



The state of PCI DSS compliance

Global, European and Irish perspectives

Irish Payments Services Organisation PCI DSS Explained

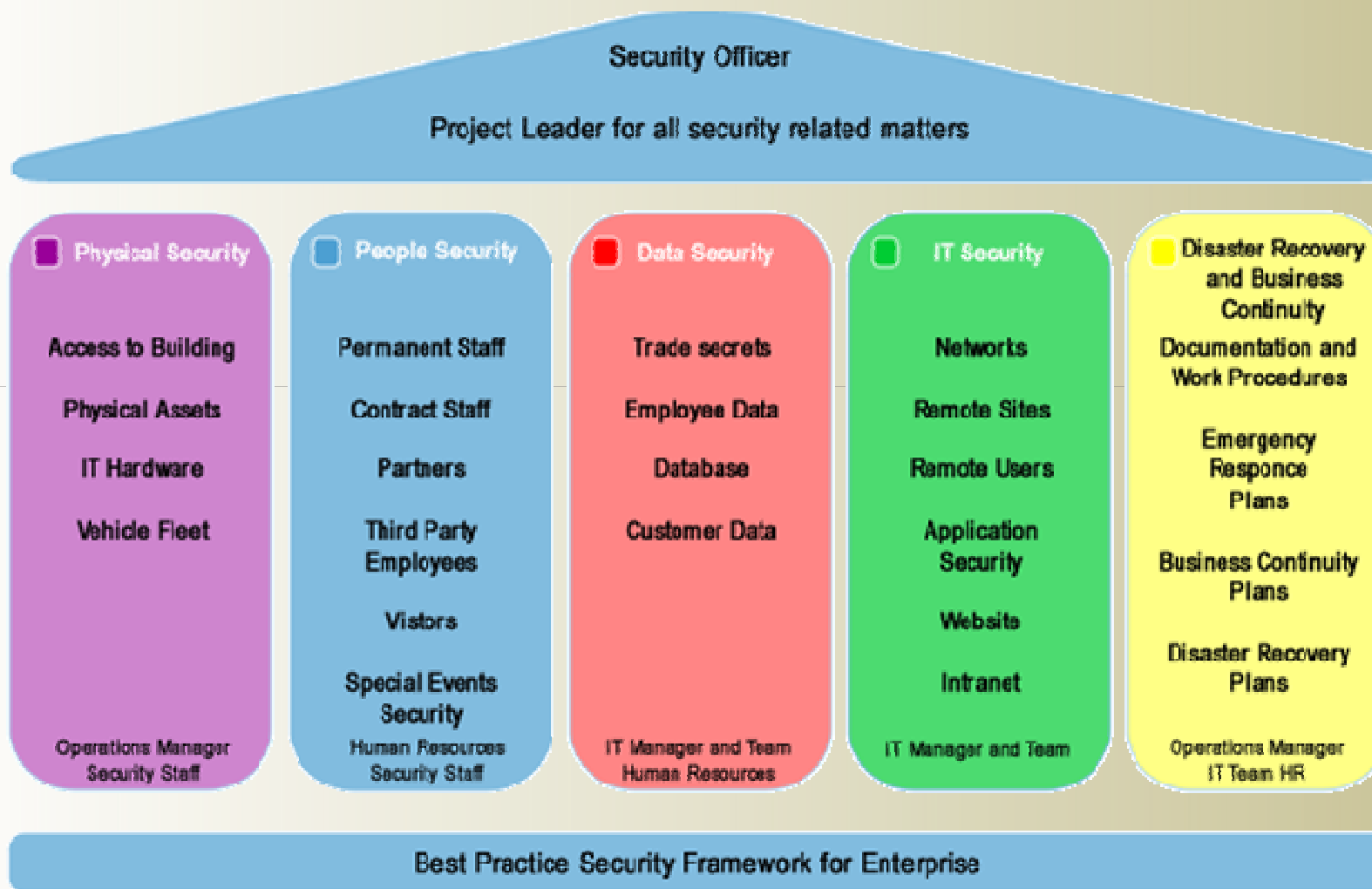
Dublin 2nd September 2010

Prepared by Mathieu Gorge, CEO – 2nd September 2010

Agenda

- **VigiTrust & The Five Pillars of Security™**
- **Update on PCI DSS**
 - Global Perspectives
 - European Perspective
 - UK Perspective
 - Irish Perspective
- **What's new with PCI DSS in 2010 - 2011**
- **Recommendations & Take aways for your organization**
- **Best Practice Tips to comply cost-effectively**
- **Q& A**

VigiTrust & The Five Pillars of Security™



Security Accreditation Process

1. Education (from top-down)
2. Pre-assessment (self governed)
3. Remediation
 - a) policies & procedures
 - b) technical solutions and settings
 - c) security skills transfer
4. Audit (QSA)
5. Maintenance phase -
 - a) to ensure that you continually monitor your compliance status

Update on PCI DSS – Global Perspectives (1)

Reminder – what are the threats of non compliance to the industry

- Increase in Fraud Levels
- Harm to your business
- Card Re-issuance Costs (Costs passed to the merchant)
- Inconvenience to customer & loss of consumer Confidence
- Adverse Publicity for your organization
 - Name & shame
 - Brand & Reputation Damage
- Legislative Interest – Threat of Governmental Regulation
 - Already have PCI DSS into Law in Nevada, Minnesota, New Hampshire
 - This will become federal Law in the US with 5 years & EU will follow

Update on PCI DSS – Global Perspectives (2)

- **US remains the most compliant territory in terms of PCI DSS**
- **Wireless & Virtualization SIG White Paper**
 - **Benefits and dangers of Virtualization for payment systems**
 - **Definition of Virtualized “Network Components”**
 - **Details on how to create security zones**
 - **Cross Virtualization Leakage**
 - **Weaknesses in Hypervisor (access control, patching, monitoring)**
 - **Change control within Virtualized environments**
- **Tokenization vs End to End Encryption**
- **PCI DSS will be updated in October 2010**
 - **PCI DSS Lifecycle Reminder – from 2 to 3 years**
 - **V2.0 – “no major changes but clarifications”**
 - **PCI DSS and PA-DSS 2.0 Summary of Changes – Highlights**

Update on PCI DSS – Global Perspectives (3)

Inflexion Point for PCI DSS in Europe

- What's the inflexion Point?
- Europe vs US
- PCI Maturity Levels Criteria
 - PCI DSS & Credit Card Related Incidents
 - Market Background Information
 - Retail Industry & PCI DSS
 - Level 1 Merchant Info
 - Acquiring banks & Aggregators PCI DSS readiness programs
 - QSAs
 - PCI DSS coverage within security circles
 - PCI DSS Council Participating Organizations

PCI DSS in the News

HOME

NEWS

World

Germany

German Reunification

Europe

Business

Science & Technology

Environment & Development

Culture & Lifestyle

Sports

GERMANY INFO

Visit Germany

Study in Germany

Map

Weather

GERMAN COURSES

Learning German

Deutsch unterrichten

German XXL

DW-RADIO

What's On?

Programs

Reception

Audio on Demand

Learning by Ear

DW-TV

What's On?

Program Guide

Programs

Video on Demand

Reception

About DW-TV

INTERACTIVE

Reader Response

Newsletters

Web Tools and Services

Podcasting

Mobile

About DW-WORLD.DE

CRIME | 18.11.2009

Massive credit card fraud exposed



A probe has been launched into credit card fraud

Concerns about data privacy have led a number of banks to replace thousands of credit cards. Mastercard and Visa uncovered the security breach after data from a Spanish partner company was stolen by thieves.

Thousands of credit card holders have been told to hand back their cards after fraudsters in Spain illegally obtained information about their accounts.

The massive credit card recall involves more than 100,000 credit cards in Germany. Customers of Germany's cooperative banks have been hardest hit with more than 60,000 affected. A spokesman for the association of cooperative banks BVR said the fraud involved Visa and Mastercard credit card holders who recently traveled to Spain.

But other banks and savings institutions in Germany are also affected.

"It's a massive replacement program. A number of credit card distributors have been affected including some from other countries. We are not sure how many cardholders were in Spain at the time in question," Andreas Martin of the German Central Credit Card Commission (ZKA), told Deutsche Welle.

Security breach

Last month around 15,000 bank customers from KarstadtQuelle-Bank had to have their cards replaced. At the beginning of November, Barclaycard and Lufthansa (Miles & More) followed suit.

High street bank Deutsche Bank has also confirmed that considerably more cards have been replaced recently. Commerzbank announced that it too had issued new credit cards and new numbers as a "precautionary measure".

Mastercard and Visa warned the banks about possible problems after irregularities were discovered at a Spanish payment processor, according to the Financial Times Deutschland newspaper. Police have launched a criminal investigation. No further details about how the fraudsters got hold of the customers' account information have been released.

Banks say that all affected customers will be notified by their banks in the coming days.

nrt/dpa/AP

Editor: Michael Lawton

RADIO NEWS



Listen to world headlines from the top of the hour.

PICTURE OF THE DAY



DW-TV EUROPE live



Journal - With Business

DW-RADIO LIVE

Concert Hour
ARD Music Competition (II)
Listen live

FEATURE



Life behind the Wall

DW-TV presents a unique animated depiction of the former German-German border.

PICTURE GALLERY



Helsinki, National Bureau of Investigation is examining the big card information burglaries in Finland

19/02/2010

More than 100 000 available in the hacker-proof card number

Helsinki police computer crime unit will examine the criminal took place in Helsinki on a large card information theft. Movement in Helsinki poorly secured payment system was exported to tens of thousands of payment card data. The system had saved more than 100,000 individual card information. Motion, the system has now been renewed.

Logs of the intrusion is made abroad. The data so far have been made to the individual copy cards, which have been used around the world.

Card issuers are in contact with their customers to exchange the cards and identify abuse.

Intrusion was discovered in the normal Board Credit card information turvallisuusmonitoroinnissa. Credit delegation informed the police immediately.

- At present, misappropriated card information is mainly caused by a risk; Credit municipality has shown no signs of large-scale information of this card abuse, said security card services director Henry Kylänlahti Credit delegation.

Card holders do not worry about that. If the card details have been compromised, the bank will contact the card holder payment card redemptions. Own bank or card issuer, please contact only if the card now or later events reveal something unjust. Events can be conveniently monitored through the bank's own network.

Card follows the instructions given to the card holder does not incur liability for the costs of card counterfeiting.

Police hope, particularly for small traders to check the commitment of the system security.

SOMMAIRE

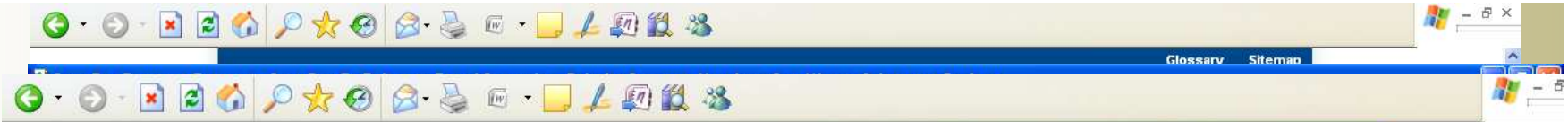
- I - INTRODUCTION 6
- II - NOTIONS DE DONNEES PORTEUR 7
- III - PRESENTATION DES ACTEURS 8
 - III.1 - Le PCI Security Standards Council (PCI-SSC) 8
 - III.2 - Les RESEAUX CARTES 9
 - III.3 - REPORTS DES CONTRAINTES PCIDSS ENTRE LES ACTEURS (SCHEMA) 12
 - III.4 - APERÇU ET COHERENCE DES STANDARDS PCI 13
 - III.4.1 - PCIPED 13
 - III.4.2 - PCIPA-DSS 13
 - III.4.3 - PCIDSS 13
- IV - CYCLE DE VIE DU STANDARD PCIDSS 15
 - IV.1 - ETAPE 1 –IMPLEMENTATION – MOIS 1 A 9 15
 - IV.2 - ETAPE 2 –RETOURS D’EXPERIENCE – MOIS 10 A 12 15
 - IV.3 - ETAPE 3 –REVUE DES RETOURS D’EXPERIENCE – MOIS 13 A 20 15
 - IV.4 - ETAPE 4 –ELABORATION ET FINALISATION DE LA NOUVELLE VERSION – MOIS 21 A 24 16
 - IV.5 - ETAPE 5 –PUBLICATION DE LA NOUVELLE VERSION DU STANDARD 16
- V - PERIMETRE D’APPLICATION DU STANDARD PCIDSS 17
 - V.1 - DEFINITION DU PERIMETRE PCIDSS 17
 - V.2 - ECHANTILLONNAGE 17
 - V.3 - LES SCANS ASV 18
- VI - REDUCTION DU PERIMETRE PCI DSS 20
 - VI.1 - PRINCIPES DE REDUCTION DU PERIMETRE PCIDSS 20
 - VI.2 - NOTION DE SEGMENTATION RESEAU APPROPRIEE 21
 - VI.3 - FOURNISSEURS DE SERVICES ET REPORTS DE RESPONSABILITES 22
 - VI.4 - DEROGATION POUR CERTIFICATIONS DE PERIMETRES SPECIFIQUES 23
 - VI.5 - AUTRES ASPECTS CONCERNANT LA REDUCTION DU PERIMETRE 23
 - VI.6 - RESPONSABILITE VIS-A-VIS DES PRESTATAIRES 24
- VII - STRATEGIE DE CONSERVATION DES DONNEES CARTE 25
 - VII.1 - QUELLES DONNEES CONSERVER ? 25
 - VII.2 - MOTIVATION ET DUREE DE STOCKAGE DE CES DONNEES 25
 - VII.3 - CONDITIONS DE STOCKAGE ET D’UTILISATION DE CES DONNEES 25
- VIII - LES MESURES COMPENSATOIRES 27
 - VIII.1 - QU’EST CE QU’UNE MESURE COMPENSATOIRE ? 27
 - VIII.2 - CONDITIONS DE LEGITIMITE D’UNE MESURE COMPENSATOIRE 27
 - VIII.3 - CONDITIONS DE VALIDITE D’UNE MESURE COMPENSATOIRE 28
 - VIII.4 - ILLUSTRATION D’UNE MESURE COMPENSATOIRE 28
- IX - PCIDSS, VERITES ET CONTRE VERITES 30

Update on PCI DSS – Global Perspectives (4)

- **The Heartland Payment issue**
 - But my QSA did confirm my compliance status...
- **QA Program for QSAs**
 - Why a QA Program
 - 8 Principles of the QA Program
 - Already have some QSAs in remediation
- **Issues due to Lack of understanding of compliance levels & validation mechanisms**
- **Focus on Security Awareness Training**
 - Recommendations for **eLearning** & tests
- **Assessors are spending more time analysing policies and procedures**
- **Overall Trends as regards continuous compliance**
 - PA-DSS – Pin Transaction Security
 - ISO 27001 cross over – multi regulations mapping
 - ROI of PCI DSS Compliance

Update on PCI DSS – The UK Perspective (1)

- PCI DSS & Credit Card Related Incidents
 - RBS WorldPay data breach incident
 - March 2009 BBC report:
 - Credit card and debit card fraud cost the UK banking industry £608m in 2008 – a rise of 14% on 2007
- Market Background Information
 - Data Protection Act 1998 & Impact on PCI DSS
- Focus on UK Online Retail
 - 2009 CyberSource UK Online Fraud Report (6th Edition)
 - “*Data security and PCI compliance is another area where responsibility varies across organizations[...]. CIOs/IT Directors* tend to be held accountable in most organisations (36%), although the *CEO/MD* is not far behind (27%).
 - The person responsible for the payment security policy should have ***complete visibility of their organisation’s end-to-end approach to managing sensitive data***. This is not simply about data storage, but moreover, all system and ***human interaction with payment data*** – this can make the task incredibly complex.”
 - “***payment tokenisation*** with remote secure storage and hosted payment acceptance services [provided by CyberSource] let you capture and process payments ***without storing or transmitting payment data***. This is a great way to streamline PCI compliance and mitigate security risk”



Merchant Compliance Portal

You are not logged in. (Login)
English (en)



Introduction to the Payment Card Industry Data Security Standard (PCI DSS)

Planet Fitness Merchant Compliance Portal

[Click here to view Merchant Compliance Portal FAQ's](#)

Live Security News

- French net filtering plan moves forward
- New browser tweaks Chrome security
- Govt throws £4.3m at internet fraud prevention
- EPIC files privacy complaint against Google Buzz
- OpenOffice 3.2 fixes several vulnerabilities

Support Helpline

Call: (646) 688-3380
Email Support: support@vigitrust.com

Latest News

29 Jan, 16:57

Update on PCI DSS – The UK Perspective (3)

QSAs in the UK

- 28 QSA's without counting Global QSAs
- We can expect market consolidation because
 - The market is too crowded in the UK: Too many assessors for too few level 1 & 2 organizations
 - Price of recertification is too high for the rewards as assessment unit prices are driven down through market over supply
- **Quality of UK QSA** is to be scrutinized because of the price war going on in the country
- Some QSAs for PCI DSS will now focus on **PA-DSS**
- QSAs are trying to become the *trusted advisors*
- QSAs are teaming up with **acquiring banks and payment service providers** to **offer PCI DSS programs** to lower levels
 - Levels 3 & 4
 - But please note that QSA validation of SAQs is **NOT** required in the UK or in Ireland – only in Canada

Update on PCI DSS – The UK Perspective (4)

PCI DSS coverage within security circles

- ISACA, ISSA, VendorCom, Financial Services Club
- Retail Cards & Payments, London 12th & 13th May 2010
- Contactless Cards & Payments, London, 21st & 22nd June 2010

UK & PCI DSS Council participating Organizations

- Barclays, HSBC, Royal Bank of Scotland Group and Lloyds TSB - one third of the overall registered POs in this category
- APACS and VendorCom listed as organizations – most represented in Europe
- UK accounts for half the POs listed as POs on the site with Kingfisher IT Services, Sanderson, Secureelectrans and Serve base.
- Remarkably the UK has 12 out of 13 merchants listed as POs:

Alliance Boots, Co-Operative Group, IL Ltd, JD Sports Fashion Plc, John Lewis, Sainsburys, Tesco Stores Ltd, Transport for London, TUI Travel Plc, Vodafone UK, WM Morrisons Plc

What about PCI DSS in Ireland then (1)?

- ☉ **PCI DSS & Credit Card Related Incidents**
 - Fraud is on the increase including credit card fraud
 - ATM fraud
 - PED fraud
- ☉ **Market Background Information**
 - Data Protection Act 2003
 - Is data breach notification really coming to Ireland?
- ☉ **Retail Industry & PCI DSS**
 - Hospitality Industry is being targeted by Visa
- ☉ **Acquiring banks & Aggregators PCI DSS readiness programs**
 - Elavon & AIB are actively writing to merchants
 - Compliance readiness programs vs. PCI DSS validation programs
 - Other programs available from security houses, Payment Service Providers and POS providers

What about PCI DSS in Ireland then (2)?

☛ QSAs

- 3 main QSAs plus 3 International QSAs
- Watch this space...

☛ PCI DSS coverage within security circles

- ISSA
- ISACA

☛ PCI DSS Council Participating Organizations

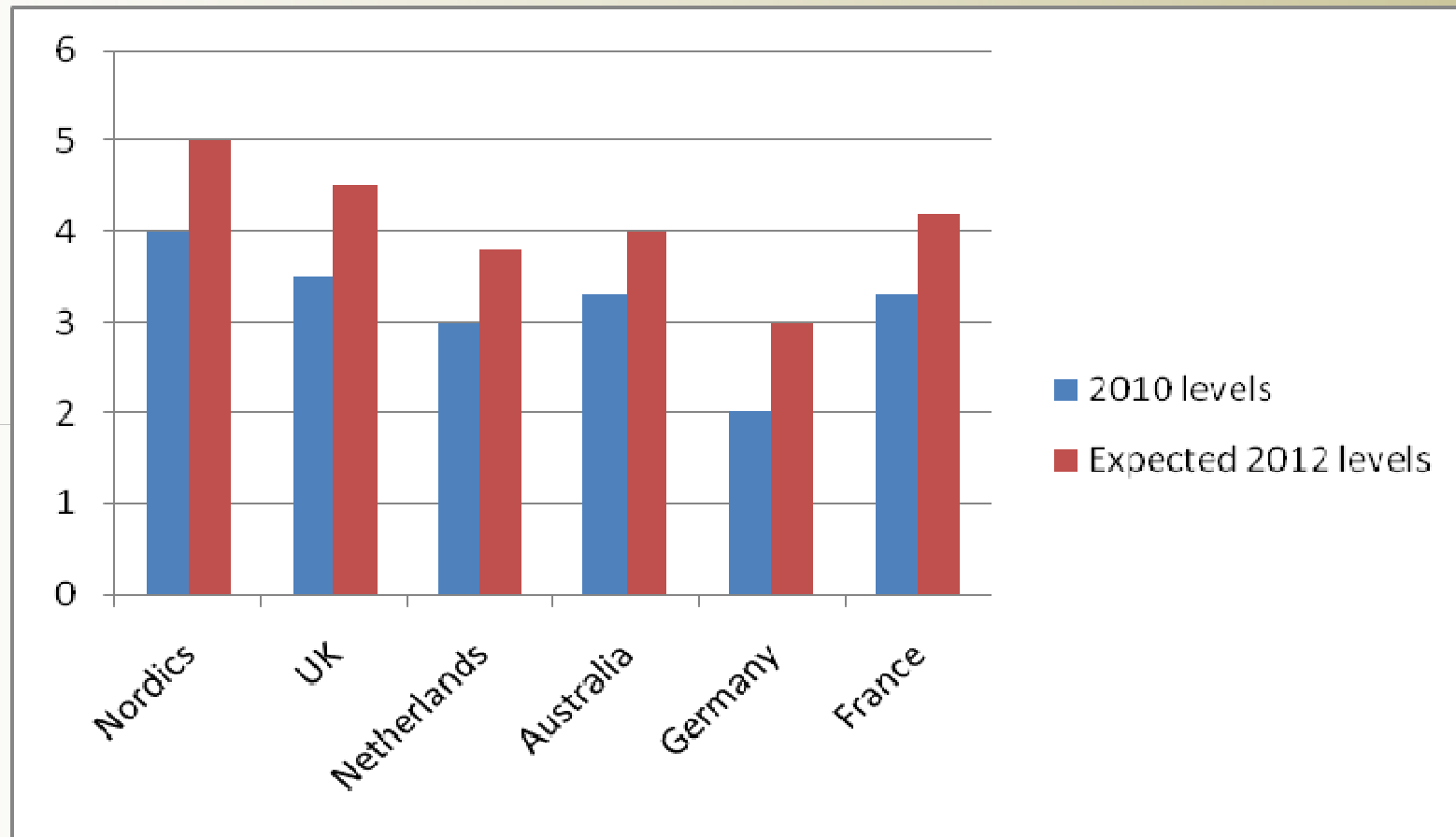
- Only 5 so far...

☛ Future for PCI DSS in Ireland looks quite bright actually

- All the signs are here – this is getting serious
- The fact that IPSO is focusing on PCI DSS is telling
- DPA already covers personal financial info
- Financial regulator may well look into it very soon...

Update on PCI DSS – UK vs other territories

Three Year outlook



Update on PCI DSS – Conclusions

What does it mean for your organization?

- PCI in the UK is happening now – be prepared! Ireland is following suit
- UK is extremely well represented within the PCI DSS community – Ireland could do better
- Security Professionals in the Ireland are very active around PCI DSS challenges and 2010 will be even busier in terms of PCI DSS events
- SearchCompliance.co.uk regularly writes about PCI DSS
- There will be more fines
 - They may initially be driven by Data Protection Act fines
 - They are already being imposed by Visa

You need to start taking corrective action now and comply by the end of 2010!

Tips & Recommendations to comply with PCI DSS in 2010

☛ What first steps can you take?

– Remember the five accreditation process steps

- Education
- Pre-assessment (internal)
- Remediation
- Actual Assessment
- Continuous compliance

If you are not already in the process of getting compliant, make sure you get started now! This is happening for real and won't go away!

– Mix of 3 key elements

- Policies & procedures
- Technical Solutions
- Awareness Training

– What do you next then?

- Policies & procedures: draw up a list of P&Ps in place @ your org.
- Technical Solutions: update your network diagram + pen test
- Awareness Training: identify in-scope employees and start the education process

– Ensure you use a comprehensive readiness program!

Validation only does not cut it for PCI DSS!

For more information on PCI DSS and how **VigiTrust** can help

www.VigiTrust.com

Credit card Security 101
PCI DSS 101
Security 101

PCI DSS & ISO 27001 White Paper
Future of Security Standards

Mathieu Gorge

mathieu.gorge@vigitrust.com

<http://www.linkedin.com/in/mgorge>

Cell: +353 87 623 8649
Office: +353 1 453 9143



www.vigitrust.com