FOODSERVICE EAST | GUEST COLUMN | AUGUST 15, 2014

SIX TIPS FOR SECURING YOUR CUSTOMER DATA ON YOUR POS

By, Jared Isaacman, CEO, Harbortouch

Jared Isaacman is CEO of Harbortouch, a leading national supplier of POS systems and payment processing services. He founded the company when he was 16 years old in the basement of his parent's home. Isaacman has been recognized as one of "America's Best Entrepreneurs" by BusinessWeek Magazine and "30 Entrepreneurs Under 30" by Inc. Magazine and has also been featured on NBC's Today Show, ABC News and Bloomberg, among other publications and media outlets.

As the foodservice industry continues to grow, there comes an increased risk with the number of data breeches. Most workers are focused on customer service, rather than security, and assume they won't be the target of a data breech. According to a study conducted by the Verizon RISK Team, 74 percent of attacks on retail, accommodation and food service companies target payment card information. Of these, 35 percent are through POS Systems.

How do you go about securing sensitive data? Here are six tips to increase protection of your system:

- Strengthen Security of Customer Information
    - Full credit card numbers should never be stored in plain text. Ensure that your terminal is truncating card numbers and only showing the last four digits on receipts. Additionally, Visa® and MasterCard® regulations prohibit merchants from recording personal information on the sales receipt/draft. This information in conjunction with the account numbers listed on the sales draft could be used to commit fraud. Keep cardholder account and personal information separate and under tight security. It is extremely critical that CVV2 card validation numbers are not written, recorded or stored electronically nor manually under any circumstances. Also, credit card numbers or cardholder account information should never be transmitted via email or unsecured gateways.

- Lock Down Your Remote Access
    - There was an increase in stolen vendor credentials in 2013. One of the biggest problems was the use of the same password for all organizations managed by the vendor. Limit any remote access into POS systems by third-party management vendors to reduce this risk.
- Protect Data Integrity – Make It SSL Secure
    - PCI requires adequate encryption of credit card holder information while being transmitted and at least 128-bit encryption must be used. The primary reason why SSL is used is to keep sensitive information sent across the Internet encrypted so that only the intended recipient can understand it. This is important because the information you send on the Internet is passed from computer to computer to get to the destination server. Any computer in between you and the server can see your credit card numbers, usernames and passwords, and other sensitive information if it is not encrypted with an SSL certificate. When an SSL certificate is used, the information becomes unreadable to everyone except for the server you are sending the information to. This protects it from hackers and identity thieves.
- Pin Protection
    - Although PINs are protected in an encrypted or enciphered form within a transaction message, they must not be retained in transaction journals or logs subsequent to PIN transaction processing.
- Keep Personal Information Separate
    - Do not browse the Web, email, use social media, play games, or do anything other than POS-related activities on POS systems.
- Change Your Password
    - Make absolutely certain that all passwords used for remote access to POS systems are not factory defaults, the names of your POS vendor, dictionary words or otherwise weak. If a third party handles this, require and verify that this is done. Make sure they are not using the same password for other customers.

With data breaches and credit card fraud running rampant, choosing the right POS system for your foodservice operation can significantly improve your productivity and profitability. Making the wrong decision, could cost you and your business. Make sure the system you do select, offers a comprehensive array of security options.