

Protecting data for PCI compliance

As many retailers make the transition towards PCI DSS compliance, smaller online merchants continue to be a target to hacks. Name, position at THUS plc discusses how next-generation network technologies can enhance security and assesses how the retail industry at large is responding to the new regulatory framework.

Next-generation security

The Payment Card Industry Data Security Standard (PCI DSS) is designed to protect customer's cardholder information that could be used to make a counterfeit card or a fraudulent online transaction. As part of this, any retailer that stores, transmits or processes customer card details must comply with 12 sets of requirements. These range from encryption of cardholder data, to installing access controls, running up to data anti-malware software and performing regular health checks on the IT system.

The deadline for PCI DSS compliancy passed on 30 June 2007 and it is now mandatory for businesses with over 100,000 transactions a year to either be PCI-DSS compliant or be able to demonstrate plans to become so. Compliance with PCI-DSS provides added security layers to stored customer data and, most importantly, it protects a company from the threats resulting from credit and debit card data being wrongly accessed.

However, while larger retailers are toeing the line, issues still remain with smaller online firms. In a recent study by Visa, more than 80 per cent of all hacks involving card data theft are against merchants carrying out less than 20,000 card transactions a year. Furthermore these merchants, usually small online retailers, do not have to provide evidence that they are following the PCI DSS standard. While they are expected to maintain a degree of compliance, they are generally exempt from audits and approved scanning vendor (ASV) scans that many larger retailers are subject to. This can create a target for a potential hacker looking to access customer databases and card details.

Securing data in transition

Today, the Internet is more than a library of information and is increasingly a trade centre where credit card and bank transactions take place every second of each day. Adding to this, private data such as customer details and purchase history is now widely stored online using IT systems. These are supported by network infrastructures which have historically been subject to hackers, potentially leading to serious financial consequences for the retailer and consumer.

PCI DSS compliance is a step in the right direction, encouraging retailers to protect customer data by complying with agreed steps of procedures but for smaller merchants using third party hosted services, security concerns remain.

As the UK's first operator to have rolled-out a next-generation network (NGN), THUS is well aware of the issues faced by large retailers and smaller online merchants as they make the transition towards PCI DSS compliance.

Name, position at THUS is available to discuss the following points:

- How PCI DSS compliance is encouraging retailers, larger or small, to reassess their IT network infrastructures
- How NGNs can ensure all online payment and credit card details are protected using MPLS networks
- How NGNs can support the transition towards PCI DSS compliance by offering high-levels of resiliency and network availability
- How a scalable next-generation network solution, capable of hosting any additional services, can also help deliver additional benefits such as faster processing speeds at peak times and improved customer service

I look forward to hearing from you.

Kind regards,