White Paper

Mako Networks

PCI and Partnerships

Exploring a collaborative approach and solution for vendor's addressing PCI issues faced by small to medium merchants.

Mako NETWORKS

Executive Summary

The myriad of outsourced services and vendors available can be daunting to any company that is required to comply with the Payment Card Industry Data Security Standard (PCI DSS).

All companies throughout the payment chain that process, store or transmit cardholder data must comply with the PCI DSS, but the fragmented approach to managing various vendors and a lack of understanding of PCI compliance is leaving many businesses vulnerable to the risk of data breaches and other consequences of non-compliance. Customers throughout the payment chain can't just outsource to one vendor to solve the compliance problem, but must instead employ, co-ordinate and monitor several.

An initiative of PCI compliance which brings together a partnership of payment technology vendors would make compliance more straightforward.

There is no doubt that if technology vendors worked more closely together PCI would become easier to implement for merchants, acquirers and issuers. In fact, a joint approach would go a long way in ensuring that the loop of compliance is closed while at the same time minimising the risk of exposure through non-compliant third parties.

PCI and Partnerships

ISSUES WITH COMPLIANCE

A recent report on PCI compliance by Verizon (2011), found that at the time of its Initial Report on Compliance (IROC), only 21% of organisations were found fully compliant.[1]

Other reports suggest that many merchants, especially Small and Medium Enterprise (SME) merchants, are turning a blind eye to data security, believing that security breaches are only a risk for larger retailers and they are at little risk of becoming a fraud target. Others simply pay non-compliance fines and carry on. It is data security breaches at the bigger retailers that hit the headlines, but smaller retailers are increasingly targeted too.

Larger retailers are becomming compliant, therefore criminals are resorting to smaller, more vulnerable retailers.

Many of the larger retailers have now put measures in place to ensure compliance, and so criminals are increasingly turning to smaller retailers because they know that security provisions are often easier to penetrate.

According to a recent report by Trustwave (2011), around 90 percent of incidents in which card data is compromised occur in Level 4 merchant environments.[2]

PCI DSS compliance can be an arduous process for smaller retailers. However, the data risks faced by a retailer in keeping card data secure throughout the transaction process are complicated, and compliance has to mitigate risk wherever possible to prevent data

1 *Verizon Payment Card Industry Compliance Report, 2011. Available at: http://www.verizonbusiness.com/resources/reports/rp_2011-payment-card-industry-compliance-report_en_xg.pdf accessed 18/06/2012*

2 *Trustwave Payment Card Trends and Risks for Small Merchants, 2011. Available at: https://www.trustwave.com/wp/payment-card-report/ accessed 18/06/2012*

breach situations. Just because compliance is seen as difficult it cannot be ignored.

Craig Bottomley, Head of Product Management at Spire Payments comments, "Interpretation of the PCI requirements can be a complex issue and we're often asked whether the payment application in the terminal has to be PCI DSS-certified. While we take the view that there can be no discussion or compromise when it comes to security, some businesses don't believe certification is necessary."

For SME merchants, implementing compliance measures is a daunting task, with limited budgets making it even more difficult.

For SME merchants, implementing compliance measures is a daunting task, with limited budgets making it even more difficult. Outsourcing services such as payment processing is becoming an increasingly popular way for smaller merchants to reach compliance. Outsourcing can reduce the scope of PCI DSS requirements applicable to a business, and make compliance more manageable.

However, there are issues with outsourcing. Any vendors that merchants partner with can also potentially pose a risk to compliance. If the merchant/vendor relationship is not properly managed in regards to compliance, there is a possibility that customer data could unwittingly be left exposed. If a breach does take place as a result, the consumer of the service (the merchant) may be responsible for the consequences. Having identified the vulnerability of the merchant/vendor relationship within the industry, it is therefore time for PCI payments technology vendors to take responsibility for this issue and come together to provide a joint approach that is easy to use, cost-effective and honest about dealing with the issues of compliance.

By increasing the understanding of PCI compliance within the vendor space, and through sharing their joint expertise, a forward-thinking and dynamic approach to PCI would become a reality, greatly reducing the difficulty and confusion in the market for merchants.

THE EVOLUTION OF PCI STANDARDS

The PCI compliance standard was first launched in 2004 to help retailers combat card fraud.

Developed by the five major credit card companies (Visa, MasterCard, American Express, Discover and JCB), the standard is a global set of security obligations which companies that handle cardholder information for the major credit, debit, prepaid, ATM, POS and e-purse cards must meet. The PCI DSS applies to all businesses that store, process or transmit cardholder data, including merchants and service providers.

PCI DSS version 2.0 was released on 26 October 2010 and is the most current version of the standard. As of 1 January 2011, all organisations that accept or process payments were required to have adopted the standard. Since the 1st January 2012, all annual assessments must now also be carried out against version 2.0 of the standard (PCI SCC, 2011).[3]

3 *PCI SSC [Press Release], 2011, PCI Security Standards Council Enters Next Phase Of Data Security Standards Development, January, 2011. Available at: https://www.pcisecuritystandards.org/pdfs/pr_110105_jan1_effective_date.pdf accessed 18/06/2012*

SIMPLIFYING PCI

Modern forms of communication such as broadband Internet benefit SME merchants by reducing costs and speeding up payment processing, but these need to be compliant and by their nature are technically more complex than legacy dial-up lines. For example, a merchant using dial-up who does not hold card data currently needs to accurately attest to 27 questions during PCI DSS auditing, and thereafter continue to meet those obligations for as long as they accept credit cards. This inflates to more than 100 questions, many technical in nature, when the same merchant moves from dial-up to an IP environment such as broadband. This raises a number of challenges and dissuades merchants from making the transition, missing an opportunity to improve the purchasing experience and reduce costs within their business.

The current Self Assessment Questionnaire (SAQ) audit process for SME merchants also contributes to the challenges they face by fostering a 'check box' approach to PCI compliance, often without accurate knowledge as to what is being attested. The industry has attempted to address this by creating online compliance portals where merchants can attest electronically rather than by completing paper-based SAQ forms. Unfortunately, and in most cases, this does not prevent the merchant from again attesting that they are complaint, when in fact no rigorous procedures or processes actually exist to ascertain the veracity of their compliance status. Even when supported by a remote scan of the merchant's systems, this only validates the compliance of a merchant's systems at a specific point in time, rather than continually throughout the year.

The appropriate approach is to provide the merchant with an intelligent portal which can obtain accurate information from certified vendors and automatically populate the SAQ on behalf of the merchant. Furthermore, the information should be shared in a compliant manner with trusted parties such as acquiring banks who have an obligation to manage and report risk.

James Lewis, Strategic Projects Director at Payzone, explains that its customers, predominantly Level 4 SMEs, struggle with understanding compliance in relation to their POS terminals: "SME merchants often fail to understand why an IP connected, PCI compliant, third party supplied POS terminal requires a more complex questionnaire and self-certification process than an identical terminal connected via PSTN.

Merchants expect their acquirer to provide advice but are often surprised to learn the acquirer is reluctant to become involved; referring the merchant, instead, to a third party Qualified Security Assessor.

Merchants expect their acquirer to provide advice but are often surprised to learn the acquirer is reluctant to become involved; referring the merchant, instead, to a third-party Qualified Security Assessor."

Lewis continues, "Many SME merchants also accept offers of help 'at very reasonable prices' from an unqualified, unethical independent service provider who is out to make a quick buck in a confused and paranoid market. Merchants are the ones at risk when they rely on this help and the clock is ticking for attitudes to change. Operators and vendors in the payments industry need to collaborate to provide services which assist merchants with compliance."

THE IMPACT OF PCI ON VENDOR RELATIONS

The PCI standard adds an extra layer of complexity to vendor relations for many organisations, however its importance should not be ignored.

The PCI DSS forms a clear business opportunity for many vendors to provide value-added services for merchants. The offering on the market for "compliant" partners is massive, and undoubtedly causes confusion over what partners can actually offer. If a retailer makes the wrong decision, the compliance consequences can be significant.

Any business considering a partnership with a service provider or vendor where that partner has access to data covered under the PCI standard should ensure that the vendor understands its responsibilities. Despite the PCI standard requiring that all businesses ensure their partners are compliant, this rarely actually happens.

Businesses consuming services from vendors that handle cardholder data protected by regulation often take for granted that partners have the proper controls in place. An initial PCI audit should assess whether the retailer has clearly defined its expectations of third parties, including taking into account any procedures that it has now been asked to follow.

Merely asking a vendor whether it complies with a set of requirements is generally seen as inadequate. It's possible the vendor will answer "yes" regardless of its actual intentions, understanding or capabilities. Businesses must ask if their vendors fully understand their responsibilities before entering into any partnership.

The merchant will likely be responsible for consequences should a data breach take place, including both financial and reputational damages.

The merchant will likely be responsible for consequences should a data breach take place, including both financial and reputational damages. A well-managed partnership needs to set up clear boundaries of responsibility, which are fully understood by both parties. The compliance of third parties should also be constantly monitored. Although service providers and vendors can't be forced into compliance, the merchant can assess whether the compliance program and security controls will meet its requirements. Exactly how merchants go about this assessment process is something that requires more industry attention, as there is currently no universally agreed best practice advice.

GROWING EXPECTATIONS FOR MERCHANTS – 2012 AND BEYOND

The main development to the PCI DSS Standards audit in 2012 is the introduction of data discovery, (Dataguise, 2011).[4]

While most organisations understand where sensitive data should reside, due to interrelationships of business processes and dynamic data usage, data tends to 'leak' and reside in systems, applications, databases and file shares that do not adequately protect information.

Locating and protecting data is a core part of PCI compliance and data discovery enables retailers to easily do this.

There have been many examples where organisations thought information was secure, but after following data discovery procedures found that sensitive data had in fact 'leaked' into insecure environments.

4 *Key Steps to Meeting PCI DSS 2.0 Requirements Using Sensitive Data Discovery and Masking, Dataguise [Online] , 2011. Available at: http://dataguise.com/pdf/Dataguise_PCI-DSS_Brief.pdf accessed 18/06/2012*

Third party compliance is also becoming an increasingly important aspect of the standard, and the council is encouraging retailers to take responsibility for the security of data throughout the transaction process.

In addition to data discovery for PCI DSS, the introduction of the European Data Protection Regulation will also heavily impact merchants. Mathieu Gorge, CEO at Vigitrust comments, "The supplier/partner relationship is notoriously complex when it comes to security protocols and with the European Data Protection Regulation set to supersede the current Data Protection Directive, this will add further pressure. Under the new Regulation, suppliers will be held responsible, just as their customers are, for breaches they cause."

Under the new Regulation suppliers will be held responsible, just as their customers are, for breaches they cause.

Gorge continues, "Currently requirement 12.8 of the PCI DSS states that if cardholder data is shared with service providers, businesses should maintain and implement policies and procedures to manage them. This puts the onus on the business using the service to ensure that their suppliers are not putting them at risk of non-compliance. In the future, collaboration between expert third-party suppliers and merchants is necessary to ensure all parties meet the requirements and remain complaint."

THE EMERGENCE OF PCI SPECIALISTS

Outsourcing payment services means retailers no longer have to worry about the risks associated with both taking payment and handling customer data. However, this is leading to retailers looking for advice on trusted companies to work with. Currently, the sources merchants turn to for advice in regards to the PCI DSS, such as Qualified Security Assessors (QSAs), acquirers and Payment Service Providers (PSPs). However, these sources may not be able to provide merchants with the entirety of the information needed, especially with regards to solution providers and a pool of certified partners to work with.

Since the inception of the PCI DSS, a number of providers have emerged to help retailers with compliance. The complexity of the PCI standard means that there are many aspects which require specialist knowledge. As the acceptance that compliance with the PCI standard is a necessity has infiltrated many sectors, products and services claiming to "meet PCI DSS" have become increasingly common offerings from various providers.

However, just because a provider claims a product or service meets the demands of the PCI standard doesn't automatically mean that it has been officially accredited. While it's not essential that a service provider be accredited to ensure its product or service meets the standard, official accreditation requires significant dedication, investment and auditing. PCI-certified vendors can give better reassurance that merchants are not putting their business at risk through a partnership.

Gorge adds, "Suppliers that reduce the scope of PCI DSS are incredibly valuable to businesses that struggle with compliance; however this often only works on a technical level. Businesses and service providers still need to validate their compliance, train users and have policies and procedures in place to support ongoing compliance. Again these are all attributes the new EU regulation will insist upon."

To deal with the growing threat of data theft and to simplify compliance, specialists are partnering to provide an easy-to-use, complete and cost-effective service. The value of this is particularly important for retailers that are looking to grow, expand and keep ahead of new technologies.

PCI MYTHS

Myth One – Retailers can achieve compliance using one vendor or product.

There are many suppliers that offer services and software that claim to ensure PCI compliance, however, none of these actually cover all 12 requirements of the PCI DSS. Unfortunately, the marketing around these solutions can often mislead retailers to think that one supplier can solve all of their PCI requirements, when they may only narrowly apply to one particular aspect.

In order to fully comply, retailers must take into account all 12 PCI DSS compliance criteria rather than focusing on one.

In order to fully comply, retailers must take into account all 12 PCI DSS compliance criteria rather than focusing on one.

For smaller retailers, this adds to the complexity. In most cases, smaller retailers do not have the resources to adequately deal with PCI compliance themselves, but they also do not have the budget to employ several different outsourced providers to deal with all the different aspects of PCI compliance.

There is a solution, as providers are coming to realise the needs of SMEs and many are forming partnerships to provide complete and cost effective PCI compliance solutions.

Myth Two – Outsourcing card processing makes the retailer compliant.

Outsourcing can simplify the payment card processing, however it doesn't provide automatic compliance.

Whilst outsourcing simplifies payment card processing it does not provide automatic compliance. Policies and procedures for cardholder transactions and data processing must be assessed. The retailer must protect cardholder data when it is received, and when processing chargebacks and refunds.

Myth Three – Compliance is an IT project.

PCI compliance is an ongoing process of assessment and there should be awareness of it throughout the business, not just in the IT department. IT may implement some of the technical requirements, but the business should have a multi-disciplinary team either within the business or outsourced to advise on complete compliance. Indeed, some procedural aspects of compliance involve policies and staff training – areas traditionally outside the purview of IT.

Myth Four – PCI is overly complicated.

PCI is complicated, but that is because the multiple threats to data security are complicated and these standards are designed to provide a high level of protection to cardholders and retailers. The risks are constantly evolving as criminals become more sophisticated in their techniques. Therefore, employing service providers with a good data security background will make compliance easier to adhere to and should also make merchants less vulnerable to ever-changing risks.

Jeremy King, European Director of the PCI Security Standards Council, comments "The PCI DSS is a fantastic foundation for establishing a core group of best practices that can serve as the foundation for [a merchant's] security efforts (King, J, 2012)."[5]

5 *King, J, 2012 , Comment: Make PCI DSS Part of Your Security Strategy, Info Security [Online]. Available at:http://www.infosecurity-magazine.com/view/23614/comment-make-pci-dss-part-of-your-security-strategy, accessed on 18/06/2012*

Myth Five – Retailers that process few credit card payments don't need to be compliant.

Any business that accepts payment using credit cards (no matter how small the quantity) must be PCI compliant.

The Hidden Risks

THE OPPORTUNITY FOR THREAT AND IDENTIFYING VULNERABILITIES

Data security thieves are targeting cardholder data, most specifically the Primary Account Number (PAN), along with sensitive authentication data. With these, a thief can readily clone a duplicate card and impersonate the cardholder. Even if cardholder data is protected, thieves will steal any other data that they perceive to have value, including employee information such as National Insurance numbers, birthdates and addresses.

Thieves can obtain this information through:

- A compromised card reader
- Hard copies of data stored in a filing cabinet
- Data in a payment system database
- Hidden cameras recording entry of authentication data
- Accessing a store's wireless or wired network

The PCI DSS is designed to combat all these aspects, covering security of physical environments as well as virtual.

EXPOSING DATA TO NONCERTIFIED PARTNERS

Exposing data to noncertified partners can lead to accidental data leaks, creating opportunities for fraudulent activity to take place.

Leaks can often go undiscovered, which is why data discovery is such an important development for the PCI standard.

All elements of the chain need to be compliant and need to be integrated correctly to form an end-to-end PCI-compliant solution.

Tim Bell, Director of Phoenix Managed Networks comments, "Just because a POS terminal or system is PA DSS/PTS compliant, it doesn't make the merchant PCI compliant. All elements of the chain need to be compliant and need to be integrated correctly to form an end-to-end PCI-compliant solution. PCI DSS is a process and not a project. Accreditation is merely a snapshot at the time of certification and maintenance is the key to ongoing compliance. Once achieved all PCI DSS measures need to be constantly monitored and managed, including those involving any partners or suppliers as this is where businesses often unknowingly put themselves at risk of non-compliance."

QUANTIFYING THE POTENTIAL DAMAGE – COST AND LOSSES

Many retailers remain ambivalent about PCI compliance without considering the full repercussions of a data breach.

While card data theft is falling in some geographies, it is still alarmingly high.

According to the PCI Security Standards Council, in 2010 there was more than 417.5 million EUR in UK card fraud – well over 1 million EUR per day (King, J, 2011).[6]

Under Visa's current enforcement scheme, a non-compliant customer could expect to be fined a one-off penalty of at least £10,000. Continued non-compliance is likely to give rise to monthly fines of approximately £5,000-£15,000. Card schemes can also charge for the cost of investigations, the cost of data restoration and other fees.

According to Visa, the average cost of a card number data breach is £7.4 million (Fiorani, 2008).[7]

Following the discovery of non-compliance, ongoing penalties can be levied against the retailer by the card scheme. In some cases, the card schemes can even refuse to accept payments from the non-compliant merchant altogether. No matter the size of the merchant, they will also be penalised by being immediately reclassified as a Level 1 merchant, equivalent to a major supermarket. This means the merchant will have to undergo the same extensive auditing procedures as all Level 1 merchants, adding both cost and time pressures.

SECURING THE PAYMENT ENVIRONMENT

The PCI DSS consists of 12 requirements which make up a framework for a secure payment environment.

No matter the size or speciality of the retailer the initial process to go through in securing data and achieving compliance should be as follows:

- **Assess**
- **Remediate**
- **Report**

A full assessment should be carried out which records a full inventory of all the IT assets and business procedures for payment card processing. The results should then be analysed and vulnerabilities that could be expose cardholder data should be identified.

Then, the remediation process should fix the identified vulnerabilities.

Finally, the reporting stage is the process of compiling records required by the PCI DSS to validate the remediation. These reports should then be submitted to the acquiring bank and card payment brands that the retailer does business with.

---

6 *King, J, 2011, 2011 is Proving that PCI DSS is working; however there are challenges to be overcome. Available at: http://www.thedata-chain.com/articles/2011/10/2011_is_proving_that_pci_dss_is_working_however_there_are_challenges_to_be_overcome accessed on 19/06/2012*

7 *Visa Europe, 2008, title of article, Info Security [Online] Available at: http://www.infosecurity-magazine.com/view/1112/pcidss-failure-could-hit-brands-gaming-firms-told/ accessed on 19/06/2012*

To emphasise: this should be considered a continuous monitoring process.

The first two steps of the PCI DSS requirements are specifically around building and maintaining a secure network. These are to set up and maintain a firewall to protect cardholder data, and to ensure that vendor-supplied defaults for system passwords and other security parameters are not used.

Securing the hardware used in the payment chain should also be an essential consideration for all businesses when looking to ensure PCI compliance.

Ian Dodd, Director at Service Logistics explains "Many POS devices claim to be fully PCI compliant and while this may be true for the devices once they're connected to a network, very few suppliers actually consider security during transport. This exposes the device to the possibility of being intercepted by a fraudster for criminal use and is a major security issue.

Tracking the location of the device to ensure it reaches its intended destination and is only connected to an approved network is one method of mitigating risk. Having the ability to control the device remotely, for example to turn it on and off, is also important to stop potential skimming attacks. We believe that partnerships between different technology suppliers across the industry are the best way to create a distribution chain which secures the POS device from delivery to use and assists with the enforcement of compliance for merchants from a hardware perspective."

A Collaborative Approach

CLOSING THE PCI LOOP (TOGETHER)

Organisations that take PCI compliance seriously have an upward struggle, not only in understanding what they need to do to comply, but also in monitoring the services that they outsource to. With a lack of available time and resource to put correct assessment procedures in place, it can be difficult for retailers to ensure vendor services are not leaving them vulnerable.

With many vendor propositions making claims about PCI compliance, the truth surrounding security and risk for merchants is made even murkier.

With many vendor propositions making claims about PCI compliance, the truth surrounding security and risk for merchants is made even murkier.

There is also a great deal of cost and time associated with using the services of several vendors. To ensure the vendor service is not a threat to compliance it must be continually assessed and managed over its lifetime.

Alan Stephenson-Brown, Director of Phoenix Managed Networks, comments, "Vendors in competing sectors have historically worked and developed solutions in isolation without fully understanding the implications of what they are providing or supporting, and the payments industry has been particularly guilty of this. As new requirements and especially around security and PCI have to be implemented, no one organisation has the full capability to deliver a complete end-to-end solution. Collaborating and sharing ideas will benefit the industry and support merchants to take on board the PCI requirements."

If PCI technology vendors were to come together to close the PCI 'loop', not only would the security provision offered be better it, would also be easier to manage.

Best Practice Guide

WHAT IS MEANT BY PCI BEST PRACTICE?

Best practice for any business refers to the optimal mode of functioning that enables the business to operate as efficiently and successfully as possible, in line with business objectives and expectations. For any business to which PCI compliance applies, best practice refers to the way in which procedures and practices are implemented to ensure the maximum and continual security of cardholder and personal data. The PCI DSS encompasses an extensive range of requirements, covering both the physical and digital environments. Best practice in relation to the PCI standard must take all aspects into consideration, from being diligent with staff training and restricting who has keys to the building, to ensuring the correct firewalls are in place and POS terminals cannot be manipulated.

Best practice in relation to the PCI standard must take all aspects into consideration...

With best practice in mind, Bottomley shared his experience of QSA certification. "Our committed approach to compliance, coupled with our confidence in the Spire payment software led to us undertaking an independent QSA evaluation. Our technology was successfully certified, but the assessment also made us improve the advice we give to merchants as part of the standard documentation. It showed us how important providing correct PCI advice to merchants is and the supplier industry should take some responsibility for this."

Bottomley continues, "Our new processes have proved successful in helping us reassure merchants that all compliance factors have been considered. A Spire terminal and adhering to the advice that comes with it goes a long way to ensuring compliance. Many merchants are now making the most of their partnership with Spire letting the terminal take the PCI strain. This works by connecting it to their till or POS and isolating all sensitive card data and processing to the terminal, whilst securing the network it communicates through."

WHO DEFINES BEST PRACTICE FOR PCI?

The PCI Security Standards Council (SSC) is responsible for the development, communication and implementation of the security standard. As stated by the SSC, its mission is "to enhance payment account data security by driving education and awareness of the PCI Security Standards (PCI SSC, 2012)."[8]

The SSC is an open global forum made up of the five founding payments brands, which have an equal share in the council's governance. Other industry stakeholders can join the SCC as Participating Organisations and review proposed additions or modifications to the standards.

As well as defining the standards, the SSC also provides supporting material to enhance payment card data security, including specification frameworks and support resources to help merchants.

8 *Bob Russo, 2012, PCI SSC webinar. Available at https://www.pcisecuritystandards.org/pdfs/2012_training_webinar.pdf accessed 19/06/2012*

QSAs provide support for implementation of the standard by ensuring validation of compliance is carried out annually for Level 1 and 2 merchants, while companies handling smaller volumes of transactions (Level 3 and 4 merchants) are required to carry out an annual Self Assessment Questionnaire (SAQ).

Some acquirers and Payment Service Providers (PSPs) have also attempted to inform merchants about the PCI standard and protection of personal data. Some provide their own lists of approved partners, however, without standardised requirements for building the list there is no guarantee of compliance.

Similarly to acquirers and PSPs, QSAs have been reluctant to give clear advice to retailers. One major issue is that QSAs must be unbiased, so it makes it impossible for them to advise on which third parties merchants should work with to ensure compliance.

INVESTIGATING ROOM FOR IMPROVEMENT

As this report suggests, there is definite room for improvement surrounding the understanding of PCI and the partnerships between vendors and merchants, and many businesses involved in the PCI chain are keen to accelerate it.

As outsourcing services becomes an increasingly popular way for Level 3 and 4 merchants to reduce the scope of PCI requirements that they must comply with, knowing which potential partners are trusted when it comes to compliance is of growing importance. Currently, the sources merchants turn to for advice in regards to the PCI DSS, such as QSAs, acquirers and PSPs, are not providing adequate support.

QSAs must appear unbiased so providing recommendations for specific vendors is difficult. Acquirers and PSPs have taken a more active role in advising retailers, however this still seems to be missing the mark as retailers are failing to listen.

Despite the existence of the PCI DSS for the best part of a decade, there are still too many retailers risking non-compliance. As the PCI DSS does not remain static, ineffective communication between all links in the PCI chain leave merchants on the back foot for compliance. Improving the mode of communication between all organisations, particularly to retailers, is one way of easing the compliance burden.

To aid effective communication, a standard set of best practice activity when it comes to selecting third party vendors would make PCI compliance for retailers more straightforward.

The below challenges highlight some of the key areas for development in the progression of PCI compliance and demonstrate the many areas for improvement, or progression in the continued evolution and understanding of PCI for all involved:

- Monitoring compliance of smaller businesses (Level 3 and 4 merchants)
- Enforcing compliance in smaller businesses (Level 3 and 4 merchants)
- Monitoring the compliance of third-party vendors/suppliers
- Ensuring consistency of compliance enforcement across all sizes of businesses
- Standardising compliance requirements across multi-channel payment platforms

AN 'IDEAL' PCI WORLD

With the current complexities surrounding PCI compliance, an "ideal" PCI world for most retailers would be one where the PCI DSS doesn't exist. Realistically however, this would leave huge volumes of cardholder and personal data exposed to criminals.

For most organisations, an "ideal" PCI world would be one where all retailers understand and meet compliance regulations.

For most organisations, an "ideal" PCI world would be one where all retailers understand and meet compliance regulations. Chris Nation, Commercial Manager Europe at Mako Networks, suggests, "In an absolute ideal PCI world there would be a single list of PCI-certified vendors that retailers could refer to. This would ensure that all outsourced services are fully PCI compliant and retailers are not left vulnerable. It would also give a clear message to the merchant that using a Level 1-certified service provider will provide safe harbour."

In fact, this can be taken one step further. If a single aggregator were to step forward and coordinate all the approved vendors, the process of choosing partners could be further simplified for merchants. With time and costs major considerations for SMEs in particular, dealing with lots of different partners isn't a viable option. An aggregator would play the role of co-ordinator, limiting the points of contact between retailers and their partners to a single one making the vendor role in compliance clearer.

Closing Thoughts and Conclusion

SUMMARY OF REPORT FINDINGS

When considering compliance, the vendor/merchant relationship needs to be simplified.

Managing multiple vendor relationships is time consuming, difficult and too complex overall for merchants.

A partnership for vendors headed up by a single aggregator would improve the current situation. The partnership would seamlessly manage and share information as required to set up standards of best practice and help give merchants comfort that they are compliant. Although some industry registers of approved vendors and service providers currently exist, a single checklist of certified partners who all meet the same standard would make choosing a trusted partner clearer for merchants.

Increased collaboration between vendors to provide single solutions helping cover multiple aspects of compliance would also consolidate costs for merchants.

Bill Farmer, CEO of Mako Networks summarises, "The vendor industry is still very segregated when it comes to compliance. Organisations work in silos, with little collaboration or standardised practices. This needs to change and the industry needs to work together more effectively in order to really make compliance more achievable. The development of more fit-for-purpose products and services with the necessary certification is one way to help ensure a standard level of practice across the industry. This is something we're highly committed to as shown in our continued investment and development of the Mako System."

Contributors

Bill Farmer
CEO
Mako Networks

Chris Nation
Commercial Manager, Europe
Mako Networks

Craig Bottomley
Head of Product Management
Spire Payments

James Lewis
Strategic Projects Director
Payzone

Mathieu Gorge
CEO
Vigitrust

Tim Bell
Director
Phoenix Managed Networks

Alan Stephenson-Brown
Director
Phoenix Managed Networks

Ian Dodd
Director
Service Logistics

About Mako Networks

Mako Networks is a network management company specializing in small site security, health record access and Payment Card Industry Data Security Standard (PCI DSS) compliance solutions. The company assists businesses around the world to secure their networks and provide the capabilities needed to better manage their network connections.

Mako provides its solutions using a unique cloud-based system consisting of two principal parts: a Central Management System accessed through a secure website, and network appliances installed at customer locations. Through this two-part system, Mako is able to deliver a range of services that provide Internet connection, protection, access control and detailed reporting.

Mako Networks currently operates from offices in San Francisco, London and Auckland, New Zealand, and through channel partners around the world.

Visit www.makonetworks.com for more information.