CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

Conformité : quel apport pour la sécurité, la continuité d'activité ?

CNIS-event

Paris, 27 avril 2011

Pascal LOINTIER
Président du CLUSIF
pascal.lointier@clusif.asso.fr

La finalité de la sécurité de l'information devrait être une contribution au maintien opérationnel de l'outil économique

Au niveau sûreté, 4 patrimoines majeurs pour l'entreprise

- Les Personnels
- Les bâtiments et les biens
- L'environnement
- Le système d'Information / les immatériels

De quoi parle-t-on ?

(in Le Robert Junior, édition 1999)

Normes : 1. Etat habituel qui correspond à la majorité des cas

Standard : qui appartient au modèle courant

Règlement : ensemble de règles que l'on doit respecter

Conformité : en accord avec le règlement

Des dizaines d'acronymes,
certains s'imposent légalement
d'autres ont une connotation commerciale très forte…

Grandes tendances

Les 90' : approche probabiliste et choix de sécurité en conséquence

2001, une mauvaise année aérienne (9/11 mais aussi de nombreux accidents) : approche par impact et létalité

2002 SOX ; 2006 PCI DSS : gouvernance juridique et non plus investissements de sécurité (cf. Etude Gartner 2007)

- 2002, la messagerie instantanée qui avait suppléé aux besoins à New-York, très sérieusement repensée par le Pentagone et des Grands Comptes… puis arrive la section 404 de SOX
- 2002, Auditor's Full Employment Act ☺

Success stories

2008 : Chaîne de supermarchés Hannaford (conforme PCI-DSS) et 4,2 millions de références bancaires subtilisées… màj de PCI-DSS dans l'urgence. **Quel feedback sur la réduction de fraude ???**

Wednesday, September 17, 2008

مصرف دبي
DUBAI BANK

About Us | Retail Banking | Corporate Banking | Investment Services Group | Dubai Bank Online | Careers | Media Center | Contact Us

Skip Navigation Links Home » Media Center

Media Centre

News

Text size: A A

News

11 Sep '08

Dubai Bank reimbursed 42 ATM fraud affected customers

With regard to the recent incidences pertaining to ATM fraud affecting most banks in the UAE. Certain sections of the media have misrepresented the facts about the impact on Dubai Bank. The correct fact is that only Forty Two customers of the bank were affected. The affected customers have already been reimbursed.

26 Aug '08

Dubai Bank achieves highest Information Security accreditation

Dubai Bank, a Dubai Group company, has announced its Information Security Management System (ISMS) has been accredited at the highest possible level, receiving ISO 27001:2005 certification. This is an all encompassing international standard, designed to protect and improve the security of financial information and transactions for the bank and its customers.

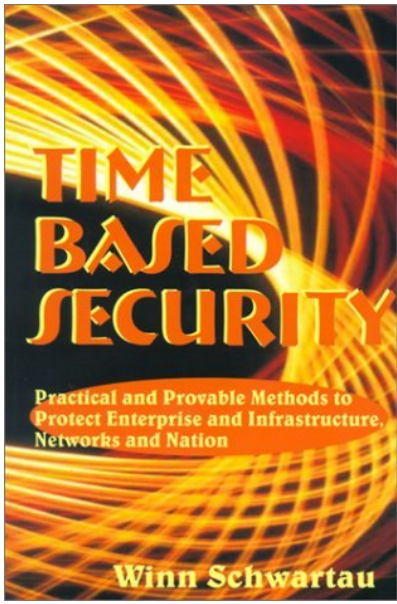
Bank with us
Call 800-55 55

Find your nearest
ATM/branch

Peut-on « normer » un S.I. ?

- Pas deux infrastructures (et PSI) identiques
- Pas deux emplois identiques d'un même S.I., c.à.d. enjeux économiques et pas seulement exposition à des scenarii de dommages
- Constante instabilité, dynamique de croissance du S.I. (Cf. TB.S. de Winn Schwartrau, une autre approche)
- Le risque majeur est humain, c.à.d. une ingéniosité malveillante constamment renouvelée

mais aujourd'hui le processus est lancé,
on n'arrête pas un courant, on le dévie…



Le business de la conformité

A un standard (conférence PCI du CLUSIF du 7 avril)

- ✓ Coûts… 6M€, 12 M€
- ✓ Contournement par les Mesures complémentaires
- ✓ « Insouciance » de l'auditeur quand au besoin de sécurité détecté (dixit)

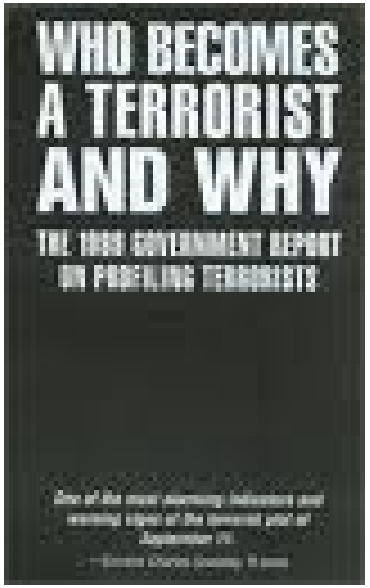
A une norme

- ✓ 27001, processus cyclique avec des contre-exemples de PCA inopérants…
- ✓ Marketing d'une normalisation portant sur un seul pan d'infrastructure

Une approche « culturelle »

ISO 2700x, à l'origine la BS (R-U), pas les Grundschutz (Allemagne)…

- ☞ Approche par checklist
- ☞ Codifier, stéréotyper (cf. démarche américaine du Criminal Profiling)



Différencier « l'inspiration d'un cadre référentiel » et la finalité d'une conformité… à un instant *t*

La valorisation d'impact et les enjeux de sécurité « économique » sont encore à améliorer/mettre en place…

Gestion du risque

4 grandes options

- Rejet total (abandon)
- Mesures de réduction
- Transfert (! Code Pénal)
- Acceptation (résignée)

Le marché de l'assurance propose un accompagnement en cas de défaillance malgré une conformité

Comment rendre « interopérables » des audits de normes et/ou/ standards et/ou règlements ?

- Réduction des dépenses pour qui est assujetti à des règlements, subit la pression commerciale de standards et souhaite créer une visibilité via une norme

Quelle pertinence, quelle adéquation ?

- ✓ Les ressources allouées à ces projets ne sont-elles pas soustraites de celles des projets de mise en œuvre d'une politique de sécurité ?
- ✓ La traçabilité imposée par un texte étranger ne s'oppose-t-elle pas à des lois locales protégeant les données personnelles et l'individu ?
- ✓ Une fois la mise en conformité réalisée, la vigilance et/ou l'effort d'amélioration d'une PSI ne risquent-ils pas d'être amoindris ?

CLUB DE LA SECURITE DE L'INFORMATION FRANCAIS

www.clusif.asso.fr libre téléchargement

Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon
954, avenue Jean Mermoz
34000 MONTPELLIER
Contact : Christian FERRAND
Site web : www.clusirlr.info

Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées
S/C INSA
Département de Génie Electrique et Informatique
135, Avenue de Rangueil
31077 TOULOUSE CEDEX 04
Contact : Laurent PELUD
Site web : www.clusir-mp.asso.fr

Club de la Sécurité des Systèmes d'Information de la Région Est
16, rue de Pont-à-Mousson
57000 METZ
Contact : Thierry RAMARD
Site web : www.clusir-est.fr

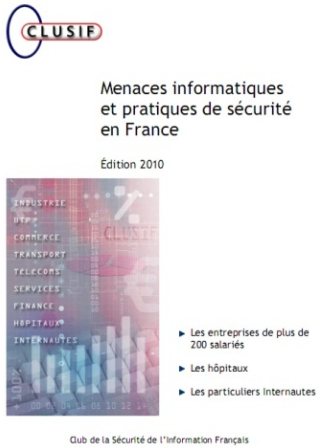
Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur
500, rue de Paradis
13008 MARSEILLE
Contact : Claude LELOUSTRE
Site web : http://www.clusif.fr/clusir-paca/

Club de la Sécurité des Systèmes d'Information de la Région Rhône-Alpes
SITIV
Passage de l'Avenir
69200 VENISSIEUX
Contact : Yannick BOUCHET
Site web : www.clusir-rha.fr

Club de la Sécurité des Systèmes d'Information de la Région Nord Pas de Calais Picardie
1862, avenue Général De Gaulle
59910 BONDUES
Contact : Gérard MOLINES
Site web : http://www.clusif.fr/clusir-npp/

Club de la Sécurité de l'Information de Poitou-Charentes
Technopole Venise Verte
Rue Euclide
BP 8421
79024 NIORT cedex 9
Contact : Sébastien Gloria
Site web : http://www.clusir-poi.fr/

Club de la Sécurité de l'Information Région Aquitaine
s/c Philippe Marty (Vice-Président)
51 rue Manon Cormier
33000 Bordeaux
Contact : Marc Ferrigno



Prochaine conférence CLUSIF :

« L'incident de sécurité : son identification, son traitement et ses enseignements »

16 juin

CNA, Paris