

2020 Payment Security Report

Fact sheet

Too few organizations understand the underlying reasons for their inability to achieve and maintain predictable data protection and compliance success. The Verizon 2020 Payment Security Report (PSR) – the 10th anniversary edition of this one-of-a-kind research – explores the challenges CISOs face in designing, implementing and maintaining an effective and sustainable security strategy and program.

Compliance continues to drop.

Compliance with the Payment Card Industry Data Security Standard (PCI DSS) continues to atrophy. The 2020 PSR rates the ability of companies to keep controls in place over time – not just the ability to achieve once-a-year compliance.

Why, for instance, are technology solutions prioritized while the mature development of capabilities and processes is ignored? How can leaders adapt, innovate and evolve to improve their security cultures? We explain the top security pitfalls and present solutions to equip CISOs with approaches to take with data security compliance challenges. We explore the essential elements needed to successfully build a compliance program without falling prey to external environmental shifts during challenging times.

Financial gain remains a primary motivator for cybercrime and accounts for nearly 9 in 10 (86%) breaches. Within the retail industry, 99% of incidents were financially motivated, with payment data remaining the most-sought-after and lucrative commodity by threat actors. Web applications, rather than point-of-sale (POS) devices, are now the main vector for retail breaches.¹

The 2020 PSR covers:

- The continuing decline of compliance with the PCI DSS
- Why CISOs often can't get the attention of corporate management
- The top 7 strategic data security management traps
- The 5 elements that make up a high-performance data security environment
- The PCI DSS compliance reference calendar

Key findings

Many organizations lack the resources or commitment from business leaders to support data security and compliance. At too many companies, data security strategies fail to align to corporate operations and strategies.

CISOs face constricted budgets, a limited hiring pool and a mountain of immediate problems to solve. This leads to short-term thinking: applying technology for quick fixes rather than developing strategic plans with top management for long-term solutions. When those quick fixes inevitably fail, CISOs move onto the next job, often in about two years. Their successors too often merely repeat the cycle.

The result: a steady multiyear decrease in PCI DSS compliance. The 2020 PSR found that only 27.9% of organizations achieved full compliance during their interim validation in 2019, down 8.8 percentage points from 2018, which was itself down 5 percentage points from 2017. Financial gain remains a primary motivator for cybercrime and accounts for nearly 9 in 10 (86%) breaches. Within the retail industry, 99% of incidents were financially motivated, with payment data remaining the most-sought-after and lucrative commodity by threat actors. Web applications, rather than point-of-sale (POS) devices, are now the main vector for retail breaches.¹

The PSR digs deep into the challenges that CISOs face and how they contribute to the breakdown of compliance, describing 7 “traps” into which data security management falls. The problems, the authors found, aren’t technological, so they can’t be solved by purchasing new tools, applications and hardware. Rather, they are organizational and require mature management skills to resolve:

- Creating formalized processes
- Building a business model for security
- Defining a sound security strategy, supported by security operating models and security frameworks
- Developing security programs and projects that drive capability and process maturity

Learn more:

To read the full Verizon 2020 PSR report, visit [verizon.com/paymentsecurityreport](https://www.verizon.com/paymentsecurityreport). For more information on improving your payment security and moving your compliance management to new levels, contact your Verizon Business Account Manager or email paymentsecurity@verizon.com

How we can help

We have one of the largest groups of PCI Qualified Security Assessors (QSAs) in the world, as ranked by the Payment Card Industry Security Standards Council (PCI SSC). We can help organizations maintain PCI compliance and reduce risk through a consistent, facilitative approach to securing payment card data.

We have:

- Delivered PCI services in 61 countries
- Over 180 security consultants in 30 countries
- Conducted more than 18,000 assessments since 2009
- Provided security consulting services since 1999 and PCI compliance services since 2003

