



PCI DSS compliance: a difficult but necessary journey

By Andre Muscat

The need to comply with the Payment Card Industry Data Security Standard (PCI DSS) has been a rude wake up call for thousands of companies who believed their networks are secure and safe from security breaches.

This standard is a set of network security requirements agreed upon by five of the major credit card companies in an attempt to stem the growth of credit card fraud around the world and to give a common interpretation of what security is all about. Since PCI DSS was launched, it has helped to expose serious security shortcomings, companies' failure to follow security best practice and a general lack of awareness of the security threats facing organizations today.

The statistics reveal a worrying increase in the level of identity theft and credit card fraud. According to a Federal Trade Commission report in January 2007, 25% of reported identity theft in 2006 was credit card fraud. Considering that more than \$49 billion was lost by financial institutions and businesses in that year due to identity theft, and \$5 billion lost by individuals, credit card fraud is digging deep into everyone's pockets. E-commerce fraud is also on the rise, reaching \$3 billion in 2006, an increase of 7% over 2005.

A growing sense of urgency to meet these requirements was spurred by TJX Companies Inc.'s loss of 45.7 million records containing customer personal account information as well as 455,000 merchant details over an 18-month period. Although the TJX breach is considered to be the biggest in US history it is not the only one. According to the Privacy Rights Clearinghouse, between 1 January 2005 and August 2007, more than 159 million records containing sensitive personal information have been involved in security breaches. The actual figure is probably higher because many cases are either under-detected or they are not reported at all.

Large retailers like TJX are not the only organizations being targeted. Public attention may be focused on high-profile data losses, but experts studying financial fraud say hackers are increasingly targeting small, commercial websites as well! In some cases, criminals were able to gain real-time access to the websites' transaction information, allowing

them to steal valid credit card numbers and use them for fraudulent purchases. Although small businesses offer fewer total victims, they often present a softer target; either due to flaws in the e-commerce infrastructure being used, or due to over-reliance on outsourced website security or simply due to the false belief that their existing security set-up is adequate.

Knee-jerk reaction?

The PCI DSS is not the result of a knee-jerk reaction to an increase in security breaches but it is a studied approach to data security

taken by each of the card companies. Before 2004, American Express, Discover Financial Services, JCB, MasterCard Worldwide, and Visa International had a proprietary set of information security requirements which were often burdensome and repetitive for participants in multiple brand networks.

Seeing the need for greater cohesion and standardization, these associations created a uniform set of information security requirements that became known as the PCI Data Security Standard (PCI DSS), governing all the payment channels: retail, mail orders, telephone orders and e-commerce.

THE PCI DSS IS NOT THE RESULT OF A KNEE-JERK REACTION TO AN INCREASE IN SECURITY BREACHES BUT IT IS A STUDIED APPROACH TO DATA SECURITY

Deadlines looming

For more than two years, credit card companies have been encouraging retailers to comply with the strict set of 12 requirements that are aimed at securing cardholder data that is processed or stored by them. Unfortunately, with two deadlines looming – 30 September and 31 December 2007 for Level 1 and Level 2 US merchants – it seems that many companies will not be ready in time. Even with a last minute push, it is highly improbable that retailers – large or small – have the time or the resources to become compliant in such a short-time frame. Most companies, especially in the SMB market, want to become compliant but they are still struggling to introduce basic security practices let alone implement all the systems needed to become compliant. The most recent compliance statistics from Visa for the month of July indicate an improvement but they are far off the targets that Visa and the other card companies hoped for.

According to figures for July, 40% of Level 1 retailers were compliant, up from the 35% compliance rate in May 2007. With the somewhat smaller Level 2 retailers, the July figures showed a 33% compliance rate – up from 26% in May – and the smaller Level 3 retailers showed 52% compliance, just slightly up from the 51% that Visa reported for that group in the same month. Visa did not release fig-

ures for Level 4 retailers; however it said compliance remained low.

Such a low compliance rate – after more than two years of preaching by the credit card companies – is possibly due to three reasons. First, some companies have taken a very laid-back approach to the issue, realizing only recently that the credit card companies mean business. Now, they are rushing to comply by the deadline, suddenly aware that they have a massive task ahead of them. Second, many small and medium sized companies do not have the resources or the finances to invest in the more personnel or a technology solution to meet the PCI requirements. Third, some retailers have complained that the standard does not distinguish between retailers on the basis of their size

According to the Retail Industry Leaders Association (RILA): "Some PCI requirements are vague. Some are unattainable. Retail companies [...] cited numerous examples of low-result PCI requirements, one-size-fits-all rules that don't work for various kinds of retail formats."

RILA has argued that although there is universal support for the goals and objectives of PCI and its efforts at making payment systems more secure, the standard's 'one size fits all' framework is imposing unrealistic

THE PCI STANDARD IS NOT ROCKET SCIENCE

hardships on smaller retailers and it does not “appreciate the practical staffing flexibility that retailers need”.

While some of the PCI requirements may be open to interpretation, it is also true that the PCI DSS standard is one of the most robust and clear when compared to other compliance regulations such as Sarbanes-Oxley. PCI is not only the least ambiguous of the lot but it is also the only standard that has gained universal approval.

What is the PCI standard?

The PCI standard is not rocket science and neither does it introduce any new, alien concepts which systems administrators should adopt; on the contrary it is an enforcement of practices that should already be in force on all

corporate networks. Although PCI DSS was developed with the protection of cardholder data in mind, more than 98% of the requirements apply to any company that needs to secure its network and its data.

In essence, PCI DSS comprises 12 distinction standards that are designed to 1) Build and maintain a secure network, 2) Protect (cardholder) data in transit or at rest, 3) Maintain a vulnerability management program, 4) Implement strong access control measures, 5) Regularly monitor and test your IT infrastructure and finally, 6) Maintain an information security policy.

The table below shows a breakdown of each category and what companies need to do to become compliant.

The PCI DSS requirements

Often referred to as the ‘digital dozen’, these define the need to:

Build and maintain a secure network

- 1: Install and maintain a firewall configuration to protect cardholder data
- 2: Do not use vendor-supplied defaults for system passwords and other security parameters

Protect cardholder data

- 3: Protect stored cardholder data
- 4: Encrypt transmission of cardholder data across open, public networks

Maintain a vulnerability management program

- 5: Use and regularly update anti-virus software or programs
- 6: Develop and maintain secure systems and applications

Implement strong access control measures

- 7: Restrict access to cardholder data by business need-to-know
- 8: Assign a unique ID to each person with computer access
- 9: Restrict physical access to cardholder data

Regularly monitor and test networks

- 10: Track and monitor all access to network resources and cardholder data
- 11: Regularly test security systems and processes

Maintain an information security policy

- 12: Maintain a policy that addresses information security for employees and contractors

There are three stages that each and every merchant or provider must go through to become compliant.

First, they are required to secure the collection of all log data and ensure that it is in tamper-proof storage and easily available for analysis. Second, companies must be in a position to prove they are compliant on the spot if they are audited and asked to present evidence that controls are in place for protecting data. Third, they must have systems in place, such as auto-alerting, which help administrators to constantly monitor access and usage of data. These systems must enable administrators to receive immediate warnings of problems and be in a position to rapidly address them. These systems should also extend to the log data itself – there must be proof that log data is being collected and stored.

The requirements make a clear distinction between merchants and service providers and what they need to do to become compliant. All merchants that acquire payment card transactions are categorized in 4 levels, determined by their number of annual transactions:

- Level 1: Merchants with more than 6 million card transactions & merchants which cardholder data has been compromised
- Level 2: Merchants with card transactions between 1 and 6 million
- Level 3: Merchants with card transaction between 20,000 and 1 million
- Level 4: All other merchants.

These levels determine the validation processes that a merchant must undertake in order to achieve and maintain compliance. For example, Level 1 merchants must carry out an annual on site security audit and quarterly network scan. On site security audits are performed by a Qualified Security Assessor (QSA). On the other hand, level 2, 3, 4 merchants must fill in an annual self assessment questionnaire and carry out a quarterly network scan. The self assessment questionnaires are compiled in-house by the merchant while the network scans are performed by an approved scan vendor (ASV). Examples of merchants include online traders such as Amazon.com, Wal-Mart retail outlets, universi-

ties, hospitals, hotels, restaurants, petrol stations and so on.

Services providers, which include payment gateways, e-commerce host providers, credit reporting agencies and paper shred companies, are categorized in three levels:

- Level 1: All payment processors and payment gateways
- Level 2: All service providers not in level 1 but with more than 1 million credit card accounts or transactions
- Level 3: Service providers not in Level 1, with fewer than 1 million annual credit card accounts or transactions.

Becoming PCI DSS compliant requires these businesses to fulfill and demonstrate compliance with all the 12 requirements as follows: Level 1 & 2 service providers must pass an annual on site security audit and quarterly network scan, while Level 3 service providers need to fulfill an annual self assessment questionnaire & quarterly network scan. Self assessment questionnaires are compiled in-house by the service provider and network scans need to be performed by an approved scan vendor (ASV).

It is also in the own interest of acquiring banks to ensure their merchants are aware and compliant to PCI DSS. Acquiring banks are the main actors that build up the line of trust between card companies and merchants and they are also the ones that end up directly in the line of fire of credit/debit card companies whenever one or more of their merchants suffer a breach. To maintain a successful and healthy business relationship with card companies, acquiring banks must ensure that their merchants are adequately protected – by being PCI DSS compliant. Similarly, merchants and service providers are expected to demonstrate their level of compliance to PCI DSS. This helps to maintain a healthy business relationship with acquiring banks and to avert non-compliance liabilities.

Although acquirers are not currently mandated to carry out any specific PCI DSS validation or certification process, they are still required to be PCI DSS compliant.

The cost of non-compliance

Level 1 merchants have until 30 September 2007 and level 2 merchants have until 31 December to become compliant otherwise they risk hefty fines, possible law suits and loss of business and credibility. The consequences can be serious because apart from card companies imposing fines on member banking institutions, acquiring banks may in turn contractually oblige merchants to indemnify and reimburse them for such fines. Fines could go up to \$500,000 per incident if data is compromised and merchants are found to be non-compliant. In a worst case scenario, merchants could also risk losing the ability to process customers' credit card transactions.

Furthermore, businesses from which cardholder data has been compromised are obliged to notify legal authorities and are expected to offer free credit-protection services to those potentially affected. It is also important to note that if a merchant in level 2, 3 or 4 suffers a breach, he will then have to fulfill the requirements for PCI DSS compliancy as if it were a level 1 merchant.

Lesson to be learnt

Achieving compliance to the PCI Data Security Standard should be high on the agenda of organizations that carry out business transactions involving the use of credit cards. Organi-

zations cannot continue to give so little importance to security nor adopt the macho attitude, 'it can't happen to me'. This is exactly what hackers and fraudsters want to hear. Implementing software tools for log management, vulnerability management, security scanning and endpoint security will go a long way towards helping you achieve compliance. However, the story does not end there. Just because a merchant receives a PCI stamp of approval, he simply cannot sit back and relax.

PCI compliance is but the beginning of a continuous process that requires regular monitoring of the security health status of the merchant's network. PCI DSS is not a one-off certification that stops with the Qualified Security Assessor (QSA) confirming you are compliant, as some merchants may think. Becoming PCI compliant means that you have reached an acceptable level of security on your network but it does not mean that from then onwards your network is secure and cannot be breached. Maintaining PCI DSS compliancy status is just as, if not more, important.

PCI DSS compliance is a long-term journey, not a destination. And this is something that all merchants need to understand irrespective of size or business. It is a cost of doing business, granted. Yet, the cost of compliance is a lot lower than having to pay \$500,000 in fines and losing your goodwill and credibility if your network is breached!

Andre Muscat is Director of Engineering at GFI Software – www.gfi.com

