Vol. 4 No. 12
December 2012

BUSINESS*insights*

Is Your Business PCI Compliant?

There's no greater risk to your business than to have a security breach of a customer's payment card transaction. In today's social networking world, that kind of mistake could generate thousands of Tweets that would cause an immediate and huge loss of business.

The Payment Card Industry Security Standards Council (PCI) was created in 2006 to increase controls that prevent this kind of breach and reduce related fraud. Getting compliant with their recommendations is a big responsibility of every business that accepts payment cards. There is some effort involved, but following their standard will protect your business and your customers.

As of January 2012 PCI requires your business to implement the following:

- **Build and maintain a secure network.**
  To fully comply with this rule, it is not enough to use the vendor-provided defaults on your system for passwords and other security. You will need to install and maintain a firewall on your network to be sure you are properly protecting cardholder data.

- **Encrypt cardholder data.**
  For proper protection, cardholder data running across open, public networks must be encrypted during transmission.

- **Maintain a vulnerability management program.**
  It's essential that you use and regularly update anti-virus software on all systems commonly affected by malware as well as to develop and maintain secure systems and applications.

- **Implement strong access control measures.**
  There are three important steps your business needs to take to control access to your network:
  1. Restrict access to cardholder data to only those directly involved in the transactional information.
  2. Assign a unique ID to each person with computer access to your network.
  3. Restrict physical access to cardholder data.

- **Regularly monitor and test networks.**
  Your business will need to track and monitor all access to network resources and cardholder data as well as test security systems and processes on a regular basis.

- **Maintain an information security policy.**
  It's required that you maintain a written policy that addresses how your business is handling the security of its customer credit card transaction data.

(continue pg. 2)

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org

How compliance is enforced.

The PCI does not monitor or enforce compliance with its PCI Security Standards. It does not impose penalties. They are enforced by the payment brands and their partners. In fact, it is the payment partners that formed the PCI and are part of its governing body.

If you have questions about the requirements or your compliance, you can contact the payment brand companies directly. Below are links to their Websites.

- American Express: www.americanexpress.com/datasecurity
- Discover Financial Services: http://www.discovernetwork.com/merchants/
- MasterCard Worldwide: http://www.mastercard.com/sdp
- Visa Inc: http://www.visa.com/cisp
- Visa Europe: http://www.visaeurope.com/ais

Getting educated on PCI requirements.

The PCI Security Standards Council provides information and events to help businesses get educated on efficient and effective ways to best meet the standards. You can learn more at their Website https://www.pcisecuritystandards.org/. The Internet also has many other resources related to helping businesses get and stay compliant.

If your business is small and you have limited IT resources, there are independent support services that focus solely on this type of security for retailers and merchants accepting payment cards. The scope of their services includes all of the above requirements and many offer additional services as needed.

Protecting your customers' payment card transactions is a vital part of protecting your business. If you haven't yet instituted all of these security measures, we strongly recommend that you start now.

IDEACOM NETWORK
1-866-IDEACOM
(433-2266)
www.ideacom.org