

# Whose responsibility for compliance is it anyway?

**Dan Raywood**

August 14 2009

In recent conversations between myself and various spokespeople there has been a recurring theme, in this case compliance. To be specific, Payment Card Industry Data Security Standard (PCI DSS) compliance.

I was talking to Francis Ofungwu, manager of security strategy at Rackspace Hosting, who was announcing the company's recent compliance achievement for its managed hosting service. The subject came up about what would happen if a service provider were to fail on compliance, and specifically what this would mean for the merchants who use the service.

Thinking laterally, if the provider is unable to provide a certificated and compliant service, then surely all of the businesses that it supplies will be unable to trade and be left high and dry.

Ofungwu claimed that in order to store credit card data you need to prove your ability to be compliant to the high PCI standards, and as Rackspace has clients who store and process payments as part of their offering, it too needed to be PCI compliant.

What if data was lost though? Ofungwu said: "If you don't follow the rules then there will be heavy fines. It will impact your business from a scrutiny perspective."

In agreement on the last point was Mike Gillespie, director at Advent IM, who pointed at the example of the Home Office data loss that was the responsibility of PA Consulting.

Gillespie said: "A lot of the details are down to contractual agreements, and who knows whose responsibility. What is less clear is where the reputational damage lies. The Home Office was more dragged through the mud than PA Consulting but it was the latter's loss."

He also claimed that there is a similar situation in local government that are now outsourcing payments to Capita to do their card processing managed service. Gillespie said: "The attitude of councils is to outsource is best, but it is still their customer's data. So if something goes wrong Capita will be liable but the blame lies with the council."

Gillespie further claimed that the responsibility of data management is that of the company who owns it, regardless of whom it is outsourced to. He said from the side of the service provider, when you outsource services you do not outsource risk, so it is at the risk of the merchant to choose wisely and monitor what is happening with their data.

Gillespie said: "Organisations will take at face value that it is securely stored, but they will determine it and show how they manage it, it is the same with disposal, you never see the process and then there are firewalls on eBay.

"From a legal liability perspective, the buck will stop with the person or company doing the processing, the liability stops there but the responsibility should still rest with the originator."

A recent news item followed this trend; with a report made that some of the firms who have recently experienced data breaches were PCI-compliant - highlighting the fact that even if a company had passed the test for compliance they must remain up to date for the regulatory front.

Reuven Harrison, chief technology officer at Tufin, claimed that 'complacency is the IT manager's worst enemy, especially when it comes to IT security'.

Harrison pointed to recent claims by Douglas Merrill, former VP of engineering with Google at the Black Hat Conference, that if senior managers become frustrated with an IT architecture, staff will look for workarounds that allows them to circumvent their own security systems.

Harrison said: "Regulatory compliance and best practice certifications are excellent indicators of management quality, but when it comes to security, the acid test is whether multiple layers of security are installed, and are reviewed - as well as tested - on a regular basis."

So is this a case for the PCI Council to insist on certain practices, and insist that things are done in a certain fashion?

Ofungwu explained how the accreditation process works: "PCI Council does its security assessment and they represent councillors who are service providers, so are customers who take credit card payments. They perform audits and submit these to the processors and once the high level of the credit card companies receive the report they approve it at a high level."

However Gillespie had a less than complimentary take on the PCI Council, stating: "The big problem with PCI is that no one is enforcing it, what message are banks sending to their customers when they don't insist on implementing it? Organisations will spend money where they have to and the FSA will claim that it is mandatory but no enforcement will be done."

What is clear is that there is a real lack of clarity when it comes to PCI compliance, with a contrast in opinions on its poignancy, ability and facility. Perhaps one message to take away from this debate is from Mike Gillespie that you need to consider who you outsource to, and realise that it is your data to manage and realise whose name will be dragged in the dirt in the event of a breach or loss.

**SC Magazine, August 2009**