securityMETRICS®

2019

PCI DSS Data Breach Analysis

SecurityMetrics Forensic Investigation Results from 2018

PCI DSS REQUIREMENTS IMPLEMENTED AT THE TIME OF COMPROMISE

The following graphs demonstrate the compliance of compromised businesses we investigated noting whether each requirement at the time of compromise in 2018 was in place or not:

NON-COMPLIANCE TO REQUIREMENTS CONTRIBUTED TO A DATA BREACH

The following graphs detail how non-compliance to the different PCI requirements affected breaches for compromised organizations we investigated in 2018:

REQUIREMENT 1 *Protect your system with firewalls*

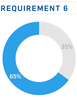
REQUIREMENT 2 *Use adequate configuration standards*

REQUIREMENT 3 *Secure cardholder data*

REQUIREMENT 4 *Secure data over open and public networks*

REQUIREMENT 5 *Protect systems with antivirus*

REQUIREMENT 6 *Update your systems*

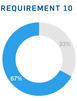


REQUIREMENT 7 *Restrict access*

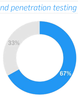
REQUIREMENT 8 *Use unique ID credentials*

REQUIREMENT 9 *Ensure physical security*

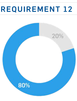
REQUIREMENT 10 *Implement logging and log monitoring*



REQUIREMENT 11 *Conduct vulnerability scans and penetration testing*



REQUIREMENT 12 *Start documentation and risk assessments*



Forensic

TAKEAWAYS FROM 2018

THE AVERAGE ORGANIZATION WAS **vulnerable*** FOR **275 DAYS**

CARDHOLDER DATA WAS **exfiltrated*** FOR AN AVERAGE OF **127 DAYS**

CARDHOLDER DATA WAS **captured*** FOR AN AVERAGE OF **127 DAYS**

57% HAD **firewalls** IN PLACE AT TIME *of compromise*

50% OF ORGANIZATIONS WERE **breached** *through* REMOTE EXECUTION/INJECTION

33% OF ORGANIZATIONS WERE **breached** INTERNALLY (i.e., employee assisted)

17% OF ORGANIZATIONS WERE **breached** *through* PHISHING EMAILS

TERMS TO KNOW

*Vulnerable: *A state in which a weakness in a system, environment, software, or website could be exploited by an attacker.*

*Captured: *The time that data is being recorded, gathered, or stored from an unauthorized source.*

*Exfiltrated: *The unauthorized transfer of data from a system.*

NEED HELP WITH PCI COMPLIANCE?

https://www.securitymetrics.com/pci-audit