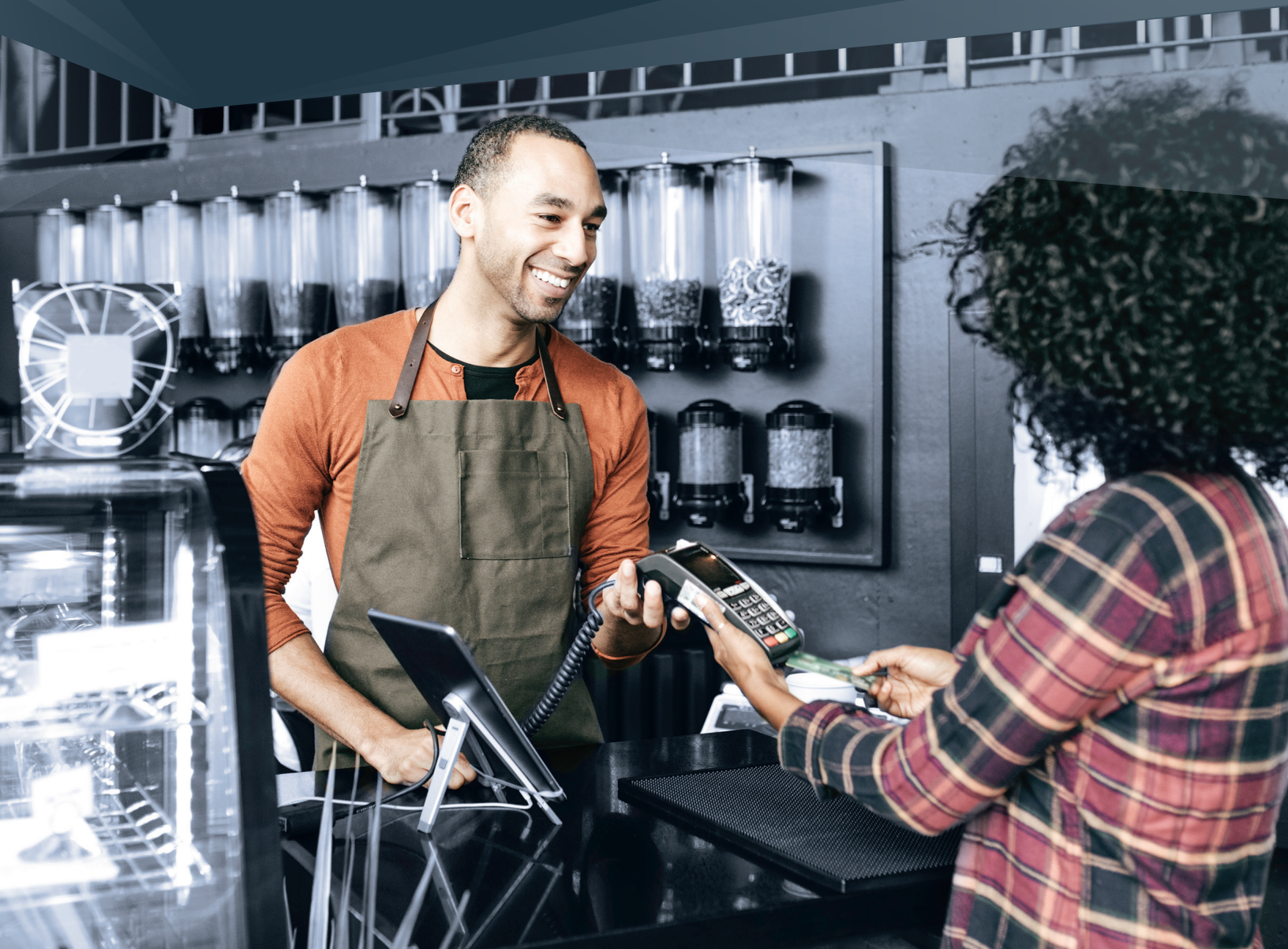
FORTINET

WHITE PAPER

# How Effective Retailers Balance Customer Engagement and PCI Compliance

## PCI DSS, PCI SSF, and Making It All Work Well



## Executive Overview

**For CIOs of retail organizations, compliance with Payment Card Industry (PCI) standards is a top concern, as the costs of noncompliance—both from the penalties assessed and potential breaches that can result—are unacceptable. Organizations now face even broader requirements when the PCI Software Security Framework (PCI SSF) replaces the 15-year-old PCI Data Security Standard (PCI DSS) over the next three years. The new standard addresses new technologies that have come online, but still adheres to the same security principles that form the basis for PCI DSS.**

**Unfortunately, PCI compliance can complicate the CIO's primary responsibility—providing IT resources that work effectively, efficiently, and at minimal cost. The fragmented security infrastructure found at many organizations complicates PCI compliance while creating operational inefficiencies, performance problems, and increased cost. This state of affairs also impedes critical efforts to engage customers in a highly competitive retail environment—efforts that sometimes can make or break a retail organization's survival. And a disaggregated security architecture also complicates broader efforts to secure an organization's infrastructure.**

**"Credit card data theft is so common that it rarely makes major headlines any more. If there is a headline, it's often framed as, 'Another day, another breach.'"[1]**

**While the requirements of PCI DSS and PCI SSF may seem daunting, they really involve implementing security best practices that every organization should adhere to in today's advanced threat landscape. What is required is a holistic, strategic approach that enables a proactive stance toward security.**

For any industry that sells products and services to consumers, the ability to accept payment cards is a business imperative, and any interruption to that ability can cause business to grind to a halt. Yet, payment card information remains an attractive target for cyber criminals. One recent survey found that fully half of U.S. retail brands had been impacted by a data breach in just a 12-month period.[2] Another study found that 23 million stolen credit cards are currently being traded on the dark web.[3]

Media reports about these breaches result in diminished brand value for retailers,[4] and the cost of remediating systems and compensating victims can be significant. Another cost is related to compliance. Although the exact amounts assessed in specific cases are not disclosed, noncompliance with PCI DSS can bring penalties of between $5,000 and $200,000 per month.[5] For the CIO, avoiding these costs is of the utmost importance.

## Evolving and Broadening PCI Standards

PCI DSS, launched in 2004, is a global standard for the security of cardholder data. The PCI Security Standards Council (PCI SSC) is responsible for maintaining, evolving, and promoting the standard.[6] Specifically, evolution of the standard has been a continual process, with several major updates and many minor ones over a decade and a half.

The PCI Security Standards Council is well into the development of the first major overhaul to PCI DSS since 2013. PCI DSS v4.0, set to release mid-2021, aims to address changes in technology, risk mitigation techniques, and the growing threat landscape. CIO's must be ready to comply with new requirements, even as compliance rates with current PCI standards may actually be slipping. PCI SSF updates the standard to encompass new technologies and a more complex threat landscape. It covers DevOps and agile development, transparent deployment, and consistency of security design.

The new framework will especially impact retailers that are leaning heavily on digital transformation (DX) initiatives to bolster or reinvent their engagement with customers.[7] The good news is that while some details of the standard are new, PCI SSF still follows the same basic security principles found in PCI DSS—and just about every other security standard:

- Identify your critical assets
- Create secure default configurations
- Protect sensitive data
- Maintain authentication and access control
- Enable attack detection
- Implement the latest guidance and patches from technology vendors

## PCI Compliance and the CIO's Key Challenges

Even for the CIO of a retail organization, PCI compliance is just one of many challenges. But problems with PCI compliance can impact almost every other priority in the CIO's charter. Consider the following business imperatives:

### Operational and cost efficiency

In a nutshell, the job of the CIO is to deliver technology that gets the job done efficiently, effectively, and at minimal cost. Even when CIOs deploy flashy new DX initiatives that have the potential to have direct, positive impact on the bottom line, these efforts will not be successful if there are problems with any of these basic elements:

- **Network performance.** As more and more services move to distant, cloud-based data centers, network traffic increases.[8] This creates opportunities for latency and problems delivering services across a network of brick-and-mortar store locations.
- **Operational efficiency.** Whether in network operations or security operations, manual processes and disconnected systems mean unnecessary cycles by highly paid IT staff, and distraction from more strategic initiatives.
- **Providing adequate staffing.** The skills shortage for cybersecurity talent, as well as other IT functions, is real and is getting worse.[9]
- **Minimizing costs.** Retail is well known for razor-thin profit margins, and every penny saved on IT increases the odds that the company will be profitable.

For retail organizations, PCI compliance issues can get in the way of these basic elements of the CIO's job. If inadequate security controls result in manual security and compliance policies, network performance and operational efficiency can be negatively impacted—and the transactions of customers trying to make purchases can even be slowed. A reactive, "all-hands-on-deck" approach to PCI audits adds to these inefficiencies and increases the chances that the aforementioned financial penalties will be assessed.

### Bolstering customer experience

Competition with online retailers has resulted in the shuttering of thousands of retail stores in the past several years,[10] and even less dominant online retailers risk being marginalized because of a lack of visibility. Research shows that the ability for customers to have a consistent, positive experience with a brand—online and, if applicable, in person—is paramount.[11] Businesses need to innovate in the following areas in order to survive:

- **Keeping pace.** Retailers cannot afford to fall behind regarding customer experience. They must meet—and exceed—competitors' standards and quickly respond to new customer preferences.
- **Engaging with customers.** Successful retailers are connecting with customers at the individual level with customized, targeted engagement campaigns, proactive live chat for mobile and desktop visitors, and online kiosks at physical store locations.
- **Making purchasing easy.** Few things are more frustrating to a consumer than wanting to make a purchase but having to jump through multiple hoops to do so. One-click purchasing and other convenience innovations can increase sales.

Accomplishing these changes often involves the use of DevOps or agile development processes to speed time to market for new applications. But if manual security processes are required for an organization to remain PCI compliant, many of the gains in efficiency and speed on the development side will be offset. And bypassing those manual controls can result in PCI noncompliance—or even a breach.

### Securing the infrastructure

Cybersecurity has become an increasingly important priority at all types of organizations in recent years. The result is that at many companies, the CISO is now a peer of the CIO, reporting directly to the CEO or even the board of directors.[12] Whether or not a CIO is responsible for day-to-day security operations, he or she still has significant responsibilities around security[13]—and those responsibilities have become more complex:

- **An expanded attack surface.** DX initiatives have greatly expanded the attack surface in recent years: multiple public and private clouds, proliferating Internet-of-Things (IoT) devices, bring-your-own-device (BYOD) policies for employees, and network traffic over the public internet. The result is often a proliferation of point security solutions and disconnected tools provided by cloud vendors to cover these new elements.
- **Increased security complexity.** The resulting silos mean a lack of visibility into the overall security infrastructure and decentralized control of security tools. This results in operational inefficiencies caused by manual processes: tedious log pulls from multiple security solutions, manual correlation of threat data and compliance reporting, and even manual threat response.
- **An advanced threat landscape.** Threat actors are delivering attacks with increasing volume, velocity, and sophistication. Cyber criminals are using advanced techniques like natural language processing (NLP), artificial intelligence (AI), and machine learning (ML) to make their attacks faster, increasingly targeted, and more effective. This means that legacy, more reactive approaches to security are no longer adequate.

These problems are closely related to PCI compliance. A fragmented security architecture results in manual processes that are too slow and cumbersome to effectively deal with today's advanced threats. These same manual processes result in a reactive approach to PCI compliance.

## A Holistic Approach Is Needed

While PCI compliance is understandably viewed in terms of a checkbox by retailers, keeping customers' payment card information safe is really more a matter of being strategic about security. Going back to the six basic security principles outlined in PCI DSS is instructive:

"The problem lies in the fact that security professionals and their bosses are still under the false impression that compliance equals security."[14]

- **Identify your critical assets.** This is increasingly difficult in today's broadly distributed corporate networks, but every CIO must know exactly where their organizations' payment card data resides.
- **Create secure default configurations.** Configuration errors are a major cause of breaches, and manual configuration introduces almost inevitable human error.
- **Protect sensitive data.** Loyalty card holders often have a lot of other personal information tied to their payment card information in retailers' systems, increasing complexity.
- **Maintain authentication and access control.** Gone are the days that a username and password were adequate to keep unauthorized users out of a system. Cyber criminals now troll networks to find credentials with which they can impersonate trusted users.
- **Enable attack detection.** Signature-based approaches to threat detection are no longer adequate, as almost all malware now changes characteristics on the fly and as many as 40% of attacks are previously unknown.
- **Implement the latest guidance and patches from technology vendors.** Manual approaches to patches and updates also introduce the potential for human error or errors in prioritization.

When placed in a bulleted list, these requirements can seem daunting. But viewed from a higher level, these are simply the best practices that every organization needs to follow to protect themselves in the current threat landscape. What is needed is a comprehensive, strategic approach to cybersecurity that enables compliance to take care of itself.

1 Taylor Armerding, "New Software Standards Aim To Slow Rampant Credit Card Theft," Forbes, January 30, 2019.
2 "2018 Thales Data Threat Report—Retail Edition," Thales Security, accessed August 8, 2019.
3 "Sixgill Threat Intelligence Report: Underground Financial Fraud: H1-2019," Sixgill, July 18, 2019.
4 For example, Dennis Green, et al., "If you bought anything from these 13 companies recently, your data may have been stolen," Business Insider, August 15, 2019.
5 "Fines for Non-compliance," PCI DSS Compliance, accessed August 8, 2019.
6 "About Us," PCI Security Standards Council, accessed August 8, 2019.
7 Taylor Armerding, "New Software Standards Aim To Slow Rampant Credit Card Theft," Forbes, January 30, 2019.
8 Andy Patrizio, "Enterprises are moving to SD-WAN beyond pilot stages to development," Network World, May 7, 2018.
9 Jon Oltsik, "The cybersecurity skills shortage is getting worse," CSO, January 10, 2019.
10 Doug Whiteman, "These Chains Have Announced a Ton of Store Closings in 2019," MoneyWise, August 16, 2019.
11 Michelle Grant, "Where Retailers Are Placing Their Omnichannel Bets In 2019," Forbes, December 14, 2018.
12 "The CISO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, April 26, 2019.
13 "The CIO and Cybersecurity: A Report on Current Priorities and Challenges," Fortinet, May 23, 2019.
14 "What does PCI compliance really mean?" TechTarget, September 3, 2009.

FORTINET

www.fortinet.com



August 17, 2020 4:09 AM

744374-0-0-EN