security Index 2019.[13]

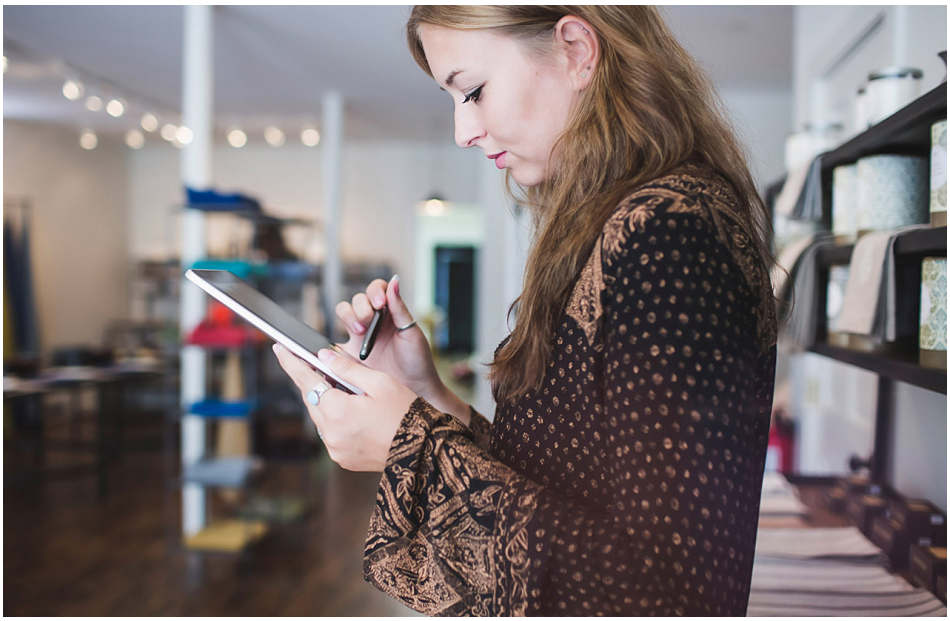
Mature your compliance program.

Organizations don't deliberately fail to design good compliance programs. Developing program maturity is difficult, but the right navigational guides make it possible. The Verizon 9-5-4 Compliance Program Performance Evaluation Framework is an integrated framework that can serve as a navigational aid to enhance a compliance program. The framework provides a new level of visibility and control to help businesses achieve repeatability, consistency and highly predictable outcomes that lead to data protection and compliance success.

Make payment security a part of securing your brand.

The retail sector's recent slide in PCI DSS compliance does not need to define your response to payment security. Despite the industry's overall lackluster performance in the 2020 PSR, we still encountered compliant retail organizations that maintain their PCI DSS controls year-round. Building a mature compliance program can allow you to join these industry leaders and gain a competitive advantage by creating the trusted brand that customers seek.

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 Business Account Manager.



verizon

1. Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/
2. Innosight, "2018 Corporate Longevity Forecast: Creative Destruction is Accelerating," Chart 4, based on data from the U.S. Census Bureau, 2018. https://www.innosight.com/insight/creative-destruction/
3. 2020 Verizon Data Breach Investigations Report, 2020. https://enterprise.verizon.com/resources/reports/
4. Ibid
5. United States Department of Commerce, U.S. Census Bureau News, Estimated Quarterly U.S. Retail Sales: Total and E-commerce, 2020. www.census.gov/retail/mrts/www/data/pdf/ec_current.pdf
6. Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/
7. Ibid
8. Ibid
9. ibid
10. Verizon Mobile Security Index 2020, page 30, 2020. https://enterprise.verizon.com/resources/reports/mobile-security-index/
11. Verizon 2020 Payment Security Report, "Mobile security" appendix, page 123. 2020. https://www.verizon.com/business/resources/reports/payment-security-report/
12. Verizon 2020 Payment Security Report, 2020. https://www.verizon.com/business/resources/reports/payment-security-report/
13. Verizon Mobile Security Index 2020, 2020. https://enterprise.verizon.com/resources/reports/mobile-security-index/

INF0520221