Challenges of Standards Compliance

Ralph Spencer Poore
Director, Emerging Standards

PCI Security Standards Council

National Institute of Standards and Technology
U.S. Department of Commerce

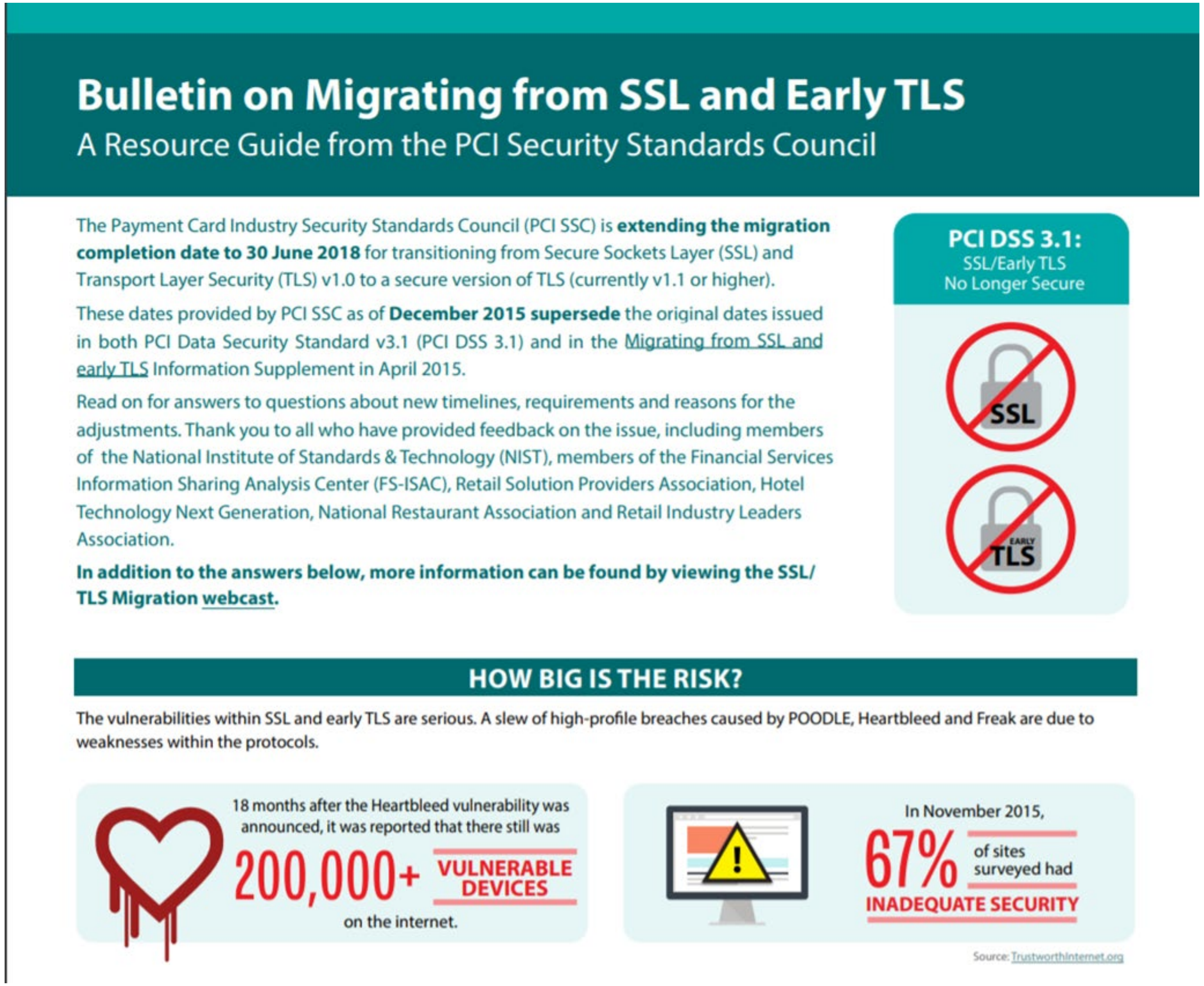
Security Standards Council™

PCI & SSL/TLS Migration

The PCI Data Security Standard (DSS)

- Had used SSL in an example—which had to be removed
- Had to produce guidance on migration to TLS 1.1 or above
- Migration to TLS 1.2 or above; protocol security is a moving target
- Balancing security requirements under TLS 1.3

PCI Documents



Bulletin on Migrating from SSL and Early TLS

A Resource Guide from the PCI Security Standards Council

The Payment Card Industry Security Standards Council (PCI SSC) is **extending the migration completion date to 30 June 2018** for transitioning from Secure Sockets Layer (SSL) and Transport Layer Security (TLS) v1.0 to a secure version of TLS (currently v1.1 or higher).

These dates provided by PCI SSC as of **December 2015 supersede** the original dates issued in both PCI Data Security Standard v3.1 (PCI DSS 3.1) and in the Migrating from SSL and early TLS Information Supplement in April 2015.

Read on for answers to questions about new timelines, requirements and reasons for the adjustments. Thank you to all who have provided feedback on the issue, including members of the National Institute of Standards & Technology (NIST), members of the Financial Services Information Sharing Analysis Center (FS-ISAC), Retail Solution Providers Association, Hotel Technology Next Generation, National Restaurant Association and Retail Industry Leaders Association.

In addition to the answers below, more information can be found by viewing the SSL/TLS Migration webcast.

PCI DSS 3.1:
SSL/Early TLS
No Longer Secure

HOW BIG IS THE RISK?

The vulnerabilities within SSL and early TLS are serious. A slew of high-profile breaches caused by POODLE, Heartbleed and Freak are due to weaknesses within the protocols.

18 months after the Heartbleed vulnerability was announced, it was reported that there still was **200,000+ VULNERABLE DEVICES** on the internet.

In November 2015, **67%** of sites surveyed had **INADEQUATE SECURITY**

Source: Trustworthinternet.org

NIST

Collaboration among Standards Bodies

PCI relies on NIST and other Industry, National, and International Standards Bodies

- On going liaisons and collaboration
- While PCI use cases may differ, we depend on common technologies
- Assessor communities rely on expertise incorporated in NIST and other applicable standards