New card security standards demand retailers to pay full attention

The security that protects in-store card payment data has always been a major concern for retailers.

Identity-theft and data-hacking continue to pose very serious threats, while inadvertent leaking of information through lax implementation can have equally catastrophic consequences.

Now the introduction of new Payment Card Industry Security Standards Council regulations on January 1, 2015 make it imperative that retailers give compliance their full attention, as infringements can result in hefty fines in addition to severe reputational damage.

The changes, known as PCI Version 3, were introduced because of a series of concerns, which included lack of awareness and education among staff about card security, inconsistency in testing and assessments, problems with third-party security compliance, and the use of weak passwords and authentication.

Any organisation taking payments via credit, debit or store cards has had plenty of warning about these new requirements, with a whole year to prepare before implementation. Even so, businesses still have until June 2015 to be fully compliant with some of the subsections of the new rules.

The changes certainly need to be a board-level concern in any retail enterprise because the ultimate responsibility for PCI compliance lies with the CEO, who, depending on the size and seriousness of the data breach, could face a fine or jail. For the business, the penalties can be severe, including loss of its PCI licence, making any further card transactions impossible.

Responsibility

One of the main changes introduced with Version 3 is greater clarity about lines of responsibility. Previously, there were grey areas about whether the retailer or the service provider was responsible for compliance. Although responsibility is shared, if there is a breach and data is compromised, it is the retailer or merchant who will be investigated first, as they have the direct commercial relationship with the card companies.

Given this responsibility, the first step for a retailer is to find out whether their in-store technology is in or out-of-scope of the PCI regulations.

This assessment must also include any third-party service providers who are involved at any point, including those processing the credit card payments. Checking the network in-house is a problem for any business if it does not own every part of it. However, a managed services provider should be capable of conducting a thorough examination to assess PCI compliance, identifying any weaknesses or threats. This is true whether a business is connecting across the Internet or has private connectivity, and is especially relevant where the enterprise is large enough to have premises in many different countries.

Continual assessment

Once a retailer has worked out the devices and connections for which it is responsible, it needs to move on to meeting the new requirements for continual assessment and reporting.

In practice, this means that organisations are expected to conduct their own rolling programme of testing, auditing and reporting on the integrity of their card payment network. The aim is for operators to spot and fix any failures in compliance as they appear, rather than wait for problems to manifest themselves in the annual audit.

It is important, therefore, for a business to have a set of tools which makes reporting easy and compliant.

If the enterprise is using Wi-Fi to enable the use of mobile devices in-store, such as tablets and PIN entry devices, it must have tools that show who has access to the network and whether any wireless rogue devices have been illicitly installed. Criminals interested in identity theft want payment details and PIN numbers and they will use devices to siphon off such information for subsequent decryption. In the case of DSL networks, they will seek to attach counterfeit devices to the end-point.

Business operators often overlook the fact that even if they do not have a wireless network, they should still be checking to see if someone, possibly a staff member, has illicitly installed a rogue device somewhere.

Efficient monitoring

A good reporting tool will not only show the presence of such devices, but also any failed attempts to intercept information in the network. These reports can be run remotely so that once a problem has been identified, the relevant in-house personnel can be alerted, obviating the need to send out consultants to the premises, which can be very costly.

The updated regulations are quite complex and require some reports to be run more regularly than others, which is why enlisting the support of an experienced provider with knowledge of the regulatory detail is a big advantage. It should be borne in mind that once a security problem has occurred, a business needs to demonstrate that it has taken all reasonable steps to prevent breaches of data protocols. However, with expert advice, organisations can maximise compliance by building reporting into their day-to-day working, either manually or through automation.

Contemporary tools facilitate this by allowing reports to be conducted every week or month, as required, and the interfaces are also designed to be user-friendly by avoiding excessive technicalities.

Since broadband data breaches involve tampering or changing end-tools, it is also important to keep an audit of all connections and to log any moves and changes, such as the introduction of new pieces of equipment or the re-routing of connections from one site to another.

It is always worth remembering that the more security tools an organisation has, the more evidence it will have to show regulators that it has taken all reasonable steps to protect payment data, should it suffer a breach.

Separation of data

Version 3 continues to require payment data to be separated from all the other information that the organisation transmits by the same technology. It is a fundamental precondition for PCI compliance that digital layers of encryption and security are installed, which is a task requiring a specialist provider. If broadband is used, the devices already deployed may be able to carry authentication software like IPSec. If more enhanced security is required then separate hardware may have to be installed.

With wireless connectivity, fulfilling compliance standards is much easier if an organisation has a single provider that can cover all aspects of the WAN. However, with broadband, monitoring is more complicated, as the data may flow over a network operated by more than one provider.

Education and emerging technology

Version 3 also stresses the importance of educating staff and partners about payment security, since many breaches occur through poor implementation and weak maintenance regimes, rather than deliberate acts. Education will include greater awareness about changing default passwords, using stronger passwords and changing them when it is believed a data breach may have taken place or have been attempted.

The increasing numbers of retailers using emerging technologies for their data, such as Cloud storage, should be aware that the updated regulations also address potential problems in these areas.

With Cloud connectivity, the servers that store data could be anywhere in the world, which brings a fresh set of challenges to security and PCI compliance. For multi-channel retailers, card data for online purchases is usually already held by the retailer so that customers do not have to register cards on each occasion. If this data is being stored in the Cloud, a retailer must consider where it is and who is monitoring and auditing it so that compliance requirements are met.

Overall, there is reason to be thankful that the updated regulations of Version 3 have brought greater clarity to compliance requirements and have sought to reduce the potential for serious security breaches by building monitoring into everyday working practices.

However, the board of any retail enterprise should be mindful that it can still fall foul of its new regulations if it does not pay full attention to this complex and business-critical area of operations.

Contact us at sales@hugheseurope.com or visit us at europe.hughes.com.

About Hughes

Hughes Network Systems, LLC (Hughes) is the global leader in satellite broadband for home and office, delivering innovative solutions and a comprehensive suite of HughesON™ managed services for enterprises and governments worldwide. HughesNet® is the #1 high-speed satellite Internet service in the marketplace, with offerings to suit every budget. To date, Hughes has shipped more than 5 million systems to customers in over 100 countries, representing approximately 50 percent market share. Its products employ global standards approved by the TIA, ETSI, and ITU organisations, including IPoS/DVB-S2, RSM-A, and GMR-1. Headquartered outside Washington, D.C., in Germantown, Maryland, USA, Hughes operates sales and support offices worldwide, and is a wholly owned subsidiary of EchoStar Corporation (NASDAQ: SATS), a premier global provider of satellite operations and digital TV solutions. For additional information about Hughes, please visit www.hughes.com.

United Kingdom: Hughes Network Systems Ltd
Hughes House
Rockingham Drive, Linford Wood
Milton Keynes, MK14 6PD
United Kingdom

Tel.: +44 (0)1908 425 300
Fax: +44 (0)1908 425 301

HUGHES®
An EchoStar Company

www.hughes.com