PCI Compliance – Are you ready?

By Syd Bolton

In life we are certain of death and taxes. For the last few years in the point of sale business we added our own certainty: PCI compliance. The problem is that, like death and taxes, we all know that we can't escape it – the issue is, understanding it completely.

To make things ever more confusing is the fact that the guidelines were developed for those using PC's as their primary point of sale device. If you use a stand alone payment processing terminal for your credit card processing then you automatically will inherit the compliance of said terminal. What if you use a point of sale device that is not a PC but talks to one? The guidelines aren't quite as clear. Either way, any PC's that are involved in your network have issues that need to be dealt with.

In a number of ways, PCI compliance can become confusing and ultimately frustrating, so we will work on each section to understand the intent rather than the actual requirement. I find this approach more digestible and you may as well.

First, you must "Build and Maintain a Secure Network". Regardless of what equipment you have, you need to have firewalls in place and stay away from using default passwords for devices. Equipment like routers and switches need to have their default security passwords changed. It is essential to follow the rules of a "strong password" to prevent someone easily guessing it. A password like "love" or the name of your dog just isn't enough anymore.

Secondly (and perhaps most obviously) you need to "Protect Cardholder Data". This tends to raise more questions than provide answers, but basically you need to encrypt any card holder data or (if at all possible) not store it at all. You must also secure the transmission of said card holder data across public networks (which include the Internet). For ultimate security you should also secure the data across a private network where possible, to prevent the possibility of someone installing a packet sniffer and discovering card holder information. If you have a legacy point of sale system, you may be out of compliance in this regard. The best course of action is to contact your POS vendor to check your status. If you are using a proprietary communication network, it's less of an issue. If you are using standard Ethernet and TCP/IP then you need to take additional steps. This is one time where standards can work against you.

"Maintaining a Vulnerability Management Program" is a fancy way of telling you that you need to have processes in place to make sure that your anti-virus software is up to date and you don't allow just anyone to install software (even upgrades) without a proper, approved process. You are well aware that any chain is only as strong as its weakest link – the same applies to PCI compliance. Any software that is custom developed for you must be secure and adhere to various policies that don't violate anything that you are reading here today.

This raises a really key point in this whole process. One of the first things you need to do in terms of PCI compliance is make a list of all the software you have installed on your machines that come in contact with card holder data. When you have that list, you need to contact each software vendor and see where they lie in terms of compliance. This is the starting point of a "gap analysis" which is a fancy term for "shortcomings".

You are also going to need to "Implement Strong Access Control Measures". This means that you need to restrict access to the machines involved in card holder data – and perhaps not just in the ways you might think. You need to limit the access to other businesses involved on a strictly need to know basis. Every person that has login access to those computer(s) will require a unique identifier (log in name or ID) so that any activity can be traced back to an individual.

You must also "Regularly Monitor and Test Networks". You need to be aware of who is accessing the computers containing sensitive information (or one's connected to computers containing sensitive data) and regularly test security systems and processes. It's not really hard to do; it's just more difficult to be diligent about doing it.

Finally, you need to "Maintain an Information Security Policy". This means you need to review your policy as it relates to security and everything previously discussed then make changes/updates as necessary. These are all really 'best practices' which is a term you are going to hear a lot about as you go down the path of PCI Compliance.

Of course there is so much more to say about this topic, and this is certainly just the start. What you need to keep in mind is that eventually, no matter how big or small, the PCI Compliance wave will wash over you. It's better to start dealing with it now so you are prepared rather than leaving it until you are forced. For more information, you can also visit www.**pcicompliance**guide.org as a good starting point for information.

Syd Bolton is the Evolutionary Product Manager at Datasym and has been involved in writing software for almost 25 years. Syd has written software used by companies like Microsoft, Merv Griffin Enterprises, Amblin Entertainment and EDS. He currently specializes in high-speed credit card solutions (and PCI compliance) and in his spare time runs a Personal Computer Museum (www.pcmuseum.ca) near Toronto, Canada. Syd writes about computers for the local newspaper and also about gaming for online magazines such as the Armchair Empire (www.armchairempire.com).