CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH

PCI/DSS CYBERSECURITY CHEAT SHEET

① Payment Card Compliance

The Payment Card Industry Data Security Standard (PCI DSS) is a set of data protection mandates developed by the major payment card companies and imposed on businesses that store, process, or transmit payment card data. As part of their contracts with the card companies, merchants and other businesses that handle card data may be subject to fines if they fail to meet the requirements of PCI DSS compliance.

② PCI Overview

Every retailer is required to comply. Depending on the e-commerce technology and backend they choose to use, PCI compliance can be an easy check on a long list of things retailers need to do to ensure their customers are transacting securely. Or it can be a big pain –– costing ample time, resources and money.

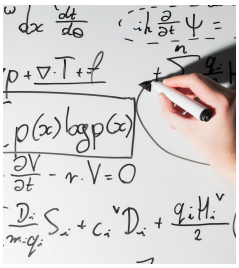
The Big "12" of PCI/DSS ③

- Install and maintain a firewall configuration to protect cardholder data.
- Create custom passwords and other unique security measures rather than using the default setting from your vendors
- Protect stored cardholder data.
- Encrypt transmission of cardholder data across open, public networks.
- Use and regularly update anti-virus software.
- Develop and maintain secure systems and applications.
- Restrict access to cardholder data by business need-to-know.
- Assign a unique ID to each person with computer access.
- Restrict physical access to cardholder data.
- Track and monitor all access to network resources and cardholder data.
- Regularly test security systems and processes.
- Maintain a policy that addresses information security.

Continue reading on next page >

PCI/DSS CYBERSECURITY CHEAT SHEET

④ Seems Easy -- not so fast



PCI DSS outlines 12 requirements for compliance. While that seems like it might be simple and straight forward once you check through their online documentation you will find that maintaining PCI compliance is onerous, complex and frustrating — those 12 requirements contain a total of 251 sub-requirements with which you must comply to fully address the growing threats to customer payment information.

CRAIG PETERSØN

AMERICA'S LEADING SECURITY COACH