Chapter 5
Navigating Through Choppy Waters of PCI DSS Compliance

Amrita Nanda
University at Buffalo, USA

Priyal Popat
University at Buffalo, USA

Deepak Vimalkumar
University at Buffalo, USA

ABSTRACT

PCI Data Security Standard is increasingly becoming one of the major compliance requirements all organizations are concerned about. This chapter taking a holistic approach, provides an overview of various components of PCI DSS. We discuss various versions of PCI DSS and the industries affected by this standard, the scope and requirements to comply and hesitation on part of most companies to imbibe it. We also look at the high-profile credit card breaches which have occurred recently and their impact on concerned industries. Additionally, we focus on the challenges faced by financial institutions to effectively meet PCI DSS requirements. Based on our analysis of different requirements of PCI DSS, challenges faced by organizations and recent security breaches of companies which were PCI DSS complaint at the time of breach, we propose recommendations to help organizations secure their cardholder data beyond the achieved compliance in place.

DOI: 10.4018/978-1-5225-2604-9.ch005

1. INTRODUCTION

Data breaches are continuously making headlines in the news today. As a result, most firms are now focusing on enforcing data protection. To make sure all entities comply with one industry accepted standard, PCI DSS was formed. This standard was introduced in 2004 to ensure security of cardholder data. PCI SSC (Payment Card Industry Security Standards Council) was established by major payment brands like Visa Inc., MasterCard Worldwide, American Express, Discover Financial Services and JCB which was responsible for development of security standards. After huge speculations and discussions, PCI SSC came up with PCI Data Security Standard (PCI DSS). All the major market players involved with storing, processing and transmitting card holder data are recommended to comply with it (PCI-SSC, 2014).

A study from (Verizon, 2013) also reported that in 2013, 11.1% of organizations were fully compliant with the standard at the time of their annual baseline assessment, up from just 7.5% in 2012. Also, according to their report organizations that are breached tend to be less compliant with PCI DSS than the average of organizations in this research. A 2011 Ponemon Institute study found 71 percent of companies do not treat PCI DSS as important and 79 percent among them have experienced data breaches (Ponemon, 2011). Codification of industry standards and complying of security standards has become top priority for all the major financial institutions since 2010. With growing political and government pressure abiding by these standards gas become very stringent.

In this paper, we conducted detailed analysis of PCI DSS scope, requirements and the industries affected by this standard. Additionally, we came across challenges faced by industries in complying with PCI DSS.

Recent news have reported many high profile breaches which have occurred in Target, Home Depot and Staples causing huge customer credit card information being lost (Tobias, 2014). The above cases instigated us to study these major breaches and analyze why the PCI DSS breach occurred even when these merchants were PCI DSS compliant at the time of breach. We analyzed the data breaches to find vulnerabilities in each case leading us to build a framework to recommending organizations on the critical aspects like Point of Sale devices, networks and software thus going beyond the PCI DSS requirements. Furthermore, we suggest that the need of advanced technologies is imminent given the fact that existing controls are being attacked immaterial of the organization being PCI DSS compliant.