PCI DSS– let's put it back and higher on the Agenda

We live in a connected world more than ever – just wait for the term 'The Internet of things' if you have not heard of it before. (see http://en.wikipedia.org/wiki/Internet_of_Things)

The consumer today is using the internet more and more – from shopping to travel and hospitality – and so by default credit cards and their like (I count PayPal in this).

The internet, Google, the OTAs and Meta-mediaries (E.g. Room 77, Hotel Tonight) have brought hotels and hospitality more in towards the general retail and consumer market – rooms and meals can be booked online in the same session as buying clothes and music on Amazon.

In the book 'The end of Money' David Wolman writes about cash now just being the realm of tax dodging and crime and manages to go a whole year without cash.

Why would you try and pay or a hotel room with cash when you can earn points on your credit card company's rewards scheme? Contactless card payments are seriously on the rise already to take things to the next level.

So from a hotel business point of view – less worrying about the contract for collection of cash and cheques to be delivered to the bank like in 'ye olde days'. However all this credit card data is now circulating in the business and industry creates just the right opportunity for lax Data Security and fraud – and hence the need for PCI DSS. (Payment Card Industry (PCI) Data Security Standard)

Our strategic partners HFTP and their CEO Frank Wolfe have recently released a blog on the latest issues and breaches – see http://blog.hftp.org/another-credit-card-breach-what-now/

Frank says, to quote briefly about a breach at White Lodging in the US, "Regardless of the tens of millions of dollars industries spend to protect credit card data, criminals who try to steal this data are constantly attacking our information systems and eventually they get lucky — for a short time. As in these recent cases, they were shut down."

PCI DSS is really all about Data Security – and the question I would have for any hotel or hospitality business as a start point is: Who has responsibility for it in your organisation?

If you don't know you need to define it PDQ (pun intended..) – As it can vary from Finance to IT Departments – but whichever way – make it clear who is responsible.

After that it is a case of working through the disciplines and controls – the PCI Security Council has produced a pretty good basic InfoGraphic as a summary (see https://www.pcisecuritystandards.org/pdfs/PCI-Top-Ten.pdf) and below.

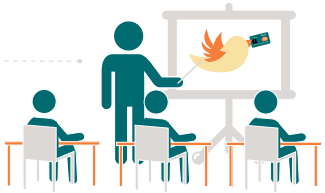
Stay Smart

on Protecting Against Card Fraud!

Trying to understand what you can do to keep your customers' card data safe and protect against fraud? Unsure of where to begin?

Take a look at these ten simple steps to help you get started in your security efforts:

1 Educate



Employees should be trained annually on both online and physical security threats as well as on the best practices for protecting cardholder data.

Just a reminder, you can also check with your Acquiring Bank or payment service provider to see what training or education they provide.

2 Update

Keep your employee manuals up-to-date with information on the proper handling of sensitive information, including cardholder data.

3 Screen

Pre-employment screening is a basic and essential practice for any business owner, especially for those employees that have access to sensitive customer or financial data.

4 Protect

Make sure your business has a firewall, anti-virus, malware and spyware detection software. And don't forget to regularly update the software.

5 Be Aware

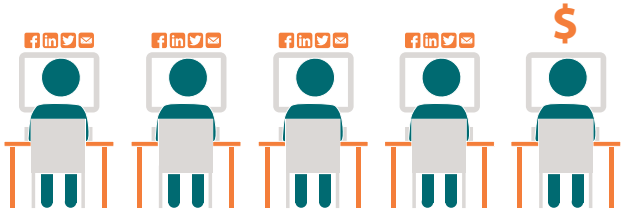
Pay attention to fraud prevention alerts from your virus and malware services, make sure you install updates as soon as they become available.

6 Control

Tightly control downloads, software installations, the use of thumb drives and public Wi-Fi connections on computers used for payment card processing.

7 Separate

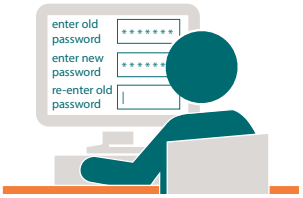
Designate a separate computer for processing of all your online financial transactions. Try to keep this computer separate from social media sites, email and general internet browsing which can present chances for the computer to be susceptible to vulnerabilities.



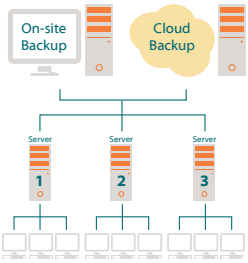
8 Change

Change your passwords regularly, and especially after you have outside contractors do hardware, software or Point of Sale System installations or upgrades.

Make sure that you use complex passwords to make them more difficult to guess (include upper case letters, numbers and special characters).



9 Back Up



Make sure you regularly back up your computers and the key data you want to protect, whether it's to a local machine or an offsite facility, so your business can be up and running again quickly in the unfortunate event of an unauthorized attack.

10 Learn

Check out the **PCI Security Standards Council Website** for more information on the Data Security Standards, education and training resources available to your organization.

Stay smart and safe by following these important security best practices. For more information on PCI Standards, visit **www.pcisecuritystandards.org**

PCI Security Standards Council

I have spoken with a few Hospitality people involved with PCI – It can be a bit like Tax as being seen a specialist 'nerdy' type of field of expertise. But here is the thing – PCI DSS enforcement is on its way – and any problems in this area could affect your business and brand much harder than any tax issues.

Let's be more specific…What about attacking this from the manual processes and guest journey point of view? Mark Jelley of Avenue9 and a previous Hotel IT Director for Mark suggests the following:

• ***Update.*** Your employee manuals with information on the proper handling of sensitive information, including cardholder data. *Have you got your SOP's in order?*

• ***Educate.*** Employees should be trained annually on both online and physical security threats as well as on the best practices for protecting cardholder data. *This should include the retaking of any assessment program AND the re-signing of any HR documentation.*

Other points I would consider...

1. Have you got your process SOP's updated for PCI?

2. Have your contracting companies (outsourced housekeeping, the fitness class tutor, golf professional) acknowledged AND SIGNED your PCI SOP?

3. Have you got your manual procedure written? What do you do if the power goes off/you lose connectivity?

4. This a BUSINESS project and NOT a Finance or IT one. Therefore operational engagement is key to successfully MITIGATING THE RISK.

5. It affects EVERY department in the business.

6. Physical security is key. Operational areas such as Reception, C&E office, back office, finance should be protected by a punch key lock OR a Vincard equivalent.

7. Archive and storage needs to be logged AND locked.

There are a few systems out there that can scan your computer networks for PCI Type Data (Credit Card numbers and patterns) and can start (and scare) you into taking action.

PCI DSS was 'all-the-rage' a few years ago and has probably drifted. Frank Wolfe believes that there are more breaches to come – or be announced. Does the UK hospitality business want to be part of this?

If we owe it to our guests to have all the Health and Hygiene disciplines for their food, all the Health and Safety managed and Fire Regulations adhered to – surely we owe it to our guests to protect the payment and financial details safe as well?

And if you don't know what to do – then find a resource to help you and talk to other HOSPA Members.

Carl Weldon – February 2014.

PCI DSS is Short for Payment Card Industry (PCI) Data Security Standard (DSS)

PCI DSS is a standard that all organizations, including online retailers, must follow when storing, processing and transmitting their customer's credit card data.

The Data Security Standard (DSS) was developed and the standard is maintained by the Payment Card Industry Security Standards Council (PCI SSC).

To be PCI complaint companies must use a firewall between wireless network and their cardholder data environment, use the latest security and authentication such as WPA/WPA2 and also change default settings for wired privacy keys, and use a network intrusion detection system.

Resource at:

https://www.pcisecuritystandards.org/index.php
http://www.hftp.org/Pages/PCI/HotelPCIResources.aspx
https://www.pcisecuritystandards.org/pdfs/PCI-Top-Ten.pdf
http://www.hftp.org/Pages/NewsPress/NewsPressContent.aspx?article=http%3a%2f%2fwww.hftp.org%2fContent%2fNews%2fHFTPNews%2f2011-03-15a.html&RSS=HFTP&auth=None