

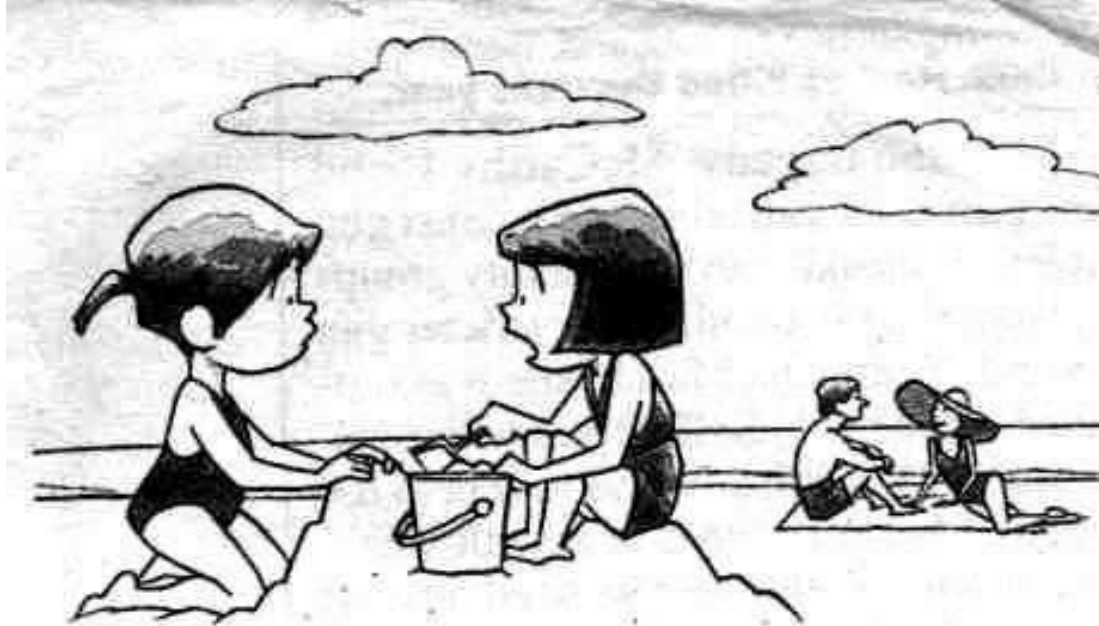


**CSO** Interchange  
FRANCE

**Industry Data Security Standard) : historique,  
objectifs et exigences ; le role du PCI Council.  
Comment se preparer au processus d'accreditation”**

Mathieu Gorge, PDG, VigiTrust

# La Sensibilisation est un facteur clé



**"I'm never having kids. I hear they take nine months to download."**



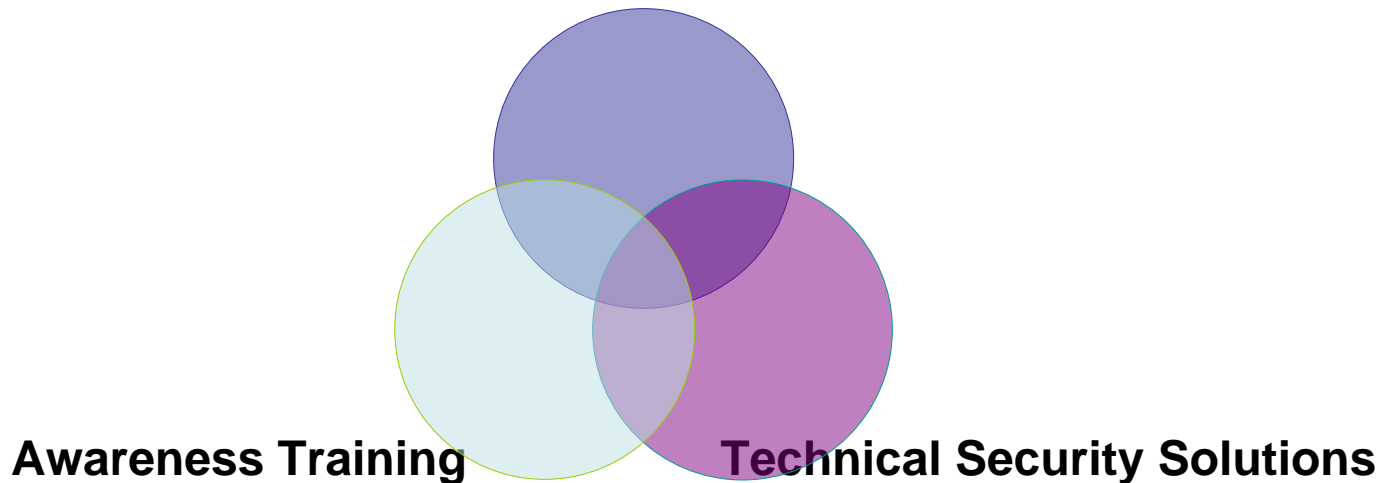
# PCI Standard – La norme PCI

- Introduction
- Historique de la norme PCI
- Objectifs
- Processus d'accréditation & Rôle du “PCI Council”
- Les risques liés à la non-conformité
- Les opportunités apportées par la norme – valeur ajoutée de la norme
- Futur de la norme
- Meilleures pratiques de mise en conformité
- Questions - Réponses – Forum & Discussion



# Les ensembles de la sécurité - VigiTrust

## Security Policies and Audits



# La norme PCI – ce qu’il faut prendre en compte

- But officiel de la norme
  - Norme(s) en matière de sécurité des données
  - “Ce document décrit les 12 exigences des Normes en matière de sécurité des données (Data Security Standard, DSS) de l’industrie des cartes de crédit (Payment Card Industry, PCI). Les exigences PCI DSS s’organisent en 6 groupes logiques liés, qui sont des « objectifs de contrôle ».”
  - Tente de répondre aux attentes des entreprises et citoyens en matière de sécurité des données et d’usurpation d’identité:
    - Depuis 2005 Gartner, FBI & SANS se sont particulièrement penchés sur les thèmes de l’usurpation d’identité et de la fraude bancaire - phishing
    - Les incidents les plus récents: Polo Ralph Lauren, TJX (2007)
      - TJX est un incident qui a catapulté la norme PCI (media, industrie, expertise)



# Structure de la norme PCI (1)

**Mettre en place et gérer un réseau sécurisé**

**Protéger les données des titulaires de carte**

**Disposer d'un programme de gestion de la vulnérabilité**

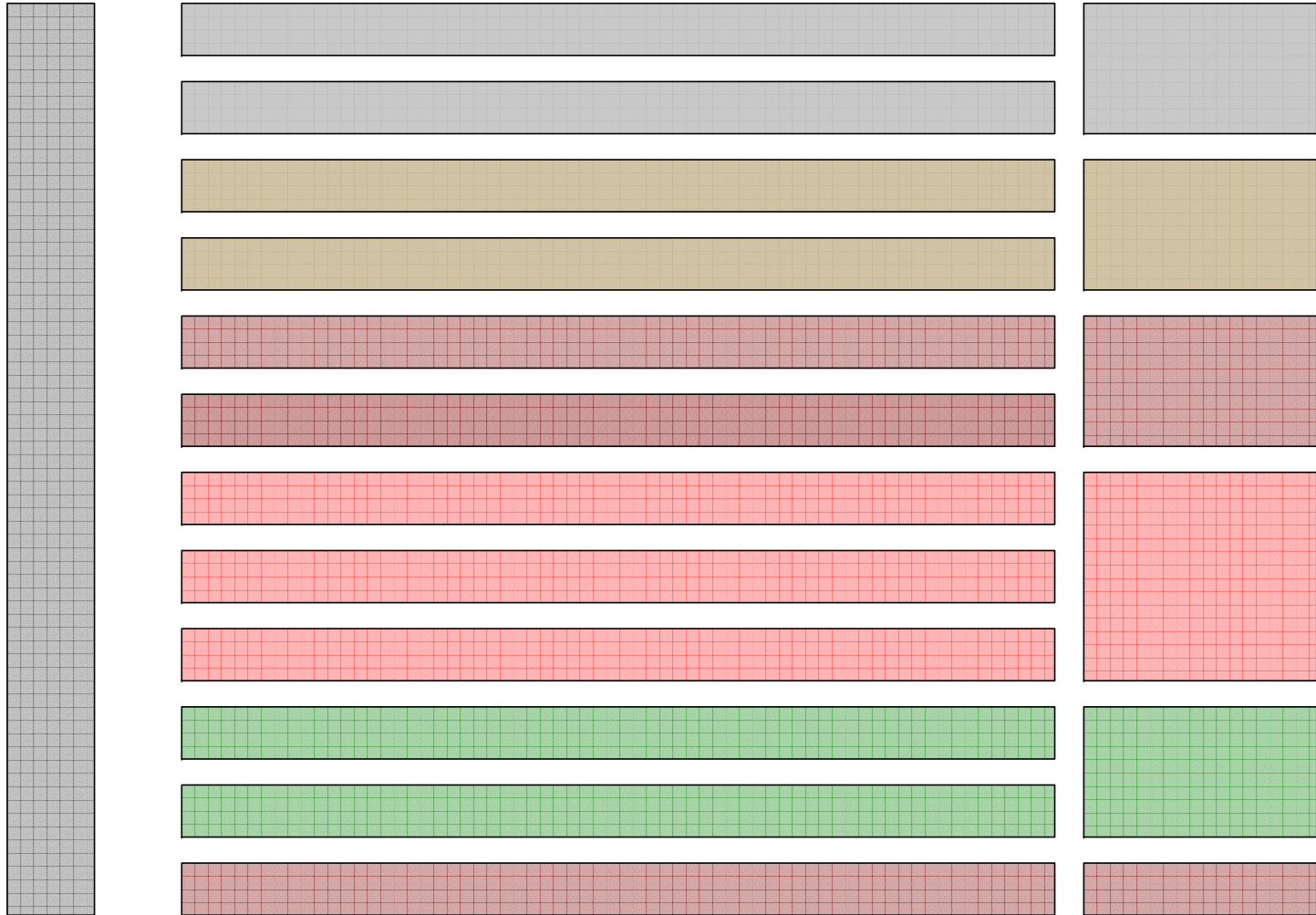
**Mettre en oeuvre des mesures de contrôle d'accès efficaces**

**Surveiller et tester régulièrement les réseaux**

**Disposer d'une politique en matière de sécurité de l'information**



# Structure de la norme PCI (2)



# Niveaux de mise en conformité, exigences & validation de la mise en conformité

<b>Opérateurs</b>				
<b>Marchands</b>				

**OU VOUS SITUEZ VOUS PAR RAPPORT A LA NORME PCI?**

*PCI Council, Banque, Marchand, Opérateur, Vendeur certifié, OSA*

*Consultant en Sécurité*

**Compliance and Validation Requirements**



# En ce qui concerne le processus d'accréditation...



- Le processus d'accréditation est long et exige un budget conséquent
- Il faut travailler avec les Qualified Security Assessors (QSAs)
- La plupart des entreprises "candidates" doit investir dans de nouvelles technologies, des politiques et procédures de sécurité ainsi que de la formation pour les utilisateurs
- Il s'agit souvent d'essayer d'adapter les systèmes en place à la norme plutôt que de développer une stratégie de mise en conformité à la norme PCI
- Concept du TTA "Time to accreditation concept"
- Notions de Coût et de Retour sur l'Investissement.



# Quels sont les points forts et les points faibles de la norme PCI?

## ▪ Les points forts

- Certaines exigences sont très claires
- Les technologies / solutions qui sont recommandées par le standard sont toutes sur le marché, souvent à des budgets acceptables
- La norme est basée sur des politiques liées aux rôles de chaque utilisateur
  - La norme PCI est basée sur les meilleures pratiques de sécurité
  - Notion de gestion des cycles de développement et du changement
  - Se penche notamment sur la formation des utilisateurs non-techniques et la formation poussée des administrateurs techniques

## ▪ Faiblesses de la norme

- Le niveau de compréhension de la norme est faible au niveau global
- Les exigences de scans & le temps écoulé entre les scans: quelle est la valeur ajoutée des scans & les scans sont-ils exigés assez régulièrement?
- La norme ne couvre pas toutes les dernières menaces de sécurité
  - Les dangers des systèmes d'impression des réseaux PCI
  - Les dangers associés à l'utilisation de L'IM
  - L'usage et les dangers de la virtualisation



# Les menaces (1)

- Menaces pour la norme PCI
  - Un certain manque de **crédibilité** du à un manque d'application de la norme (dates butoir changées, peines imposées)
  - **Contrôles Compensatoires / Correctifs** ouvert à différentes interprétations
    - “Des contrôles correctifs peuvent être envisagés en liaison avec la plupart des exigences des Normes PCI DSS, lorsqu'une entité n'est pas en mesure de se conformer aux spécifications techniques relatives à une exigence, mais a suffisamment atténué le risque associé.”
    - Sont utilisés pour répondre à “des contraintes techniques ou commerciales”
    - “Seules les entreprises ayant complété une analyse de risques et ayant dûment documenté les contraintes technologiques ou commerciales les empêchant de se mettre en conformité avec un contrôle précis sont autorisés à utiliser les contrôles compensatoires”
      - Méthodes préférées pour mener une étude de risques? (v1.1: NIST & SANS)
      - Le QSA a-t-il assez de compétences pour comprendre le contrôle correctif et son efficacité?



## Menaces (2)

- Comment les QSA sont-ils sélectionnés – A quoi doit se limiter leur rôle – Sont-ils assez indépendants pour mener les audits PCI?
  - Issue d'éthique – Les QSA doivent-ils être autorisés à proposer d'autres services que des services d'audit à leur clients?
  - Comment les QSAs sont-ils formés à leur rôle??
- Les solutions ne paiement sont souvent vendues “ouvertes” et non-conformes
- Les éditeurs “abusent” de l'angle commercial que la norme PCI leur donne – leur message aux entreprises est parfois trompeur
  - Par ex la Solution XYZ rendra votre société conforme....
- Time-to-Accreditation (TTA) – considérations de coûts
  - TTA peut s'étendre à 18 mois
  - Les coûts sont parfois très élevés, le Retour sur Investissement n'est pas toujours évident, les budgets ne sont pas accordés à temps, le rapport temps/accréditation est rallongé



# Opportunités (1)

- Opportunités pour le “**PCI Council**”
  - Opportunité Immediate pour promouvoir la norme PCI
    - Website, newsletter, Evènements?
    - Opportunité pour la version v1.1 vers les cibles (marchands, opérateurs)
    - Opportunité d'utiliser le feedback des membres du conseil pour les prochaines versions
- Opportunités pour les “cibles” de la norme de construire une stratégie de sécurité autour de la mission de mise en conformité
  - Gouvernance d'entreprise – convergence de la sécurité et de la mise en conformité
  - ROI – Retour sur investissement
  - Productivité & nouvelles opportunités commerciales



## Opportunités (2)

- Opportunités pour l' **industrie de la sécurité** de promouvoir des normes avec des objectifs "réalisables"
  - Les 12 sections et les 220+ contrôles de la norme sont en ligne avec les meilleures pratiques et sont **réalisables**
  - La norme impose des notions de **responsabilité**:
    - Banques, Opérateurs, Marchands, Hosting Providers
  - **Opportunité unique** et exceptionnelle de promouvoir une vraie norme dédiée à l'industrie des paiements bancaires – de v1.0 à 1.1: les prochaines versions seront-elles régulières?
    - Spyware & adware sont désormais ajoutées à l'AV de v1.0 à v1.1
    - Les éléments de guidance sur les contrôles correctifs
    - Hosting providers doivent séparer les marchands ce qui devrait faciliter l'audit PCI
    - Web app firewall and/or code reviews – exigence 6



# La norme PCI et les autres normes et lois en sécurité – opportunités de mutualisation

- **ISO 27001**
  - Certification mutuelle entre PCI et 27001?
- **OWASP & Center for Internet Security (CIS)**
- SOX, SB 1386, EU Data Protection Directive – Basel II
- Valeur juridique de la norme?
  - **Minnesota Plastic Card Security Act, Mai 2007**
  - En général, la valeur non-juridique et commerciale de la norme aide
    - La norme est bien reçue par l'industrie de la sécurité
  - Des sanctions financières mais aussi des opportunités de Rol et de meilleure productivité



# Autres considérations

- Les solutions de scans et autres fonctions automatiques aident à la mise en conformité
  - Solutions d'analyse de logs
  - Authentification & IAM solutions
  - Firewalls, IDS/IPS, web app firewall, chiffrement
  - Solution de gestion du processus d'accréditation?
    - Solutions disponibles pour 27001 (exige des connaissances de la norme) mais pas encore pour PCI
  - Solutions techniques pour conformité PCI déjà sur le marché – sont-elles fiables? Guides de configuration?
  - Peu de Forums PCI et de sources d'information indépendantes



# Futur de la Norme...



Copyright 2005 by Randy Glasbergen. [www.glasbergen.com](http://www.glasbergen.com)

Le taux de **sensibilisation** à la norme doit rester une priorité pour le Conseil

Les **éditeurs** vont continuer à jouer la carte PCI – risques?

Il sera de plus en plus facile d'avoir **accès à des informations indépendantes sur la norme**

**TTA** – réduction?

- Solution de gestion d'accréditation PCI

**TJX** va continuer à servir d'exemple pour le moment mais le prochain incident sera encore plus marqué en ce qui concerne l'application de la norme



# Meilleures pratiques de mise en conformité

- **Conseils pour les entreprises qui doivent se soumettre à la norme PCI**
  - Utiliser les informations mises à votre disposition
    - <https://www.pcisecuritystandards.org/>
    - [www.visaeurope.com/aboutvisa/services/accountinformationsecurity](http://www.visaeurope.com/aboutvisa/services/accountinformationsecurity)
    - [www.pcialliance.org](http://www.pcialliance.org) - <https://www.pcisecuritystandards.org/>
    - <http://www.mastercard.com/us/sdp/index.html> - [www.vigitrust.com](http://www.vigitrust.com) (Livre blanc)
  - **Partage d'expériences – le manque de politique de sécurité et de focus stratégique resque le plus gros obstacle au processus d'accréditation**
  - **Ne vous limitez pas au savoir de votre QSA – Testez les QSA!**
  - “vendez” la **valeur ajoutée** de l'accréditation aux top management (par ex ROI)
    - *Changer le concept de mise en conformité obligatoire en stratégie pro-active en sécurité – maximisez vos investissements en sécurité*
  - L'adaptation de systèmes existants exige du temps supplémentaire - **TTA**
  - Les entreprises sont invitées à profiter des **opportunités stratégiques** que la mise en conformité PCI apporte (ROI, productivité, Sécurité des Systèmes) – Win/Win
  - **PCI est là pour rester** – L'industrie de la sécurité va vous y pousser



# Summary – Q&A – Forum Discussion

© 1999 Randy Glasbergen. www.glasbergen.com



**"It's the latest innovation in office safety.  
When your computer crashes, an air bag is activated  
so you won't bang your head in frustration."**

Merci!

Questions?

[mathieu@vigitrust.com](mailto:mathieu@vigitrust.com)

+353 87 6238649

[www.vigitrust.com](http://www.vigitrust.com)

