marcusevans conferences

Enterprise Risk Management

01/12/09

La gestion des risques de sécurité informatique

De la protection du SI à la protection de l'information

Patrick CHAMBET

http://www.chambet.com

Bouygues Telecom

DSI/DGOA/SSI

Sommaire

- Les risques informatiques - vulnérabilités, menaces, impacts
- Cartographie des risques sur un Système d'Information
- Gestion et réduction des risques de sécurité sur un SI
- Protection des données sensibles

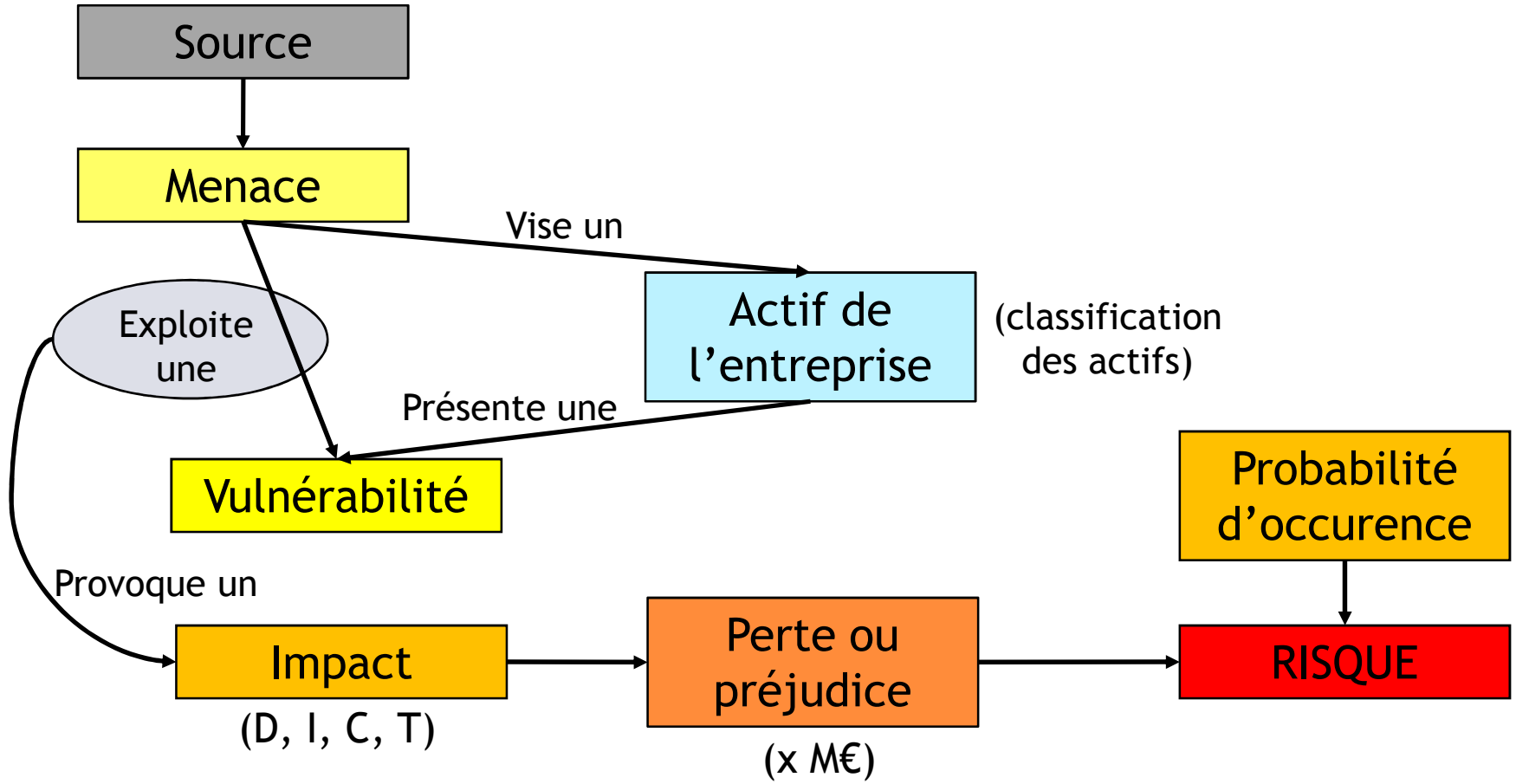
Les risques informatiques : généralités

- Les risques informatiques font partie des autres risques de l'entreprise
  - Risques juridiques, financiers, etc… (traités par ailleurs durant cette conférence)
- Les risques informatiques induisent eux-mêmes d'autres risques
  - Juridiques (CNIL), financiers (perte de CA), perte d'image de marque, perte de clients, …
- La gestion des risques informatiques est souvent déléguée par le Risk Manager au Directeur de la Sécurité ou au RSSI

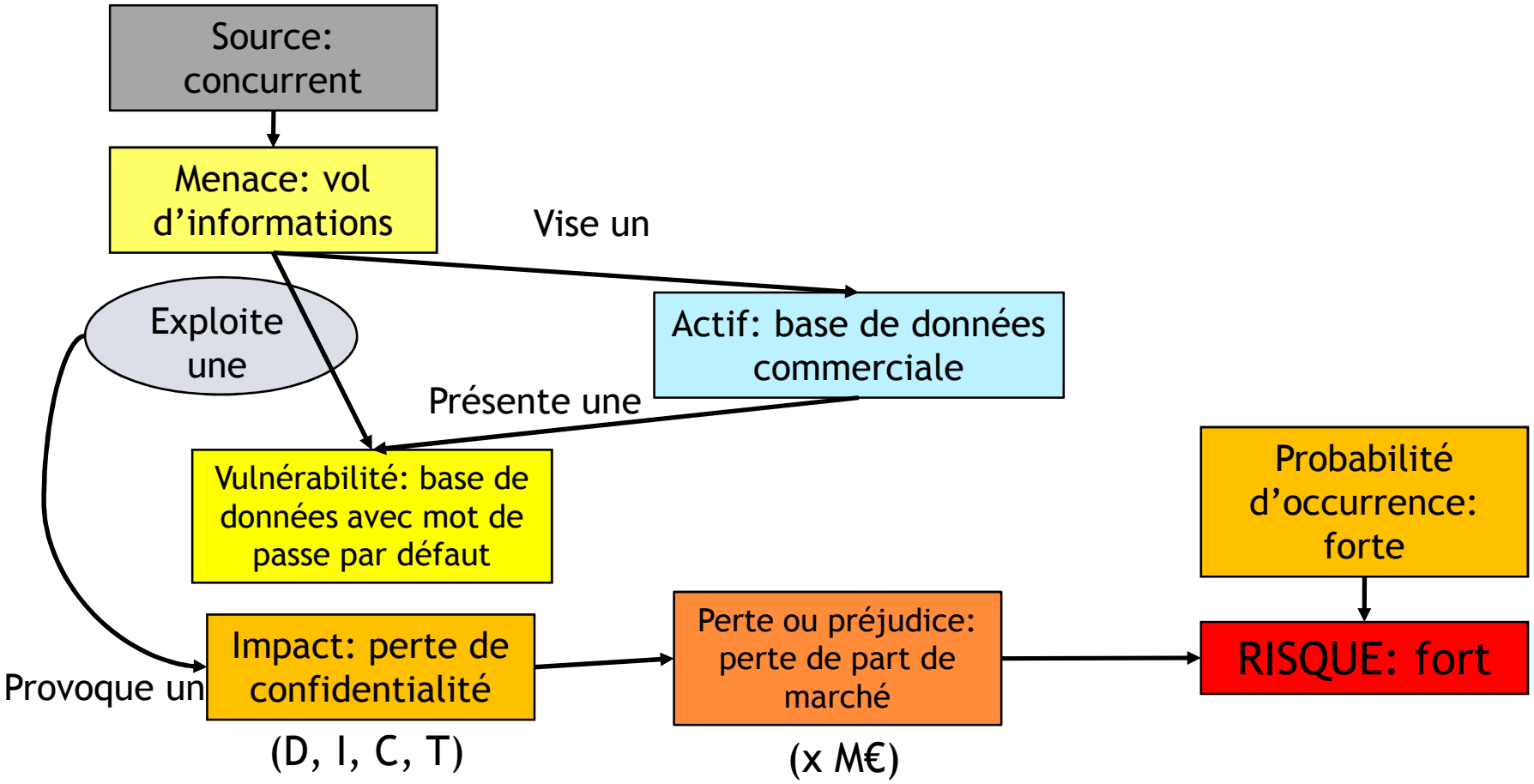
Les risques informatiques

- Risque informatique
  - Possibilité qu'une menace exploite une vulnérabilité d'un actif de l'entreprise et cause une perte ou un préjudice
- Mesuré par
  - Une probabilité d'occurrence
  - Un impact
- Niveau de risque
  - Echelle propre à l'entreprise en fonction du préjudice potentiel
  - 4, 6 ou 10 niveaux par ex.

Les risques informatiques



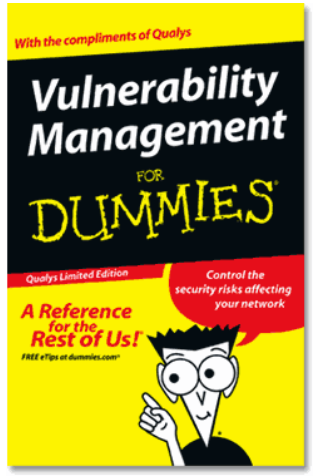
Risque informatique: exemple



Les risques informatiques

- Exemples de menaces
  - Dommage physique, panne
  - Vol, perte
  - Perte ou déni de service
    - ➔Perte d'un site Internet, d'une application critique
  - Intrusion
    - ➔Accès non autorisé au SI, en interne ou en externe
  - Divulgation de données sensibles
    - ➔Sortie de nouveaux produits, liste de clients, …

Les risques informatiques



- Exemples de vulnérabilités et de leur exploitation
  - Débordement de buffer
  - Contournement de l'authentification, vol de session, tentatives de rejeu
  - Saisie de données hostiles
    - ➔Injection SQL, Cross Site Scripting (XSS), corruption de base de données
  - Cross Site Request Forgery (CSRF)
  - Vulnérabilités des navigateurs Web
    - ➔Phishing, installation de malwares, …

Sommaire

- Les risques informatiques - vulnérabilités, menaces, impacts
- Cartographie des risques sur un Système d'Information
- Gestion et réduction des risques de sécurité sur un SI
- Protection des données sensibles

Cartographie des risques

A-t-on pensé à tout ?

La mesure de protection est-elle adaptée ?

Le risque résiduel est-il acceptable ?

Cartographie des risques informatiques

- Il existe des méthodes d'analyse spécialisées pour les risques informatiques
  - MARION (Méthode d'Analyse de Risques Informatiques Optimisée par Niveau), du CLUSIF
  - MEHARI (MEthode Harmonisée d'Analyse des Risques), du CLUSIF
    - ➔ http://www.clusif.fr
    - ➔ http://mehari.info
  - EBIOS (Expression des Besoins et Identification des Objectifs de Sécurité), de l'ANSI (ex-DCSSI)
    - ➔ http://www.ssi.gouv.fr/site_article45.html
  - Critères Communs
    - ➔ http://www.commoncriteriaportal.org

Les normes ISO

Organisation internationale de normalisation

- ISO 31000: Management du risque - Principes et lignes directrices
  - Principes généraux de management du risque
  - Peut s'appliquer à tout type de risque

- ISO 27000
  - S’applique aux Systèmes de Management de la Sécurité de l’Information
  - ISO27000 : norme "chapeau" sur la sécurité de l'information
  - ISO27001 : mise en œuvre d’un SMSI

Les normes ISO

Organisation internationale de normalisation

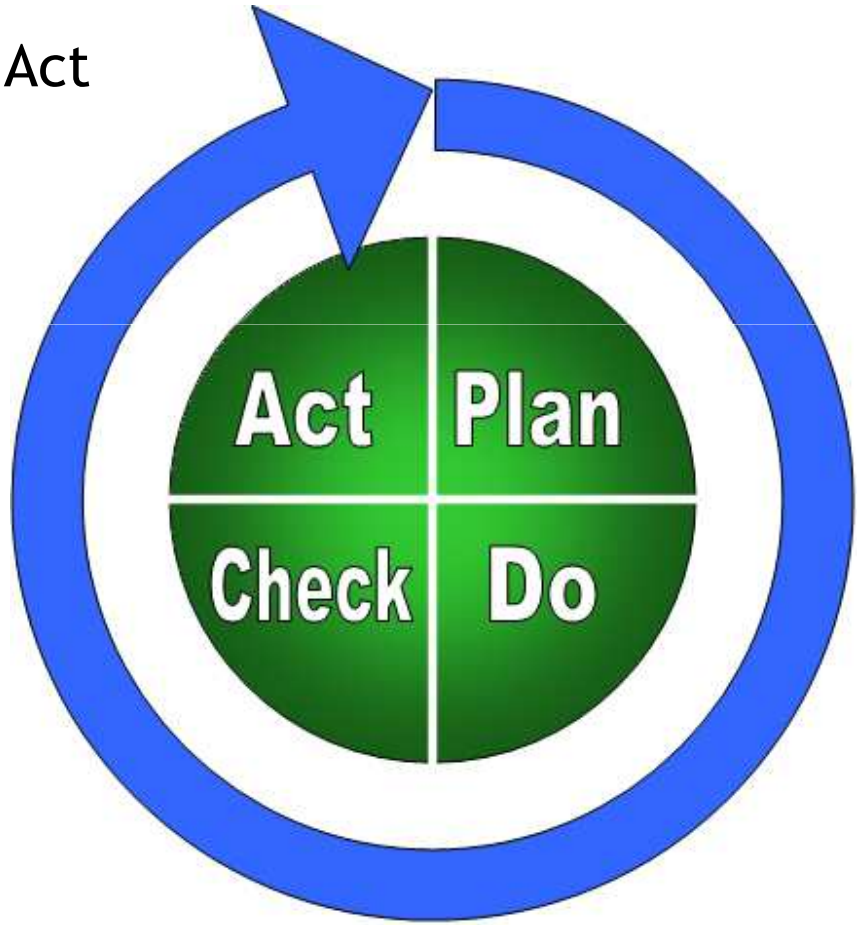
- ISO 27000 (suite)
  - ISO27002 : bonnes pratiques de sécurité informatique
  - ISO27003 : implémentation d'un SMSI
  - ISO27004 : métriques de sécurité (tableaux de bord de la Sécurité des Systèmes d'Information)
  - ISO27005 : analyse de risques
  - ISO27006 : critères d'accréditation des certificateurs

Sommaire

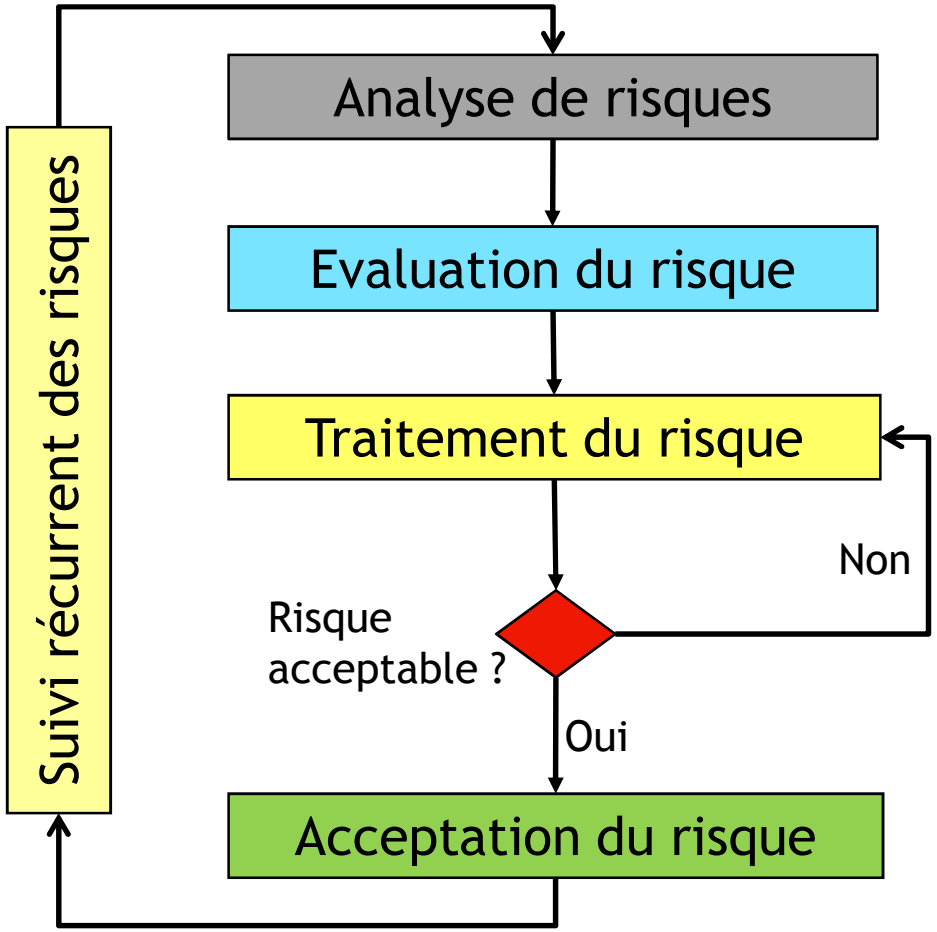
- Les risques informatiques - vulnérabilités, menaces, impacts
- Cartographie des risques sur un Système d'Information
- Gestion et réduction des risques de sécurité sur un SI
- Protection des données sensibles

Processus de gestion des risques

- PDCA: Plan, Do, Check, Act
- Amélioration continue (roue de Deming)
  ➔ Cf ISO 27001



Processus de gestion des risques de sécurité (simplifié)



- Traitement du risque:
  - Refus du risque

  Ou
  - Transfert du risque

  Ou
  - Réduction du risque

  Ou
  - Maintien du risque

Traitement du risque

- Refus du risque
  - On décide de ne pas faire l'activité à risque
- Transfert du risque
  - On assure le risque par ex.
- Réduction du risque
  - On met en place des mesures de sécurité
- Maintien du risque
  - On ne fait rien et on accepte les impacts tels quels si le risque se concrétise

Réduction des risques informatiques

- Critères de sécurité: DICT
  - Disponibilité
  - Intégrité
  - Confidentialité
  - Traçabilité (imputabilité)

- Intégrité: OK
- Disponibilité: non ! (vol)

➔ Mauvais choix de mesure de sécurité

Réduction des risques informatiques

- Grands principes de sécurisation
  - Identification
  - Authentification
  - Habilitation
  - Contrôle d'accès
  - Traçabilité

Réduction des risques informatiques

- Grands principes de protection d'un SI
  - Continuité d'activité (PCA, PRA)
  - Sécurité périmétrique
    - ➔ Filtrage réseau, firewalls, DMZ, protection de l'accès Internet de l'entreprise, anti-spam et anti-virus de messagerie, VPN et accès nomades
  - Défense en profondeur
    - ➔ Segmentation en espaces de confiance internes, gestion des identités et des habilitations, authentification et contrôle d'accès aux ressources, suivi des mises à jour de sécurité, protection des postes de travail, anti-virus et anti-malwares, chiffrement des données sensibles
  - Supervision / détection
    - ➔ Traces, logs, détection d'intrusion, scanners de vulnérabilités, tableaux de bord, suivi des risques

Sommaire

- Les risques informatiques - vulnérabilités, menaces, impacts
- Cartographie des risques sur un Système d'Information
- Gestion et réduction des risques de sécurité sur un SI
- Protection des données sensibles

Protection des données

- Les données qui transitent ou qui sont stockées dans le SI constituent le cœur du business de l'entreprise

- La protection des données et de l'information en général devient donc de plus en plus critique
  - Risques légaux (CNIL)
  - Risques d'image de marque (divulgation de données clients)
  - Risques concurrentiels (divulgation d'un business plan)

Les données sensibles

- Données personnelles
  - Clients, collaborateurs, partenaires
- Données financières
  - N° de CB, RIB, virements
- Données business
  - Produits, offres, tarifs, investisseurs
- Données techniques
  - Architecture réseau, liste de machines, plans de nommage, annuaires de comptes, mots de passe

Protection des données

- Mesures de protection des données
  - Habilitation et contrôle d'accès fin
    - ➔Données accessibles en fonction des profils utilisateurs
  - Chiffrement des données dans les bases de données
    - ➔Ex: Oracle TDE
  - Chiffrement des flux réseau
    - ➔Ex sur Internet: HTTPS
    - ➔Attention: le chiffrement ne protège pas contre les intrusions !
  - Traçabilité des accès aux données
    - ➔Ex: qui a accédé à un dossier client
  - Intégration de la sécurité dans les projets informatiques

La sécurité dans les projets

- La sécurité doit être intégrée en standard dans les projets informatiques dès le départ
  - Dès la rédaction des Expressions de Besoins par les MOA
  - Lors de la conception du système ou de l'application
    - ➔Intégrer les bonnes pratiques dans les normes de sécurité des développements informatiques de l'entreprise
  - Lors de l'implémentation / codage
  - Tests de sécurité du produit en fin de projet
  - Audits de sécurité réguliers durant la vie de l'applicatif

La traçabilité sur un SI

- Les actions effectuées sur le SI doivent être tracées
  - C'est parfois une obligation légale
    - ➔ Ex: accès Internet pour un FAI
  - Sinon, cela permet de se couvrir en cas d'enquête
- Informations à enregistrer
  - Utilisateur
  - Action effectuée
  - Données sensibles manipulées
- Gestion de journaux d'événements / de logs
  - Générer des logs (systèmes, bases de données, applications)
  - Collecter et centraliser
  - Analyser et détecter les incidents
  - Produire des indicateurs

Conclusion

- La gestion des risques informatiques s'intègre à la gestion globale des risques de l'entreprise
- L'évaluation et la réduction des risques nécessite une expertise en sécurité informatique
- La protection des données est essentielle et souvent une obligation légale
- Cela implique la prise en compte de la sécurité dans les projets informatiques
- Un grand nombre d'acteurs sont impliqués, de bout en bout des processus de l'entreprise

Pour aller plus loin…

- Norme ISO 31000
  - http://www.iso.org/iso/fr/catalogue_detail.htm?csnumber=43170
- Normes ISO 27000
  - http://www.27000.org
- Portail de la sécurité informatique
  - http://www.securite-informatique.gouv.fr
- CLUSIF
  - http://www.clusif.asso.fr
- OSSIR
  - http://www.ossir.org
- Top Cyber Security Risks
  - http://www.sans.org/top-cyber-security-risks/
- Risques sur les sites et applications Web
  - http://www.chambet.com/publications/sec-web-apps/

Questions ?