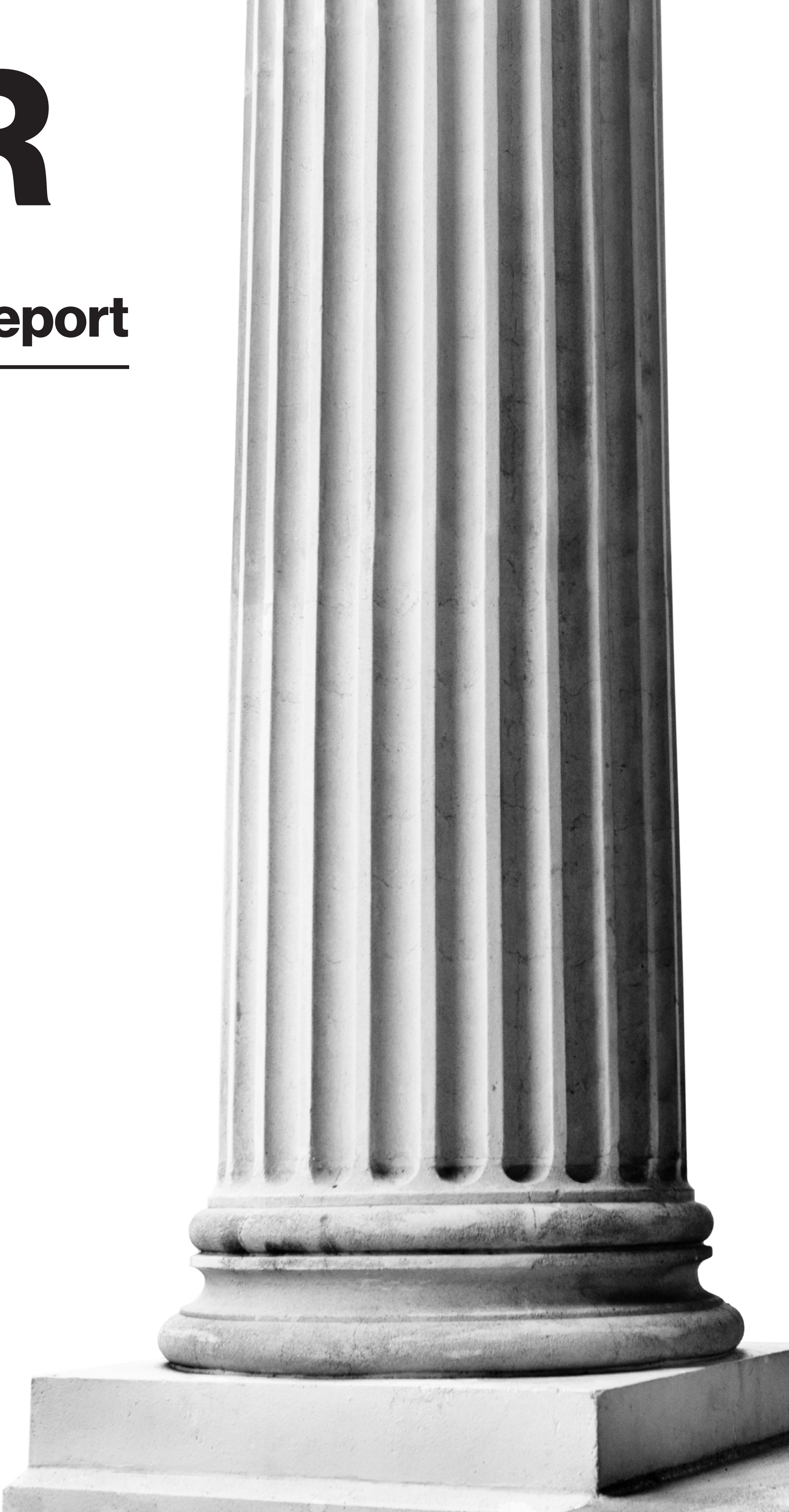
PSR

2020 Payment Security Report

Public Sector



verizon✓

Public sector organizations: Are your payments safe?

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

Data has become the universal language of the public sector, from small municipal agencies to sprawling state governments and federal agencies. Citizens rely on government organizations to safeguard this data from potential threats. While all sensitive data should be protected, payment data demands even more vigilance since it can lead to financial losses. Is your payment data secure? Maybe. And "maybe" isn't good enough in an era of escalating cyberattacks on the public sector.

Any public sector organization that accepts payments—directly or through a third-party provider—needs to address payment security as a part of its overall security plan. Credit card data and other financial and personal information must be protected at all times. No public institution wants to expose its constituents' sensitive financial data to loss, address the subsequent legal and financial impact, or damage the public's trust.

More online payments mean new security challenges.

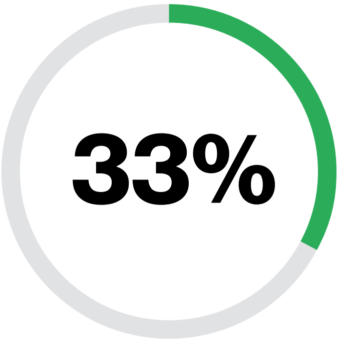
The need for security is greater than ever, thanks to the expansion of digital services offered by governmental organizations, accompanied by more (and more sophisticated) cyberattacks and data breaches. Consumer preferences were already moving from in-person to online payments before the COVID-19 pandemic, which added even more urgency to the need for contactless payments.

The risks are significant—and growing.

Recent research on data breaches raises some disturbing trends. The 2020 Verizon Data Breach Investigations Report (DBIR) highlighted a year-over-year two-fold increase in web application breaches. (All data is drawn from the 2020 PSR and DBIR.)

Stolen credentials were used in more than 80% of these cases, a worrying trend as business-critical workflows and payments continue to move to the cloud.

Ransomware continues to be a top cyberattack, disproportionately affecting the public sector. In fact, 80% of all malware attacks on educational institutions involved ransomware. Fortunately, it's possible to limit the success of ransomware attacks through good cyber hygiene and defensive strategies. That said, 33% of breaches in the public sector were caused accidentally by insiders, compared to only 12% in the manufacturing sector.



Thirty-three percent of breaches in the public sector were caused accidentally by insiders.

Here are some of the general steps you can take to keep your payment data secure, as highlighted in Verizon's 2020 PSR:

Ensure compliance with payment security standards.

The Payment Card Industry Data Security Standard (PCI DSS) is a comprehensive control framework established in 2004 that helps your agency meet the minimum data security requirements to help prevent the loss of sensitive payment data. At the standard's core are 12 requirements designed to promote data security and reduce vulnerabilities, covering security policies and standards; network architecture; configuration standards; monitoring; incident response procedures; and general rules and practices for handling, storing, processing and transmitting sensitive data. The PCI DSS covers areas of protection ranging from data storage to processing to transmittal between systems and organizations. While compliance can be a challenge for public sector organizations, noncompliance opens the door to escalating risk.

Include third-party vendors in your payment security plan.

Even if your organization relies on third-party vendors to collect payments, there are key areas of PCI data security compliance that you need to address. For example, several compliance requirements still apply, such as protocols to manage and the requirement to maintain any data that is shared with those third parties, including how that information is transmitted.

Know that technology alone isn't the answer.

A strong security strategy that helps protect against threats to sensitive payment card data must address people, processes and technology, not just one element. The PCI DSS provides a base of security requirements that can help you build this strategy.

Recognize the need for cybersecurity talent.

The well-documented talent shortage in the cybersecurity workforce affects the abilities of public sector organizations to manage the security of their increasingly complex information networks. It's important to recognize that technology alone cannot protect your payment data from cyberattacks. It requires recruiting, training and retaining dedicated, skilled security professionals and partnering with professional, reputable and expert cybersecurity service providers.

Stick with it.

Data security is not a one-time process. It requires commitment and long-term attention to strategic initiatives.

How can you protect your payments?

Given these risks and others, how can you keep your data as secure as possible, meet regulatory requirements and reduce the risk of a data breach? With preparation and planning, compliance with standards, and ongoing vigilance.

Get more details and recommended actions in the full report.

The Verizon 2020 PSR takes a careful look at this critical issue and offers valuable advice to public sector organizations and the people who lead them. In this extensive report, you'll find a detailed list of recommended actions that your organization should take to improve the effectiveness and sustainability of its data security. These recommendations can help you create a resilient security plan that mitigates risk and protects your payments.

The full report also includes information on the PCI DSS, which helps ensure compliance with this critical standard, as well as more details on public-sector cyberattacks from the 2020 Verizon DBIR.

Knowledge is one of the best ways to protect your digital government and ensure continuity of operations. Request the full, detailed report at verizon.com/paymentsecurityreport or contact Verizon today.

INF12430121