SMALL BUSINESS COMPLIANCE WITH PCI DSS

Danial Clapper, Western Carolina University
William Richmond, Western Carolina University

ABSTRACT

Americans increasingly use payment cards (debit cards and credit cards) for their purchases. To satisfy their customers and thus increase sales, more small businesses accept payment cards. Accepting payment cards, however, comes with additional risks and costs. One of those costs is complying with the Payment Card Industry Data Security Standard (PCI DSS) – a set of security standards developed in 2004 as a cooperative effort among card issuers such as Visa and MasterCard to protect cardholder data. This standard was developed and is updated by the PCI Security Standards Council and applies to any entity that processes, stores or transmits cardholder data.

The focus of the PCI Council was initially on very large merchants with millions of payment card transactions per year. Those efforts have paid off and it now appears that the PCI Council is turning its focus to small merchants. Recognizing the high costs and technical barriers to the PCI compliance process, in 2015 the council created a taskforce dedicated to improving small merchant card security. Also in 2015, Visa issued a security bulletin stating that all small merchants that accept Visa cards must be in PCI compliance by 2017. This new focus of the PCI Council seems to indicate that small merchants who have not currently gained PCI compliance are going to face increasing pressure to do so.

PCI DSS requires the merchant to take a number of actions as part of their compliance. These include, but are not limited to, installing and automatically updating anti-virus software, completing a self-assessment, developing a security plan, having their network evaluated. Complying with PCI DSS is difficult for small businesses, and it is not always done, even by businesses that accept payment cards.

This study examines small business compliance with PCI DSS. A compliance model based on earlier research on security policy compliance is developed. The model posits that compliance with PCI DSS depends on the business's intention to comply and that intention to comply is influenced by its awareness of PCI DSS, normative beliefs, peer behavior, self-efficacy, value of complying and the cost of compliance. Additionally, the knowledge of PCI DSS depends on the business's general IT awareness coupled with communications from their merchant bank. This model is tested with data gathered from 74 small, rural businesses in western North Carolina.

Parts of the model are supported. Knowledge of PCI DSS is associated with general IT security knowledge and merchant bank communication. This knowledge of PCI DSS coupled with self-efficacy and peer behavior does influence the business's intention to comply. Surprisingly, nether neither the cost of compliance nor the benefit of compliance (cost of non-