

## New payment regulations are a board-level concern

The introduction of the new PCI Security Standards Council regulations on January 1 should have caught the eyes of retail executives.

Version 3.0 of the regulations places the ultimate responsibility for compliance squarely on the retailer's chief executive's shoulders, meaning a serious breach of data security could result in a prison sentence.

Even if the cell doors are not slammed shut, infringements can still result in hefty fines and loss of an enterprise's PCI licence, besides severe reputational damage.

However, help with full compliance is readily at hand, both in the form of technological solutions and the expertise of managed services providers well-schooled in the regulatory requirements of Version 3.0.

One of the stand-out themes of Version 3.0 is responsibility.

Once an official investigation is underway, a board needs to show it has done all it could to meet the regulations. Take, for instance, three areas of Version 3.0 that could be onerous without specialist help.

Firstly, retailers need to establish an inventory of system components within scope of the new regulations. Secondly, they must each have an accurate diagram showing all cardholder data across all systems and networks used for payment data. And thirdly, they must maintain information about who is responsible for compliance in each area—whether it is the retailer or the third-party service provider.

Fulfilling these requirements is no easy matter for a contemporary retailer that may not own its entire network and is quite likely to be using cloud-based services. Multi-channel retailers, for instance, may be storing data for online purchases in the cloud.

Nonetheless, scoping must cover all third-party service providers

involved, including those processing the credit card payments.

However, the requirements of Version 3.0 do not end here. Retailers must also meet the stipulations for continual reporting on the integrity of their organisation's card payment network.

The reporting requirement covers the increasingly important area of Wi-Fi, where store operators often overlook the fact that even if they do not have a wireless network, they are still required to check for rogue devices that have been connected to skim off customer data.

The answer to these challenges is to use specialist providers who can both fulfil the scoping requirements of Version 3.0 and identify and remedy any weak-points and threats. The use of a wireless intrusion prevention system will automatically detect and foil any attempts to breach the network, while sophisticated reporting tools will ensure compliance is constantly monitored.

As part of its security provision, the reporting software can also provide a complete audit of all changes to the network over which payment data is transmitted, along with its connections. In the case of DSL networks, the problem may be counterfeit devices attached to the end-point.

These tools can be managed remotely by a service provider, saving retailers time on training, monitoring and the expense of calling out consultants.

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.

Version 3 has built monitoring of PCI compliance into everyday working practices, and executives must give it their full attention to avoid serious consequences for themselves and their organisation.

Contact us at [sales@hugheseurope.com](mailto:sales@hugheseurope.com) or visit us at [europe.hughes.com](http://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](http://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

©2017 Hughes Network Systems, LLC. HUGHES is a registered trademark of Hughes Network Systems, LLC.  
All information is subject to change. All rights reserved. H58423 APR 17

**HUGHES**  
An EchoStar Company

[www.hughes.com](http://www.hughes.com)