PAYMENT CARD INDUSTRY DATA SECURITY STANDARD (PCI DSS)

BUSINESS INFO SYSTEMS & ANALYTICS- CA02

PROFESSOR BRYAN REAGAN

NOVEMBER 11TH, 2016

Giana Fernander
Freddie Armour
Ian Edwards

The Payment Card Industry Data Security Standards (PCI DSS) is a global organization that maintains and promotes PCI standards for the safety of cardholders all over the world (PCI Security Standards Council, n.d.). PCI strives to serve merchants whether big or small, point of sale vendors, financial institutions and developers of hardware and software mainly those who work with and are associated with payment cards.

PCI lists two priorities for their work which are helping financial institutions and merchants understand and implement standards for security policies. Secondly, they help these vendors understand and implement standards to create secure payment solutions (PCI Security Standards Council, n.d.). They are helping to protect the safety of data so it is evident that every entity involved follows the PCI DSS.

PCI has compliance levels that each merchant must fall under based on Visa transactions over twelve months. PCI bases this transaction volume on a number of Visa transactions including prepaid, debit and credit from a merchant "Doing Business As" (PCI Compliance Guide, n.d.) There are four merchant levels and they are as follows along with the requirements needed to fall under any one of the categories.

Merchant Level	Requirements
1	Any merchant that is processing over six million Visa transactions per year
2	Any merchant that is processing between one and six million Visa transactions per year

3	Any merchant that is processing between twenty thousand and one million Visa e-commerce transactions per year
4	Any merchant that is processing less than twenty thousand Visa e-commerce transactions per year

The founding members of the PCI DSS Council are, American Express, Discover Financial Services, JCB International, MasterCard, and Visa Inc., and they all incorporate the PCI DSS as a requirement for the data security compliance programs. These payment brands and members equally share the governance of the council and share input equally about the PCI standards and work responsibility of the entire organization. Other organizations that may participate include banks, merchants, hardware and software developers, and point of sale vendors. The PCI council is ran by an executive committee that sets policies, this is comprised of representatives from the founding payment brands and members that take part in the governance of the organization. An advisory board is made up from the participant organizations and they provide their opinions on the organization and give their feedback on how the PCI Standards are evolving.

PCI claims that their biggest challenge has been global adoption among the smaller merchants who find PCI DSS to be a bit complex for the size of the business (Kitten, 2016). The month before the article was written PCI came up with a resource to simplify the compliance process by identifying critical requirements.

In conclusion, the fact that the PCI council took the complexity out of PCI DSS compliance is a big accomplishment as well as educating their merchants on how critical these standards and basic security measures are for their companies. This resulted in broadening the horizon for most merchants and making them realize the need for security regardless of the size of the organization.

Works Cited

Kitten, T. (2016, August 15). *How PCI Acceptance Has Improved Security*. Retrieved from Bank Info Security: http://www.bankinfosecurity.com/blogs/how-pci-acceptance-has-improved-security-p-2219

PCI Compliance Guide. (n.d.). Retrieved from https://www.pcicomplianceguide.org/pci-faqs-2/

PCI Security Standards Council. (n.d.). Retrieved from https://www.pcisecuritystandards.org/pci_security/