2016 PCI COMPLIANCE TRENDS

HOW DOES YOUR ORGANIZATION RANK?

SECURITYMETRICS CUSTOMER TRENDS

Average time to compliance:
156 days

85%
of SecurityMetrics customers that started their SAQ finished it

84%
of SecurityMetrics customers that started their SAQ are passing

On average, customers use support
2.5 times
before becoming compliant

Average time from finished first scan to first passing scan
19 days

Average number of times scanned until merchants pass their PCI scan:
1.79 times

TOP 5 FAILED VULNERABILITIES

SENSITIVE DATA EXPOSURE
Occurs when applications do not properly protect sensitive data from attackers (e.g., lack of encryption).

PLAINTEXT PASSWORD COMMUNICATION
Happens when users incorrectly handle plaintext of passwords (i.e., saving passwords in web browsers).

SECURITY MISCONFIGURATION
Exists when applications and/or systems don't have proper security hardening in place (e.g., out-of-date software).

EXPOSED DATABASE PORT
Occurs when a database port is open and not fully upgraded/patched, due to a software vulnerability that could be exploited.

CROSS-SITE SCRIPTING (XSS)
An attack that ultimately allows attackers to gather user data like payment cards or passwords.

TOP 10 FAILING SAQ SECTIONS

We reviewed our merchant database in search of the top 10 areas where merchants struggle to become compliant. These are the results:

1 REQUIREMENT 12.5.3–12.6.A:
Establish, document, and distribute security incident response and escalation procedures, administer user accounts, and monitor/control access to data.

2 REQUIREMENT 12.10.1.A:
Verify incident response plan responsibilities, business recovery procedures, data backup processes, and legal requirements for reporting compromises.

3 REQUIREMENT 9.9.2.B:
Verify personnel are aware of procedures for inspecting devices and that devices are periodically inspected for evidence of tampering.

4 REQUIREMENT 12.1:
Establish, publish, maintain, and disseminate a security policy.

5 REQUIREMENT 1.1.3.A:
Establish a current diagram that shows all cardholder data flows across systems and networks.

6 REQUIREMENT 9.9.2.A:
Verify documented processes include procedures for inspecting devices and frequency of inspections.

7 REQUIREMENT 12.3.3:
List devices and personnel with access to data.

8 REQUIREMENT 12.3.5:
List acceptable uses of used technology.

9 REQUIREMENT 1.1.1.B:
Examine firewall and router configurations to verify inbound and outbound traffic is limited to that which is necessary for the cardholder data environment.

10 REQUIREMENT 1.1.3.B:
Ensure a process exists to keep the cardholder diagram current.

Questions About PCI Compliance?
Download our 2016 Guide to PCI DSS Compliance

securityMETRICS®