SOLUTION PROVIDERS FOR RETAIL

Two Ways Retail Can Immediately Improve Data

By Jake Weatherly

June 9, 2014

Retailers must be sensitive to customer concerns about security, particularly around their personally identifiable information and financial data. As we discussed on Friday in my post, Ramping Up Your Omnichannel Experience to Maximize ROI, as retailers expand into e-commerce and mobile transactions by forging new partnerships with third-party service providers, precautions must be taken to protect customers' data. According to the 2013 Trustwave report, 63% of data breaches were connected to a third-party. For example, delivery drivers for Lowe's Home Improvement recently learned that their names, addresses, social security numbers, birthdays, and driver's license numbers were exposed by a third-party vendor that monitored driver safety.

To protect consumers, retailers and third-party consultants should do two things immediately.

1. Limit what information they require and only ask for what they need, thereby reducing risk. Customers are reluctant to share sensitive information, especially their social security numbers. A recent survey of college students, a population especially susceptible to cybercrime, revealed that 53% won't give out the last four digits of their social security number to receive a special offer or discount and 88% refuse to disclose their full social security numbers. Therefore, to increase confidence as well as to strengthen the level of security, any information that is collected should be hashed or encrypted to encode and safeguard the data.

2. Be aware of who has remote access to corporate networks and how third-party remote access software is implemented. Nearly half of the companies who suffered breaches in the 2013 Trustwave Global Security Report were infiltrated through remote access or remote desktop services. Weak or stolen passwords are another major cause of data breaches, according to the 2013 Verizon Data Breach Investigations Report. That is why third-party service providers must conform to company password policies by formulating strong passwords and using unique passwords for each of their clients' systems.

3. As cyber criminals become more sophisticated and corporate networks more vulnerable to unintentional or malicious exposure, it is becoming more challenging to protect customers' data and prevent security breaches. To meet customer expectations, retailers must utilize third-party service providers appropriately and ensure that consultants and vendors adhere to security policies. By choosing vendors they can trust, retailers can deliver the omnichannel user experience customers desire – along with security they need.