Overcoming PCI DSS compliance challenges for small and medium-sized businesses

Article

No matter which industry you operate in or what size business you have—small, medium or large—you need to meet the payment card industry (PCI) security compliance requirements and validate compliance annually if you accept card payments and process, transmit or store cardholder data (CHD).

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards that has existed since 2004. The card brands (Visa, Mastercard,® American Express,® Discover® and JCB) created the PCI DSS to ensure that businesses storing, processing or transmitting payment card data do so within a secured environment that meets a minimum baseline of security control requirements.

PCI DSS comprises a set of 12 Key Requirements that cover six high-level objectives. The standard's fundamental purpose is to inform entities about how to become more secure, specify a baseline data security standard for building and maintaining a secure network, protect CHD, regularly test and monitor critical system components, and provide overall management guidelines for sustaining a secure payment environment.

These standards, discussed in the Verizon 2020 Payment Security Report (PSR), are designed to protect entities and their customers from breaches that could negatively affect their businesses, finances and reputations. Customers trust that merchants will protect their payment card information. If the merchants fail to do so, customers are unlikely to continue to support that business—which is why securing your customers' payment data should always be a priority.

Data security and compliance challenges

Small and medium-sized businesses (SMBs) have unique struggles with securing their data. While smaller businesses generally have less card data to process and store than larger businesses, they have fewer resources and smaller budgets for security. Their organizations often do not have the same available resources that larger corporations can access to maintain compliance with the PCI DSS. The measures needed to protect sensitive payment card data should not be perceived as too time-consuming and costly just because of the size of the organization. Worth noting is that the likelihood of a data breach for SMBs is high.[1] Therefore, it is not a viable option to avoid committing resources for maintaining PCI DSS compliance.

Smaller businesses are not immune to data breaches.

Threats to payment card data continue to increase and impact the payment security landscape in numerous and increasingly insidious ways. According to the 2020 Verizon Data Breach Investigations Report (DBIR),[1] a growing number of SMBs are using cloud- and web-based applications and tools. These services can make them prime targets for threat actors determined to compromise payment security data.

Findings from the 2020 DBIR show that:

- Phishing is the biggest threat for small organizations, accounting for over 30% of breaches, followed by the use of stolen credentials (27%) and password dumpers (16%)
- Threat actors target credentials, personal data and other internal business-related data, such as medical records, internal secrets or payment information
- Over 20% of attacks are against web applications and involve the use of stolen credentials

Small and medium-sized organizations experience more payment card data-related breaches than large organizations, according to Verizon's six-year data breach trends for 2014 to 2019.[1] Combined, SMBs account for 55% of confirmed payment card data breaches.

Organization size	Number of employees	% of breaches
Very small	1 to 10	12%
Small	11 to 100	7%
Medium	101 to 1,000	19%
Large	1,001 to 10,000	17%
	10,001 to 25,000	2%
	25,001 to 50,000	17%
Very large	50,001 to over 100,000	22%

Lack of sustainable data security

Based on Verizon research, fewer than one-third of organizations (27.9%) maintained their required set of PCI data security controls during their 12-month compliance cycle in 2019. This is a further 8.8 percentage-point (pp) drop from 2018, when only 36.7% of organizations demonstrated full compliance.

With the potential for such severe repercussions, it's not clear why compliance sustainability continues to decline, as seen in the 2020 PSR. Fewer and fewer organizations are demonstrating the ability to keep a minimum baseline of security controls in place.

Small-business owners need to use available resources, primarily their acquiring banks and third-party vendors, to ensure their systems meet PCI DSS requirements.

Recommended data security actions for SMBs

To maintain PCI data security compliance, all applicable requirements must be met. In PCI DSS v3.2.1, there are over 400 actions your business is required to take in order to ensure that your operations remain PCI compliant.

Data security governance	**Establish, publish, maintain and disseminate a security policy.** • Design, implement and maintain a data security and compliance strategy for your business • Create a security policy for your business that addresses all aspects of the PCI DSS
Service providers	**Maintain and implement policies and procedures to manage service providers.** • Choose a PCI-compliant payment gateway • Use a PCI Security Standards Council (SSC)-validated point-to-point encryption (P2PE) solution • Monitor service provider compliance status to prevent lapses in compliance
Security awareness	**Implement a formal security awareness program to make all personnel aware of the cardholder data security policy and procedures.** • Educate your employees about security and protecting CHD • Have a program in place that teaches employees what they should and shouldn't be doing when accepting payments from customers • Ensure that staff is educated on an annual basis (at minimum) to include education on device tampering
Security testing	**Maintain an inventory of system components that are in scope for PCI DSS.** • Run internal and external network vulnerability scans at least quarterly and after any significant change • Maintain accurate asset inventory and ensure that vulnerability scanning is being performed regularly while obtaining a passing scan on, at minimum, a quarterly basis • Make sure that penetration test(s) are performed in adherence to PCI DSS Requirement 11.3

Physical security	**Protect devices that capture payment card data via direct physical interaction with the card from tampering and substitution.** • Periodically inspect device surfaces to detect tampering • Regularly check terminals, PIN pads and computers to ensure that rogue software or "skimming" devices are not installed • Secure physical backup media that contains sensitive information • Maintain camera data retention and perform point-of-sale (POS)/point-of-interaction (POI) device inspections at least weekly and have a documented process in place
Wireless security	**Change all wireless vendor defaults at installation.** • Make sure your wireless devices are password-protected and use strong encryption. Set a strong password for your wireless router, and make sure that all available security and encryption features are enabled and properly configured • Never use default passwords; it's critically important that you replace the default passwords on your networked devices with the strongest ones possible • Ensure that detection of unauthorized wireless access devices is included in the incident response plan
Data transmission security	**Use strong cryptography and security protocols to safeguard sensitive cardholder data.** • Use only secure transmission protocols, such as Transport Layer Security (TLS) v1.2, to prevent unauthorized access and mitigate risk of interception and capture of sensitive data • Proactively develop a migration plan should transmission encryption protocols be cracked and thus deemed no longer secure • Make sure you only collect payment card information on a secure web page
Data retention	**Keep cardholder data storage to a minimum by implementing data retention and disposal policies, procedures and processes.** • Do not store any payment card data unnecessarily • Do not capture credit card information in written form unless the process is authorized and formally documented, and checks and balances are in place to make sure that the data does not exceed the defined retention period • Never store the magnetic track data from any card, in any format • Never store the CID/CVV2 card security code (the three-digit number on the back of Visa/MasterCard/ Discover cards, or the four-digit number on the front of American Express cards) in any format, in any way, ever
Incident response	**Establish, document and distribute security incident response and escalation procedures to ensure timely and effective handling of all situations.** • Implement an incident response plan. Be prepared to respond immediately to a system breach • In the event of a breach or suspected data breach, contact the acquiring bank immediately • Provide appropriate training to staff with security breach response responsibilities
Capacity planning and resource management	**Ensure that staffing for roles involving information security responsibility is adequate for the size of the environment and the technologies in scope.** • Make the best use of available people and technology
Avoiding the use of outdated infrastructure	**Ensure that all system components and software are protected from known vulnerabilities by installing applicable vendor-supplied security patches. Install critical security patches within one month of release.** • Maintain hardware and software support for all critical system components • Be proactive in monitoring the support life cycle for all critical system components to include both hardware and software • Plan upgrades and decommissions in a timely manner

For more details on the state of payment security, visit verizon.com/paymentsecurityreport

The ultimate goal of PCI compliance should be to develop and maintain a mature data security compliance program based on a sound strategy that results in sustainable and effective data security with continuous improvement in a consistent and predictable manner, as noted in the Verizon 2020 PSR.

Top 7 strategic data security management traps

Lack of data security sustainability and effectiveness is largely the result of poor business, strategic and operational architecture design and execution.

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 lack of continuous improvement
7. Communication and culture constraints

At a time when organizations of all sizes are struggling to maintain a minimum baseline of security controls, small and medium-sized businesses face unique challenges with meeting PCI compliance. At a bare minimum, they need to stay vigilant and well-educated on all available resources to ensure their systems meet PCI DSS requirements, and take the essential steps necessary to safeguard payment security.

Additional guidance

A handy PCI Data Security Essentials Evaluation Tool for Small Merchants is available at https//www.pcisecuritystandards.org/pci_security/small_merchant_tool_resources

Common data security mistakes

Chief Information Security Officers (CISOs) need to correct unproductive practices in their organizations that don't promote and sustain effective data security, 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:** inability to balance quick wins with long-term strategic initiatives
- **Being unaware of data and IT assets:** operating with many blind spots; not knowing where data exists and its sensitivity level; 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:** people and departments not believing they're at risk; thinking they are too insignificant to become a target

verizon

1 Verizon 2020 Data Breach Investigations Report, 2020. enterprise.verizon.com/resources/reports/dbir/