NETBENEFIT
Hosting peace of mind

In association with

HOW TO TAKE THE PAIN OUT OF THE PCI PROCESS.

A whitepaper by Tom Moores, Solutions Consultant, NetBenefit in collaboration with Ruth Xovox, Chief Compliance Strategist, Exois and former PCI Security Standards Council Board of Advisors Member

Foreword by
Neira Jones,
Head of Payment Security,

Barclaycard
and Board of Advisors member
PCI Security Standards Council

In the online world trust can be won or lost overnight.

No one has been able to escape the news and numerous commentaries on the recent high profile breaches. Evidently, hackers are no longer lonely teenagers in their back room trying to impress their friends: today's cybercrime industry has evolved and automated itself to improve efficiency, scalability, and profitability with a clear intent on obtaining information that can be monetised. With the Internet as their superhighway, they have no boundaries.

Perversely, the hackers' best friends are those very same businesses with their inadequate and often outdated information security practices, as well as those very individuals whose identities end up being stolen - particularly when they don't keep their antivirus and firewalls up to date and don't check the privacy settings on the many social networking sites they frequent, or fall prey to phishing attacks!

Undeniably, businesses are dependent on their customers' trust. This is even more crucial for online businesses and if ecommerce security is not high on the agenda, those businesses may lose more than they think. However -whilst governments around the world are looking to strengthen oversight and enforcement and business leaders are turning their attention to enterprise risk management as a strategic business driver - the awareness of how to protect against cybercrime is still lacking in the commercial world. This is not surprising, as companies often feel under pressure to meet compliance deadlines of one type or another and panic to implement solutions they believe will address the most visible, urgent or potentially costly to ignore regulation looming on the horizon (e.g. PCI DSS, Data Protection, FSA, SOX and others). Every year we share more of ourselves online - a trend that is set to continue. Each time we do this, we place our data and our faith in the security measures taken by those that manage that information on our behalf and those that advise them. With the rise in cloud computing adoption, business will introduce more and more players in their value chain.

The Payment Card Industry Data Security Standard (PCI DSS) was introduced in 2004 to help protect businesses and their customers' payment card information. PCI DSS is not a standard for standards' sake; it is, in my opinion, a collection of good data security practices and controls that any organisation should already have in place. It just happens to focus specifically on cardholder data. PCI DSS is about preventing card payment information held by merchants, or their third parties, from being used fraudulently and all the consequential financial and reputational losses associated with this.

As a very first step in simplifying merchant payment security endeavours, Barclaycard always advises retailers to seek PCI DSS compliant service providers (e.g. payment gateways, processors, managed hosting providers, shopping carts). But we understand that security can be tricky to navigate and businesses may not always have the in-house expertise to embed information security in their environments. As in everything, picking the right partners and advisers is key.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 01

Install and maintain a firewall configuration to protect cardholder data.

INTRODUCTION

Whichever way you cut it, achieving PCI DSS compliance is a significant undertaking for any business. When first approaching the process, many have described it as overwhelming, confusing and a little daunting in terms of the time, resource and budget it seems to take. It's no wonder many park the paperwork at the back of a bottom drawer, in a file marked 'to do later'. In many cases, that means much later or even, for the really brave, never.

Although choosing non-compliance may alleviate stress in the short-term, there's a very real risk that your decision will come back and bite you. The number of security breaches is increasing on a daily basis and although it may feel like it's only the biggest merchants that are under threat, research suggests that data breaches are now a statistical certainty. The simple truth is that your security will be breached at some point and if you don't have the right controls in place, it could cost you your business.

The good news is that help is at hand and if approached in the right way, becoming PCI DSS compliant does not have to be a painful process. Nor does it have to take as much time or effort as you may have been led to believe. The truth is that everyone involved in the PCI DSS process specifically, and in online payments in general, has a vested interest in creating a safe and secure environment for consumers. So there are plenty of people available that can help you achieve compliance. Your first, and possibly most important job, is to pick the right partners.

There are 2 key partnerships that you need to consider when taking on PCI DSS compliance:

- Qualified Security Assessor (QSA)
- Approved Scanning Vendor (ASV)

We understand the importance of choosing the right partners for PCI compliance. After all we've been through the process ourselves and experienced the ups and downs first hand. We know that if you pick the right partners you can find that the scope of the project is more manageable, that much of the confusion is taken away and that you achieve compliance significantly quicker and more cost effectively than you hoped possible.

CHOOSING A QSA

The Qualified Security Assessor or QSA is by far your most important partner. They are the trusted advisor who guides you through the compliance process. They are there to help you define the scope of the project, to identify the controls that need to put in place, discover where the gaps are and essentially, calculate the cost of achieving compliance.

Tom Moores
Business Development Manager, NetBenefit

"In this whitepaper we will take a look at who the QSA and the ASV are, the role they play and how to choose the right one for your business. We will then talk through how to get the most out of everyone that will be involved."

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 02

Do not use vendor-supplied defaults for system passwords and other security parameters.

The problem is that some merchants view them as auditors and approach the relationship as if that is what they are. This could not be further from the truth. PCI DSS is not an audit, it is an assessment and as such, the QSA is not an auditor who has been put on this earth to catch you out and make your life a misery. In fact, quite the opposite is true. Their aim is to ensure that the burden of compliance is as light as possible and that you achieve your goal as quickly and efficiently as you can.

Your relationship with the QSA should therefore be viewed as a partnership. After all you are in this together and have a joint responsibility to achieve a successful assessment. Their reputation quite literally depends on it.

Failure to properly assess a merchant can have dire consequences for a QSA. They will face fines and could be struck off the PCI SSC register. It is in their best interests to do the best job possible.

To get the most out of a QSA it is important that they are the right people for you and your business. Like any external consultant, be it an accountant or solicitor, you have to feel comfortable that they have the knowledge and expertise necessary to do what needs to be done. They must also be available as and when you need them, which is likely to be a lot. Being thorough in your selection is vital. Here are some tips on what to look for.

Does the QSA Consultancy have the right credentials?

There is no such thing as an independent QSA. They must all be part of a certified QSA Company. All certified QSA companies are listed on the PCI Security Standard Council's website. You can find them here:

https://www.pcisecuritystandards.org/approved_companies_providers/qsa_companies.php

Something that you should also look out for is whether the company is in remediation. Remediation usually means that one or a number of QSA's from that company have failed to meet the PCI SSC Quality Assurance criteria for the production of a number of Reports of Compliance. This doesn't necessarily mean that the company should be avoided but it is worth finding out what they are doing to put the situation right.

Is the QSA right for your business?

Becoming a QSA is not something that is taken lightly. Before they can begin the training, candidates need to prove that they have the right technical background for the job. Once this has been proven they are taken through a training process that starts with an online evaluation. If the online evaluation is successfully completed, the QSA then has to complete face-to-face-training and a further assessment to qualify.

Qualification is not the end of the process. Every QSA has to re-qualify every year and show that they are up-to-date with the latest improvements to the standard. Knowing their way around the standard is essential if they are to bring clarity to the scope of the project. The more they understand the standard the better their advice on the solutions you need to buy in and those you don't.

Interpreter

There is a fair amount of ambiguity in the standard and purposefully so. It is in effect a guide that highlights key areas of your business that you and your QSA should be investigating. Anyone that takes the guidelines literally is likely to miss important areas that could be exploited by hackers. You want someone who can interpret the guidelines and apply them in the best way possible to your business.

Payment experience

Payment specific experience is a must. Because of the ambiguity of the standard it is best to approach the assessment as if it is an audit. You have to look at everything and ask yourself whether it poses any level of risk to yourselves or your customers, regardless of whether there is a control that calls it out.

It is important that the QSA understands how your payment systems work, how data moves through your organisation and then on to all your suppliers involved in the processing of payments. No avenue of investigation should be disregarded.

Having an approved Report of Compliance (RoC) and being secure is not necessarily the same thing. There are many stories of companies that have ticked all the boxes of the assessment and fallen foul of hackers. Most of the breaches happen to what we call the unknown unknowns. The problem will be on a system that wasn't officially in scope but offers a breach point for hackers. There are examples of these types of tech in every business and it's important that your QSA can help you spot them.

Remember having a RoC does not insure you against data breaches. If your company is breached, regardless of whether you have a RoC or not, a PCI Forensic Investigator will have to complete an investigation of your environment. Should they prove that you were not compliant at the time of the breach, you would be liable to incur fines and fraud losses from your acquiring bank. If, however, the forensic investigator declares that you were PCI DSS compliant at the time of the breach, you would benefit from what is called "safe harbour" and not incur any fines or associated fraud losses. This is why you should always look at a continuous assurance posture instead of a 12 monthly audit.

Industry expertise

The QSA needs to be more than a security expert. They not only need a strong technical background but they must also have experience in payment systems and critically in your industry sector. The QSA should be prepared to spend the necessary

> "Just because you have a RoC doesn't mean that you are secure. This is where the ambiguity lies. There is security, having compliance and having a RoC. You should achieve all three; be secure, compliant and have a RoC,"
>
> Ruth Xovox, Chief Compliance Strategist, Exois and former PCI Security Standards Council Board of Advisors Member.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 04

Encrypt transmission of cardholder data across open, public networks.

time to understand the idiosyncrasies of your business and how they apply to the standard. There are industries that have greater complexities in their payment model that will offer different challenges. Airlines and hospitality are very complicated. Payments require a number of different steps. QSAs that have not experienced the nuances of these types of companies in the past will not know where the pitfalls are.

Communicator

The personality of the QSA is also very important. The scoping will result in decisions, both budgetary and strategic, that need to be made at the highest level of your business. There is no doubt that the head of finance and the business owner, MD or CEO will need to be involved at some point. You need to feel comfortable that the QSA can communicate comfortably with everyone involved from the IT team to the Board.

Networker

True, the QSA has the ability to approve your RoC but the people who have the ultimate say on whether you achieve compliance are usually a rung higher up the food chain, e.g. your Bank or Credit Card Company. These relationships need to be effectively managed in order to get the final decision made quickly and efficiently. A QSA who does not have relationships with the acquirers or financial institutions will not be able to manage this final part of the process for you. The earlier these organisations are brought into the process, the better your compliance endeavours will be. Make sure your acquiring bank is involved early instead of just presenting them with a final RoC.

Does the QSA consultancy have their own agenda?

Being suspicious of external consultants is only natural. While they are bringing in much needed skills and knowledge, you may feel that they will make you spend money on stuff that you don't actually need. It is certainly worth finding out what else the QSA consultancy sells. They may have technical solutions that they can make available to you but these should not be offered upfront.

If during the compliance process it becomes obvious that you need a technical solution to enforce a control, then it may actually make sense to purchase what the QSA has. Dealing with one supplier is always simpler than having a number of partners. The QSA should be supplier agnostic. Their number one priority should be helping you to achieve compliance, not selling you ancillary services.

Make sure that your QSA is upfront about the other services that their consultancy offers and whether they also deal with other technology suppliers. In addition, when they have technical solutions to offer, make sure to ask what the alternative solutions would be. Your acquiring bank can also help with this and make sure you ask the right people before committing to a purchase.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 05

Use and regularly update anti-virus software.

The Top 5 Questions you must ask your QSA

1. How many assessments has your company undertaken this year?

More assessments mean more experience. The greater the experience the more likely they will be able to spot gaps and enable you to avoid pitfalls.

2. How many assessments have you undertaken in our industry sector?

Not having experience in your sector is not the end of the world but having it will make them eminently more qualified to help you.

3. How many assessments have you undertaken for a company our size?

Like you industry, your company's technology infrastructure will have its own idiosyncrasies. You want someone that has experience dealing with a system of your complexity.

4. How long have you been with your consultancy?

Make sure that the person has a good history with the consultancy and is not the type that moves from one business to another in quick succession. The last thing you want is for your QSA to leave half way through the process.

5. What other services does you company provide?

Remember it may not be a bad thing that your QSA consultancy has technical services that can help to make the process of updating your systems more efficient. What is important is that they can remain independent of these services and only offer them if they are relevant.

"There are lots of grey areas in the PCI process and so it's essential to partner with someone who can give you straightforward answers that enable you to make the right business decisions. A QSA should understand your business, be familiar with the latest updates to the standard and be available to give you advice as and when you need it,"

Sarah Edwards, Operations Manager,
NetBenefit.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 06

Develop and maintain secure systems and applications.

> By attaining the service provider accreditation, NetBenefit has demonstrated that its processes, systems, policies and procedures comply with the relevant requirements and can now provide a comprehensive PCI DSS compliant environment to its customers seeking PCI DSS as a merchant.
>
> Kevin Dowd,
> Director of Security Assessment, CNS

CHOOSING AN ASV

The Approved Scanning Vendor or ASV is responsible for testing your system's vulnerabilities and detecting potential threats to it. To meet compliance your network must be scanned once a quarter both during and after you have been approved. The results tell you whether you are meeting compliance and also highlight anything that might present a risk, e.g. residual cardholder data.

Many of the ASVs in the UK are either QSAs or part of a security vendor's offering. It is a fairly generic service and so the criterion for choosing your vendor is nowhere near as involved as choosing your QSA. For many it comes down to price. I would suggest that if you feel comfortable using your QSA to do the scanning, then it may make sense to do so. After all it is one less contact point that you have to manage. However the same rules apply here as they did with the QSA. Scans can be used to sell you further services. Some you may need, some you may not. Always ensure that you need any additional services that you are offered.

STREAMLING THE COMPLIANCE PROCESS

NetBenefit was recently asked by the head of a digital agency whether they could just hand the whole PCI bit over to us, so that they didn't have to worry about it. Unfortunately the answer is no.

Yes, we offer a hosted solution that could dramatically minimise the technical pressure but they would always be responsible for their internal policies and the actions of their staff.

It occurred to me that what he was actually asking me was how to make this process as quick and pain free as possible. Again the answer is very straightforward; the earlier you engage with everybody that needs to be involved from the acquiring bank to your QSA and the stakeholders from inside your business, the smoother your journey will be.

The design agency provides a good example of why this approach works. This particular agency is responsible for the creation of iPhone apps for some of the largest consumer brands in the UK. To date their applications have been downloaded by 1.4 million users.
They had very minimal exposure to the Cardholder Data because it simply touched

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 07

Restrict access to cardholder data by business need to know.

their system on its way to their client. We had been asked in because they felt it made sense to have their application hosted on a PCI compliant platform that would minimise the scope of their technical compliance and make them exempt from answering certain areas of the Self-Assessment Questionnaire (SAQ).

They had 5 key questions that they wanted answered:

1. Should they be considered as a merchant or a service provider?

2. How long was compliance going to take?

3. How much was it going to cost?

4. What resources would they need internally to achieve compliance?

While it would be difficult to answer these questions emphatically, we were able to move each from unknown quantities into a clear vision of what lay ahead, after just one meeting.

We got everyone that needed to be involved in the PCI process together and draw a simple schematic of their system onto a whiteboard. We then talked them through what would be needed to achieve compliance. It was important that the QSA was there to agree the strategy. If they had not been and had not agreed with the approach we had laid out, it would have meant going back to the drawing board.

By the end of the meeting the digital agency understood the technical scope of the project and had the added assurance that it had the QSA's seal of approval. It meant that we could go away and quickly cost out the solution and the QSA could focus on the internal policies of the company.

Once the QSA had done their gap analysis, there would be a very clear view of the length of the project, the cost and the internal resource needed.

Of course not everybody will be able to benefit from a hosted platform but the process is the same:

- Identify all of the stakeholders that will be involved.

- Blueprint your system.

- Detect the gaps in your security and work with the QSA to identify the technical fixes.

- Agree upfront with internal stakeholders what their involvement should be and the strategic and budgetary decisions that need to be made.

Do this as early as possible and the easier the process will be for you.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 08

Assign a unique ID to each person with computer access.

Glossary

Acquiring Bank: A bank that issues payment or credit cards from a card issuer

ASV: Approved Scanning Vendor (responsible for scanning the network on a quarterly basis)

PCI (DSS): Payment Card Industry (Data Security Standards)

PCI Security Standards Council: The body that sets PCI DSS Standards

QSA: Qualified Security Assessor (certified by the PCI Security Standards Council to carry out independent on-site annual audits)

ROC: Report on Compliance (a formal document completed for the acquiring bank by the QSA)

RDP: Remote Desktop Protocol

SAQ: Self-Assessment Questionnaire (used for certification of merchants processing fewer than 6m transactions per year)

SSH: Secure Shell

Tier 1 – Tier 4: The PCI Security Standards Council has tiered merchants according to the number of transactions they carry out each year, and acquiring banks have focused most attention on Tier 1 merchants, i.e. those carrying out over 6m transactions per year and which require QSA assessment. Tiers 2 to 4 – which include merchants of all other sizes – must all undertake self-certification and quarterly network checks.

Further reading

Official PCI Security Standards Council web site: www.pcisecuritystandards.org

About NetBenefit

Established in 1995, NetBenefit is one of the UK's most experienced managed hosting companies. We specialise in providing tailored managed hosting solutions that deliver security, resilience and online performance for business critical websites, applications and online advertising campaigns.

We have evolved with the internet to our position today as a leading provider of bespoke, flexible managed hosting solutions to well known brands while remaining small enough to be committed to the success of all our customers.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 09

Restrict physical access to cardholder data.

NETBENEFIT
Hosting peace of mind

Our team consists of experienced consultants, pre-sales, project managers, technical architects and engineers, all of whom are here to help guarantee the online success of your business. We are focused on delivering hosting peace of mind so that our customers can focus on what they do best.

- The NetBenefit team consists of approximately 70 members of staff committed to making our customers' business a success.
- We have offices in both the UK and France.
- We provide technical, professional UK based support 24x7 365 days a year.
- We have three customer data centres and a fourth located in Copenhagen for additional resilience.
- Our team is vetted to Baseline Personnel Security Standard.
- In addition to providing technical support and information architecture for our customers, we work closely with both Dell and Microsoft to develop, test and launch new hosting services.
- NetBenefit is a part of Group NBT. Group NBT is AIM listed and has successfully established its brands as leading providers of domain name and internet related services across Europe and into the United States.

About ExoIS

Founded just before the new millennium in the heart of Silicon Valley, ExoIS provides Information Security, Compliance and IT advisory and support to businesses, helping our clients identify and mitigate the risks inherent in today's increasingly interconnected business environments. As a PCI Qualified Security Assessor, today our services include a wide range of PCI services and other security and compliance offerings, covering the full spectrum of our clients' information security requirements. We also offer a range of managed services including secure cloud hosting, datacenter outsourcing, compliance SaaS solutions and storage services.

.

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 10

Track and monitor all access to network resources and cardholder data.

NETBENEFIT
Hosting peace of mind

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 11

Regularly test security systems and processes.

NETBENEFIT
Hosting peace of mind

12 STEPS TO BECOMING PCI DSS COMPLIANT

STEP 12

Maintain a policy that addresses information security.