PCI DSS 3.0: what the experts say

The PCI Security Standards Council has published version 3.0 of the PCI Data Security Standard and Payment Application Data Security Standard. Essential Retail gauged the payments industry's reaction.
Published: 14:22:00 on the 14th Nov 2013Author: Ben Sillitoe

Last week saw the PCI Security Standards Council (PCI SSC) publish version 3.0 of the PCI Data Security Standard (PCI DSS) and Payment Application Data Security Standard (PA-DSS) – a move that the organisation makes on a three-year cycle to ensure vendors and merchants are meeting the latest requirements in payments security.

Available now on the PCI SSC website, version 3.0 becomes effective on 1 January 2014, but version 2.0 will remain active until the end of 2014 to ensure adequate time for businesses to make the transition.

Version 3.0 has been introduced with the aim of helping organisations make payment security part of their business-as-usual activities "by introducing more flexibility, and an increased focus on education, awareness and security as a shared responsibility".

Essential Retail has collated the views of a number of industry representatives to see what the PCI standards means for retail and the payments sector.
Bob Russo, general manager at the PCI SSC, commented: "PCI Standards continue to provide a strong framework for payment card security. The core principles at work when we first published PCI DSS are still relevant today. Version 3.0 builds on these to address the feedback we've heard from our community and to help organisations make payment security good business practice – every day, all year round."
Marc White, director, information security & compliance at VeriFone, said: "We welcome the release of PCI DSS v3. It goes some way to strengthen the requirements that were already in place and is in line with what VeriFone has adopted within our business for several years.
"Compliance is not an annual event, a once-a-year tick in the box, it is an on-going process that requires security to be built in at the outset, from the foundations upwards, instilling strong business as usual process to ensure that compliance is maintained 24/7/365. After all, compliance does not equal security."

Ross Brewer, vice president and managing director for international markets at LogRhythm, remarked: "Following a number of recent high profile data breaches, it couldn't be a better time for the latest iteration of PCI to rear its head. There's no doubt that cyber attacks are continuing to grow in sophistication and pose a very real, very serious threat to all businesses, not just those processing cardholder information.
"As a result, it's become crucial that issues such as weak passwords, lack of authentication processes and inconsistent assessments are addressed – and regulated – to reflect this. That said, a lack of awareness and inadequate training on standards such as PCI is simply no longer acceptable."

Robert Crutchington, director of Encoded, commented: "Version 3.0 aims to make data and payment security part of everyday business processes. Merchants are often at the forefront of innovation when it comes to advances in payment technology but they are also the ones fined if breaches in security happen. These latest revisions go some way to closing any gaps that may have appeared in recent years between PCI compliance and the reality of card data security.
"Previous iterations of the standards have been very prescriptive with instructions as to what to do to meet requirements, which meant the process was very restrictive. ISO security standards, on the other hand, allow merchants to take the best practice route. Version 3 appears to give more detailed explanation on how to achieve the necessary requirements which has to be a good thing."

Tom O'Kill, marketing and operations director at Us (Unique-Secure), said: "One change in particular that we welcomed, was something we have been championing for some time now – the heightened need to protect payment devices from tampering and substitution.
"So we strongly welcome and embrace Requirement 9.9. Only best practice until it becomes a requirement in June 2015, we believe it couldn't come soon enough for the public.

"As an industry, we of course need to continue to make it increasingly difficult to attack PEDs physically and electronically. Consumers don't see the extent of the electronic protection, but by making the physical security visible (whilst still being sympathetic to the store environment of course), this is something tangible they can see and relate to. As they can see the lengths being gone to, this in turn allows us to build more trust with consumers, improving their experience in-store.

"At the end of the day, the consumer is the most important party, and the changes in v3 keep pace with the security requirements needed to continue to protect them from data fraud. Therefore this must be a good thing for all of us."

Mark McMurtrie, director of the Payments Consultancy, added: "The PCI standards are being updated on a regular basis in order to stay one step ahead of the fraudster. The payments industry can't stand still – data security protection levels need to continually be enhanced in order to safeguard the business, protect brand reputation and look after the interests of customers.

"Retailers used to view PCI as a one-time task driven by the IT department, but in reality it needs to be treated as an organisation-wide project as it encompasses people, processes and products. Compliance has to become part of standard operational procedures, rather than simply satisfying bank compliance demands. It's not a one-time tick-box exercise, it's an on-going journey.

"The impact will be that retailers will have to strengthen security protection in order to become compliant with the latest version of standards. This will require investment in product enhancements, procedures will need to be improved, more staff education is required and resources will have to be allocated. It's not something that can be avoided and will be expensive – but in reality it is about following best security practice and as such just needs to be planned and managed efficiently.

"Data security is a shared responsibility – the PCI Council has articulated as much. This is how it should be viewed, rather than a necessary job imposed on them by the banking community. There's nothing that PCI covers that doesn't make logical sense; it's all about looking after their brand and their customers, so which retailer wouldn't want to do that?