Numérique et sciences de l'information

Tous niveaux
Module No 10

Un enjeu majeur, la cybersécurité. Première partie

“So cyberspace is real. And so are the risks that come with it.”

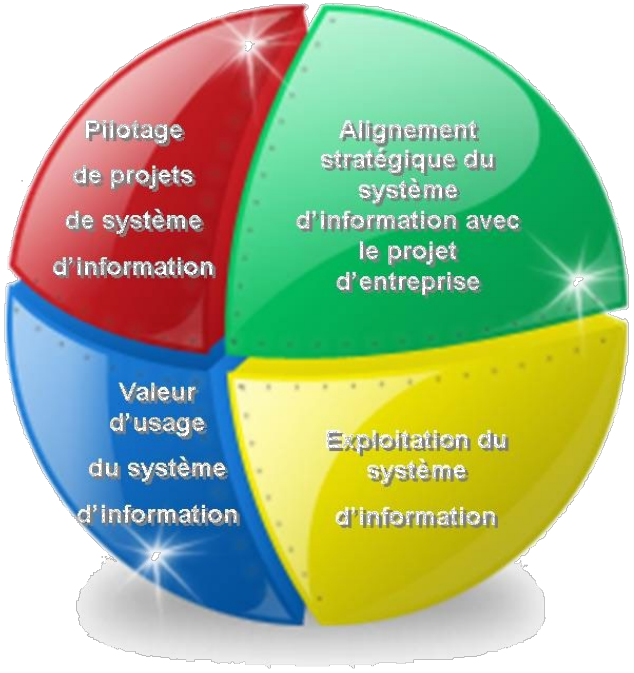
La cybermenace est l'un des plus sérieux défis auxquels nous soyons confrontés en tant que nation

Mai 2009.

Barack Obama
Président des Etats-Unis

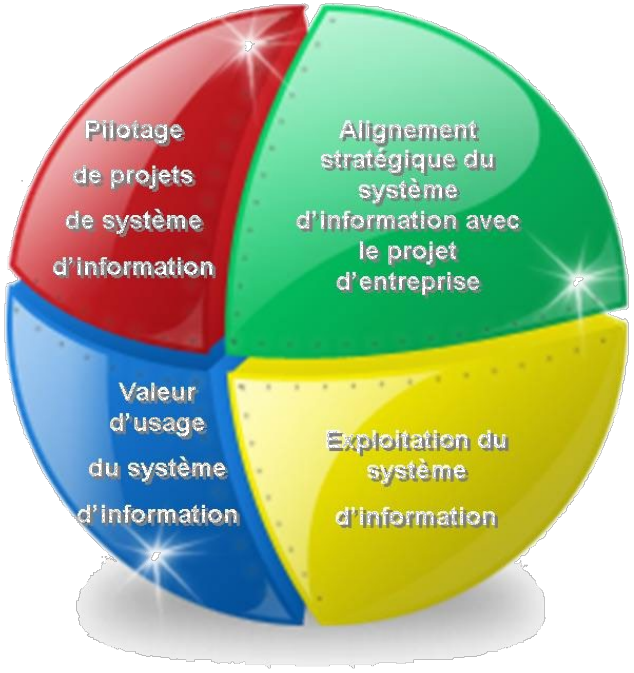
Introduction

- Puisque le SI devient vital pour les entreprises, tout ce qui le menace est potentiellement mortel.
- Ces **menaces** peuvent être très diverses : atteinte à la disponibilité des systèmes et des données, destruction, corruption ou falsification de données, espionnage, vol ou usage illicite de ressources, usage d'un système compromis pour attaquer d'autres sources.
- Les menaces exploitent les **vulnérabilités** et engendrent des **risques** qui eux-mêmes peuvent être générateurs de coûts humains et financiers : perte de confidentialité de donnés sensibles, indisponibilité des infrastructures, paralysie des processus, etc.



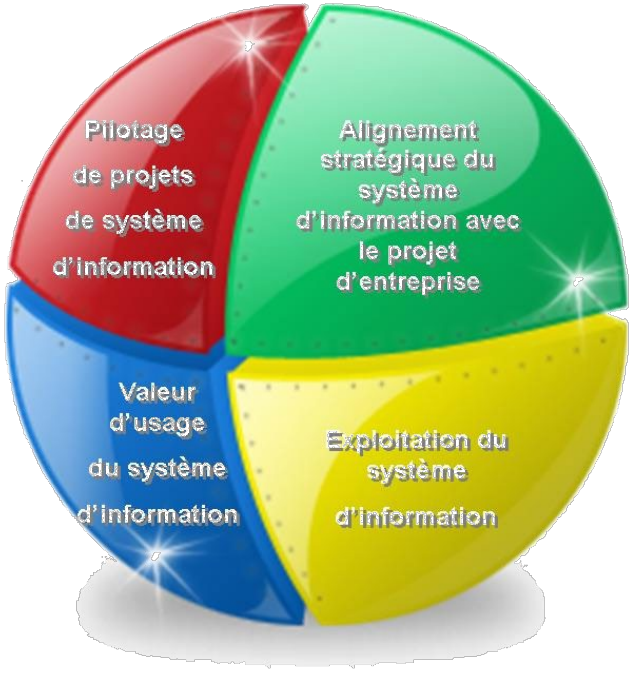
Introduction

- L'activité industrielle et commerciale est par nature risquée. Certains risques, **endogènes**, sont dans la nature même du business : développer un nouveau produit, choisir une stratégie de prix, s'engager avec un partenaire.
- D'autres sont **exogènes** et ne sont que facteurs de perturbation pour le bon déroulement des affaires : panne d'un équipement, mauvaises conditions météo, incendie, inondation, acte terroriste, ..
- L'effet de tels évènements est accentué par les nouvelles pratiques de gestion qui privilégient l'interdépendance et la minimisation des sécurités spatiales (stocks) et temporelles (délais) : production « just-in-time », supply chain aux flux tendus, ...



Introduction

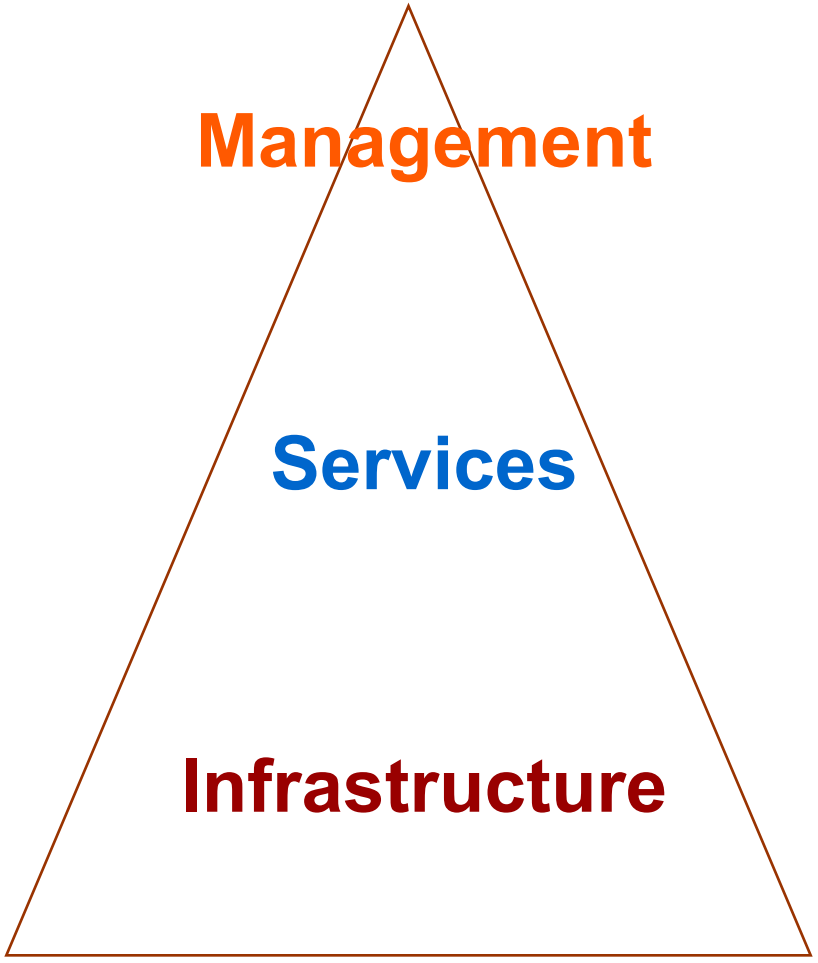
- Ces réductions ont été rendues possibles par la capacité à disposer d'information accessibles en permanence et actualisées en temps réel.
- La fiabilité du Système d'Information est donc devenue un élément clef.
- Ce système est composé d'éléments physiques matériels et humains ainsi que d'éléments logiques, donc de composants vulnérables aux dangers que nous évoquions plus haut.



Quelques questions

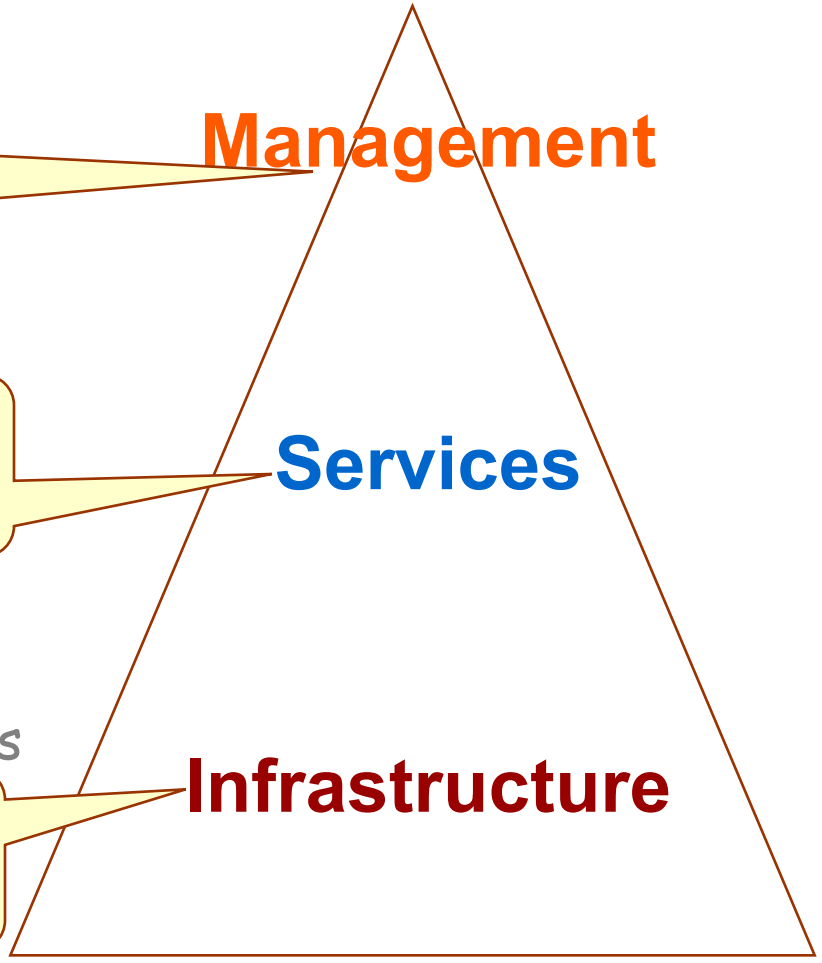
Un découpage en trois niveaux

- ✓ Piloter l'ensemble
- ✓ Organiser ces fonctions en un ensemble cohérent de services
- ✓ Mettre en place les moyens techniques nécessaires pour assurer les fonctions de collecte, stockage, traitement et communication des informations nécessaires à la bonne marche de l'organisation.



Situer le souci de sécurité

- ✓ *Sensibiliser les individus à la sécurité*
- ✓ *Sécurité logique des processus*
- ✓ Mettre en place les moyens techniques pour assurer les fonctions
  Sécurité physique des installations
  l'organisation.



Objectifs généraux

Ce module a pour objectif de sensibiliser les informaticiens et les utilisateurs à la problématique de la sécurité des systèmes d'information.

Objectifs pédagogiques

- A la fin de la formation, chaque participant devra :
  - avoir recensé les principaux risques pesant sur le bon fonctionnement d'un système d'information ;
  - avoir identifié les différents modes d'actions envisageables pour réduire les risques, atténuer leur impact et remédier à leurs conséquences.

Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Agenda

- ***A. Les principes et les enjeux***
  - ***C01 Aspects et enjeux de la sécurité***
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - *C04 Sécurité et commerce électronique. Sécurité et banqueSécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse.*
  - *C06 Architectures de sécurité*
  - *C07 Renforcer la sécurité des réseaux et des systèmes*
  - *C08 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C09 Renforcer la sécurité des applications et des services*
  - *C10 Renforcer la sécurité des dispositifs mobiles*
  - *C11 Evaluer la sécurité*
  - *C12 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- **A. Les principes et les enjeux**
  - **C01 Aspects et enjeux de la sécurité**
    - **Définitions.**
    - *Divers aspects de la sécurité. Typologie des risques. Exemples dans chaque catégorie de la typologie : nature, attaquants (menaces), impact.*
    - *Une remise en cause face à de nouvelles menaces*
    - *Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.*
    - *Recenser les actifs à protéger.*
    - *Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)*
    - *Etude de cas : Evaluation du RMT.*

Aspects de la sécurité

Définitions : Risque, menace, vulnérabilité

Définitions

Définitions : Sécurité

- Propriété d'un système d'information de présenter pour son environnement comme pour lui-même des risques directs ou indirects acceptables, déterminés en fonction des dangers potentiels (menaces) inhérents à sa réalisation et à son utilisation.
- La **sécurité informatique** concerne principalement la sécurité :
  - Du matériel
  - Des logiciels
  - Des données (lors du stockage, lors du traitement, lors de la transmission)
  - Des utilisateurs

Aspects de la sécurité

Définitions : Risque, menace, vulnérabilité

- **Risque**
- Danger ou inconvénient plus ou moins probable auquel on est exposé (Exemple : perte de fichier)
- *Risque = probabilité d'occurrence * préjudice*
- Panne de disque dur : préjudice minime si sauvegardes régulières et probabilité élevée => risque acceptable
- Chute météorite : fort préjudice mais probabilité faible => risque acceptable
- Panne de disque dur : préjudice élevé si pas de mesure prévention et probabilité élevée => risque inacceptable

Aspects de la sécurité

Définitions : Risque, menace, vulnérabilité

- **Menace**
- Personne, signe ou indice qui laisse prévoir un danger (Exemple : pirate informatique)

- **Vulnérabilité**
- Point faible ou défectueux qui donne prise à une attaque

Aspects de la sécurité

Définitions : Périmètre et politique de sécurité

- **Périmètre de sécurité**
- Inutile de se préoccuper de sécurité sans avoir défini ce qui doit être protégé.
- Le périmètre définit les limites et recense les actifs à protéger (serveur, programme, données, etc.).
- **Politique de sécurité**
- Une fois le périmètre fixé, il faut élaborer une politique de sécurité, c'est à dire définir ce qui est autorisé et ce qui est interdit.
- A cette politique s'ajoutent les lois et règlements en vigueur, tout en sachant qu'il est parfois difficile de les appliquer : comment appliquer une loi sur un serveur virtualisé qui peut se déplacer de pays en pays, au gré des serveurs physiques qui le l'hébergent.

Définitions : Identifier et authentifier

- **Identification et authentification**
- Les individus qui accèdent à un actif informatique doivent s'identifier, par le bais d'un code d'identification (*user id*)
- Cette identité doit ensuite être authentifiée, âr exemple à l'aide d'un mot de passe ou d'un processus beaucoup plus sécurisé (biométrique par exemple)
- Les procédures d'identification et d'authentification des utilisateurs sont un corollaire à toute stratégie de protection.
- Bien administrer les entités pour éviter les usurpations.
- Les utilisateurs doivent s'approprier facilement le système d'identification.

Définitions : habiliter

- **Droits d'accès et habilitation**
- Une fois l'utilisateur identifié et authentifié, ses droits d'accès (accès partiel, accès total, mise à jour, ..) doivent être vérifiés en regard de ses habilitations.
- La **séparation des privilèges** consiste à attribuer à chaque utilisateur, ou à chaque activité du système, les privilèges ont il a besoin;
- **... Et pas d'autres !**
- C'est le principe du **privilège minimum**.

Définitions : Chiffrer

- **Chiffrement**
- La sécurité des accès par le réseau à une ressource protégée n'est pas suffisamment garantie par la seule identification des accédants.
- Sur un réseau local de type Ethernet ou wifi où la circulation des données fonctionne selon le modèle d'une émission que tout le monde peut capter, il est possible à un tiers de l'intercepter.
- Sur Internet, les données circulent à la manière d'une carte postale que peuvent lire le facteur et le concierge.
- Dés lors que les données doivent être protégées, il faut faire appel au chiffrement pour rendre les données illisibles à ceux qui n'ont pas l'autorisation, donc la clef pour les rendre lisibles.

Définitions : Chiffrer

- **Chiffrement et authentification**
- Chiffrement et authentification sont indissociables.
- Chiffrer sans authentifier ne protège pas des usurpations d'identité.
- Authentifier sans chiffrer laisse la porte ouverte au vol de données.

Définitions : Intrusions

- Chiffrement et authentification ne suffisent pas.
- Il faut aussi se prémunir contre les intrusions destinées à détruire ou corrompre les données, ou a rendre l'accès impossible.
- Les techniques pour ce faire sont l'usage des **pare-feux** (*firewalls*) et le **filtrage** des communications réseau.
- Les machines qui doivent être accessibles au public sont réunies dans une **zone démilitarisée** (*DMZ*), isolée du réseau intérieur.
- Les machines de la DMZ exposée aux attaques venues de l'Internet sont des **bastions**.
- Cette défense peut être renforcée par des **systèmes de détection d'intrusion** (*IDS*), voire par des **systèmes de prévention d'intrusion** (*IPS*).

Plan

➔ A. Les principes et les enjeux

- *C01 Aspects et enjeux de la sécurité*
  - *Définitions.*
  - ***Divers aspects de la sécurité. Typologie des risques. Exemples dans chaque catégorie de la typologie : nature, attaquants (menaces), impact.***
  - *Une remise en cause face à de nouvelles menaces*
  - *Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.*
  - *Recenser les actifs à protéger.*
  - *Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)*
  - *Etude de cas : Evaluation du RMT.*

Aspects de la sécurité

Divers aspects de la sécurité

Actions envisageables

- Notre introduction fait état de **risques endogènes** et de **risques exogènes**.
- Une organisation peut traiter ses risques endogènes de manière exhaustive.
- Le choix est guidé par le coût de diminution du risque face aux effets potentiel du risque.
- Son action est par contre limitée en ce qui concerne les risques exogènes.
- Elle ne peut influer sur les causes.
- Elle peut seulement en diminuer les effets :
  - en essayant d ’y échapper,
  - en atténuant leur impact,
  - en remédiant à leurs conséquences.

Typologie

- Un autre mode de classement des risques repose sur leur nature :

- **Les accidents**
  - Accidents physiques
  - Pannes
  - Force majeure
  - Pertes de services essentiels
- **Les erreurs**
  - Erreurs à la conception
  - Erreurs à la réalisation
  - Erreurs à l'utilisation

- **La malveillance**
  - Vols et vandalisme;
  - Fraude
  - Sabotage
  - Attaques logiques
  - Divulgations
  - Autres

Typologie

- **Les accidents**
  - Accidents physiques
  - Pannes et dysfonctionnements
  - Force majeure
  - Pertes de services essentiels

Accidents physiques

A1 - Incendie, explosion, implosion, dégâts des eaux, bris de machine

Banque *: Incendie d'un centre informatique de traitement de chèques. Ce centre disposait d'un contrat de télé-back-up avec une société de services, mais il avait été insuffisamment testé, notamment au plan des télécommunications.*

La chaîne n'a pu fonctionner à nouveau - en mode très dégradé - que vingt jours après le sinistre.

Le dommage matériel (essentiellement dû aux fumées et au gaz de décomposition du gaz extincteur) est évalué à près de 200 k€, tandis que les pertes indirectes sont évaluées à plus de 2 M€.

Pannes et dysfonctionnements

A2 - Pannes (matérielles et logiques) : Il s'agit de l'ensemble des causes d'origine ou de révélation interne entraînant l'indisponibilité ou le dysfonctionnement (non conformité aux fonctionnalités et performances nominales) total ou partiel du système.

Services *: Hyperdessication de l'atmosphère de la salle ordinateurs due à une défaillance de la climatisation (report d'alarme défectueux) : la température s'élève à plus de 60° C.*

Le constructeur estime que le matériel est irréversiblement endommagé et refuse toute maintenance en cas de sauvetage partiel.

Les données sont également endommagées et les sauvegardes partielles ne permettront pas de tout récupérer. Pertes matériels et frais : environ 8 M€, autres pertes évaluées à plus de 9 M€.

Force majeure

A3 - Evénements naturels : Il s'agit des événements naturels d'origine externe au système : inondation, tempête, cyclone, ouragan, vent, poids de la neige sur les toitures, foudre, grêle, avalanche, coulée de boue, glissement de terrain, phénomènes sismiques et volcaniques, etc.

Banque *: Dégâts des eaux dans les locaux techniques de l'informatique suite à une inondation "catastrophique naturelle".*

Le matériel endommagé est évalué à près de 1 M€ , les frais supplémentaires à 600 k€ et les pertes d'exploitation à près de 2 M€ (arrêt d'une semaine).

Perte de services essentiels

A4 - Perte de services essentiels : Il s'agit de l'ensemble des causes d'origine externe entraînant l'indisponibilité ou le dysfonctionnement (non conformité aux fonctionnalités et performances nominales) total ou partiel du système :

. électricité, télécommunications, eau,

. fluides divers,

. fournitures spécifiques.

Diverses activités *: L'explosion d'une centrale thermique en région parisienne, produisant également de l'eau glacée pour le refroidissement d'une centaine de systèmes, a privé ceux-ci de climatisation pendant plusieurs semaines, entraînant des arrêts de fonctionnement dont le total des conséquences approche 8 M€.*

Aspects de la sécurité

Typologie

- **Les erreurs**
  - Erreurs à l'utilisation
  - Erreurs à la conception
  - Erreurs à la réalisation

Aspects de la sécurité

Erreurs d'utilisation

E1 - Erreurs d'utilisation : Erreurs de saisie et transmission des données quel qu'en soit le moyen, erreurs d'exploitation du système.

Assurance *: Erreurs de transmission en chaîne, pendant plusieurs semaines, sans détection, de la télésauvegarde des fichiers de base. C'est essentiellement le fichier des contrats automobiles qui a été touché.*

Sa reconstitution a pu être faire à partir d'une sauvegarde ancienne (trois mois) à haute protection et de la collecte d'informations complémentaires (qui a duré deux mois).

La perte d'exploitation due au retard de quittancement est de plus de 600 k€ .

Erreurs de conception et de réalisation

E2-E3 - Erreurs de conception et de réalisation de logiciels et procédures d'application.

Assurance *: Erreur de conception d'un logiciel d'optimisation des placements financiers, conduisant à une perte de fonds de 3 M€ en deux mois (temps de fonctionnement avant détection de l'anomalie).*

Aspects de la sécurité

Typologie

- **La malveillance**
  - Vols et vandalisme;
  - Fraude ;
  - Sabotage;
  - Attaques logiques ;
  - Divulgations ;
  - Autres.

Aspects de la sécurité

Malveillance. Vols.

M1 - Vol de matériels principaux ou accessoires

Vandalisme sur le matériel.

Services *: Vol de matériel (la plus grande partie des micro-ordinateurs et machines de traitement de texte) dans un cabinet de services juridiques et fiscaux (CA annuel 1,2 M€) en une seule nuit : dommages matériels évalués à 80 K€ et dommages immatériels évalués à 50 k€ plus 300 k€ en responsabilité civile.*

Malveillance. Fraude.

M2 - Fraude : Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice évaluable monétairement pour la victime, essentiellement formé par le détournement de biens au profit du criminel :

- détournement de fonds (direct ou indirect),
- détournement de biens ou services matériels ou immatériels (direct ou indirect),
- les attaques ciblées vers une entreprise pour récupérer des informations ou modifier des dispositifs en vue d'opérer ultérieurement une autre opération malveillante (par exemple de type M4).

Aspects de la sécurité

Malveillance. Fraude.

Banque *: Un cadre ayant autrefois travaillé au service informatique, entre sur écran une série d'écritures, dont le compte d'origine est "Réserves" et le compte d'aboutissement est un numéro de compte personnel dans une banque étrangère.*

Les opérations sur réserves sont rejetées en anomalies dans un fichier d'attente, afin d'être ultérieurement recyclées.

Le fraudeur utilise alors une chaîne de recyclage batch, normalement employée en mode dégradé dans le cadre du plan de secours.

Cette chaîne, ancienne, n'est pas à jour, et les écritures passent. Ce n'est que le lendemain, lors du contrôle quotidien, que l'anomalie est identifiée.

Les mouvements de fonds ont déjà été réalisés pour 1,15 M€.

Aspects de la sécurité

Malveillance. Fraude.

Industrie : *Modification des programmes de facturation de quelques gros clients en deux temps : mise à zéro du prix de certains produits sur la première facture ; puis envoi d'une seconde facture (non comptabilisée), avec la mention "régularisation par virement au compte..." portant sur les produits facturés zéro.*

Le compte "produits à facturer" était soldé par la première facture. La différence était récupérée sur le compte de l'informaticien fraudeur.

La fraude a été stoppée à la quatrième facture, pour un montant de 530 k€ .

Aspects de la sécurité

Malveillance. Sabotage.

M3 - Sabotage : Attentat, vandalisme, action malveillante conduisant à un sinistre matériel (type A1 ou A2).

Banque *: Sabotage physique d'une trieuse de chèques très spécialisée (760 k€).*

Le retard de traitement (transfert vers un centre régional) a entraîné environ 300 k€ de pertes supplémentaires.

Le budget informatique annuel de cette banque est de l'ordre de 50 M€.

Aspects de la sécurité

Malveillance. Attaque logique.

M4 - Attaque logique : Utilisation non autorisée des ressources du système d'information, conduisant à un préjudice au moins qualitatif pour la victime, se traduisant essentiellement par une perte d'intégrité et/ou de disponibilité, entraînant le plus souvent un profit indirect pour le criminel et/ou le commanditaire éventuel (sabotage immatériel, infection informatique, programme "simple", bombe logique, cheval de Troie, sabotage "manuel", programme auto-reproducteur, ver, virus (système ou programme)).

Cette rubrique se subdivise en deux catégories :

- les attaques non ciblées (comme les virus) qui représentent l'immense majorité des attaques en nombre, mais avec un impact modéré,
- les attaques ciblées vers une entreprise (bombe logique, manipulation de données ou de programmes, etc.) dans le but de la paralyser au moins momentanément. Ces attaques sont très peu nombreuses, mais leur impact est très élevé.

Aspects de la sécurité

Malveillance. Attaque logique.

Organisme de crédit *: Destruction de tous les fichiers et tous les programmes, ainsi que des sauvegardes d'une mutuelle.*

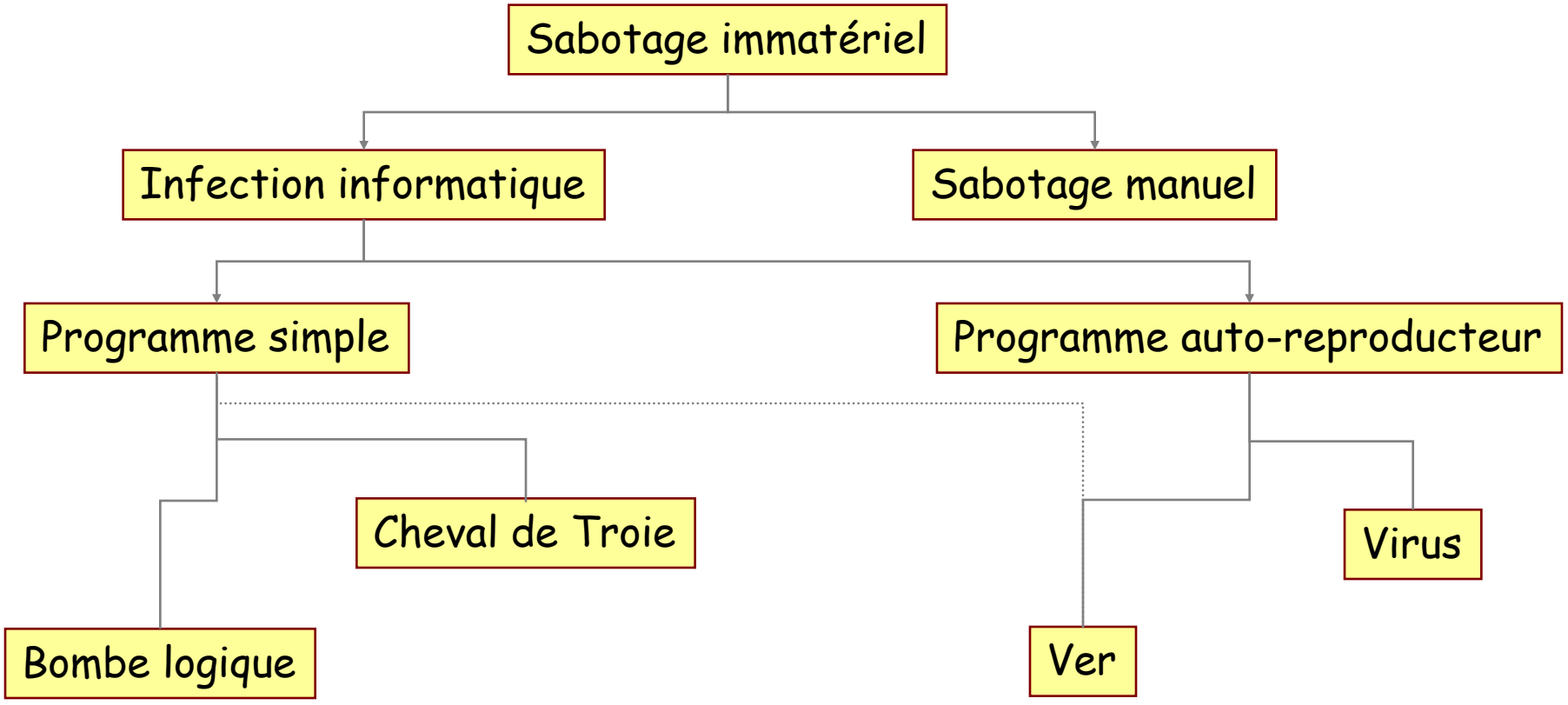
La reconstitution des données faite à partir des archives et d'un appel aux sociétaires a coûté 3 M€.

La reconstitution des programmes, qui a duré onze mois, a coûté 11,5 M€ .

Les autres frais supplémentaires, pertes d'exploitation et pertes de clientèle sont estimés à environ 24 M€.

Aspects de la sécurité

Malveillance. Attaque logique.



Aspects de la sécurité

Malveillance. Attaque logique.

Virus : Un virus est un programme qui se réplique en s'attachant à d'autres programmes.

Le programme infecté doit être lancé pour que le virus agisse.

Le virus peut alors se contenter de se reproduire ou faire des dégâts en effectuant immédiatement une action nuisible.

Un virus peut être programmé en y intégrant une bombe pour exécuter son action nuisible à une date précise, ou lorsqu'une certaine logique est activée dans le programme hôte .

Aspects de la sécurité

Malveillance. Attaque logique.

Ver : Un ver est un programme qui propage des copies de lui-même à travers un réseau ou sur Internet sans le support d'un programme hôte.

Un ver engendre une surcharge du réseau car il se répète rapidement.

Dans une machine, un ver fait des dégâts par sa seule présence, plutôt que par l'exécution d'une action nuisible spécifique, comme le fait un virus.

Le ver surcharge la mémoire ou le disque dur en se répliquant à de nombreuses reprises.

Quand un ver se propage sur l'Internet, il peut faire des dégâts tels que les envois en masse d'e-mails.

Aspects de la sécurité

Malveillance. Attaque logique.

- Il y a quinze ans, les virus n'étaient pas des vers (ils ne se propageaient pas par le réseau) …
- Les vers n'étaient pas des virus (ils ne se reproduisaient pas) …
- Aujourd'hui la confusion entre les deux espèces est presque totale !

Aspects de la sécurité

Malveillance. Attaque logique.

Cheval de Troie *:* Un cheval de Troie est un troisième type d'infection informatique qui, comme un ver, n'a pas besoin d'un programme hôte pour agir, mais, de plus, il prend l'apparence d'un programme légitime.

La plupart des chevaux de Troie ne peuvent pas se reproduire, bien qu'il existe quelques exceptions.

Un programme de ce type prenait l'apparence d'un utilitaire de sauvegarde automatique téléchargeable sur l'Internet.

Lorsqu'il était utilisé, il créait des sauvegardes et s'auto-répliquait dans ces sauvegardes.

Il était programmé pour endommager plusieurs systèmes à une certaine date.

Dans ce cas, ce cheval de Troie peut également être considéré comme un virus en raison de sa capacité à se répliquer.

Parce que les infections à base de chevaux de Troie ne peuvent généralement pas reproduire et parce qu'ils exigent une intervention humaine pour se déplacer d'un endroit à l'autre, ils ne sont pas aussi communs que les virus.

Aspects de la sécurité

Malveillance. Attaque logique.

Bombe logique : Une bombe logique est un code dormant ajouté à un logiciel, et déclenché à un moment prédéterminé ou lors d'un événement prédéterminé.

Par exemple, un employé peut mettre du code dans un programme pour détruire des fichiers importants si son nom est retiré de la liste de paie.

Aussi, les virus, chevaux de Troie, bombes logiques, et les vers peuvent se combiner, par exemple quand un virus obtient l'autorisation d'accès à un réseau par le biais d'un cheval de Troie.

Le virus peut implanter une bombe logique dans un logiciel d'application sur le réseau qui active un ver lorsque l'application s'exécute.

Malveillance. Attaque logique.

Le virus/ver Conflicker

L'épidémie Conflicker (depuis 2008) est la plus grave depuis Slammer.

Il aurait infecté entre 3 000 000 et 9 000 000 d'ordinateurs.

Conflicker est un virus réticulaire (bot) c.a.d. un virus qui se propage silencieusement sur des millions d'ordinateurs, éventuellement sans commettre le moindre dégât.

Puis, à un signal donné, ou à une date fixée, ces millions de machines vont constituer un réseau (botnet) et se connecter à un même serveur web pour provoquer son effondrement (DDoS).

Conflicker exploite une vulnérabilité connue et corrigée de Windows.

Conflicker désactive les services comme les mises à jour automatiques (pour éviter les correctifs de l'OS et de l'antivirus); le contrôle de sécurité et la journalisation des erreurs.

Conflicker communique avec son maître au moyen du protocole RPC pour recevoir ses propres mises à jour, des listes d'actions à efectuer, des informations collectée dans la machine.

Les virus classiques travaillaient avec les adresses IP. Conflicker innove en utilisant les DNS, c.a.d. en créant ou en usurpant des milliers de noms de domaine.

Aspects de la sécurité

Malveillance. Attaque logique.

Le virus Flame

Kaspersky a découvert au Proche-Orient un virus informatique décrit comme la troisième arme informatique la plus sophistiquée jamais vue au niveau mondial (après Stuxnet et Duqu).

Le virus baptisé Flame touche plusieurs milliers de PC sous Windows en Iran, en Israël et en Palestine, ainsi qu'en Amérique du Nord.

En termes de lignes de code, Flame est vingt fois plus important que Stuxnet, le virus qui avait attaqué le système informatique des centrifugeuses nucléaires iraniennes.

Kaspersky indique que ce virus peut collecter des données à distance, intervenir sur les réglages de l'ordinateur, activer certains périphériques d'un PC (micro, webcam) pour enregistrer des conversations, réaliser des captures d'écran et se connecter aux messageries instantanées.

Pour agir, il exploite les mêmes failles que Stuxnet, qui ont pourtant été comblées par Microsoft depuis.

Dans une zone où la diplomatie est très perturbée, Flame pourrait servir d'arme de déstabilisation.

Le niveau de complexité indique que seul un Etat peut être à l'origine du développement.

Aspects de la sécurité

Malveillance. Attaque logique.

Attaque de l'Elysée

En mai 2012, quelques jours avant le second tour de l'élection présidentielle, des pirates ont réussi à s'introduire dans les réseaux informatiques de l'Elysée.

Des notes secrètes et des plans stratégiques ont été récupérées sur des disques durs.

Comme souvent dans ce type d'attaque, une négligence humaine est à l'origine de la catastrophe.

Les assaillants ont d'abord identifié, sur le réseau social Facebook, le profil de personnes travaillant au palais présidentiel.

Se faisant passer pour des amis, ils les ont ensuite invitées, par un message électronique, à se connecter sur l'intranet de l'Elysée, mais ce lien menait à une fausse page Web, réplique de celle de l'Elysée.

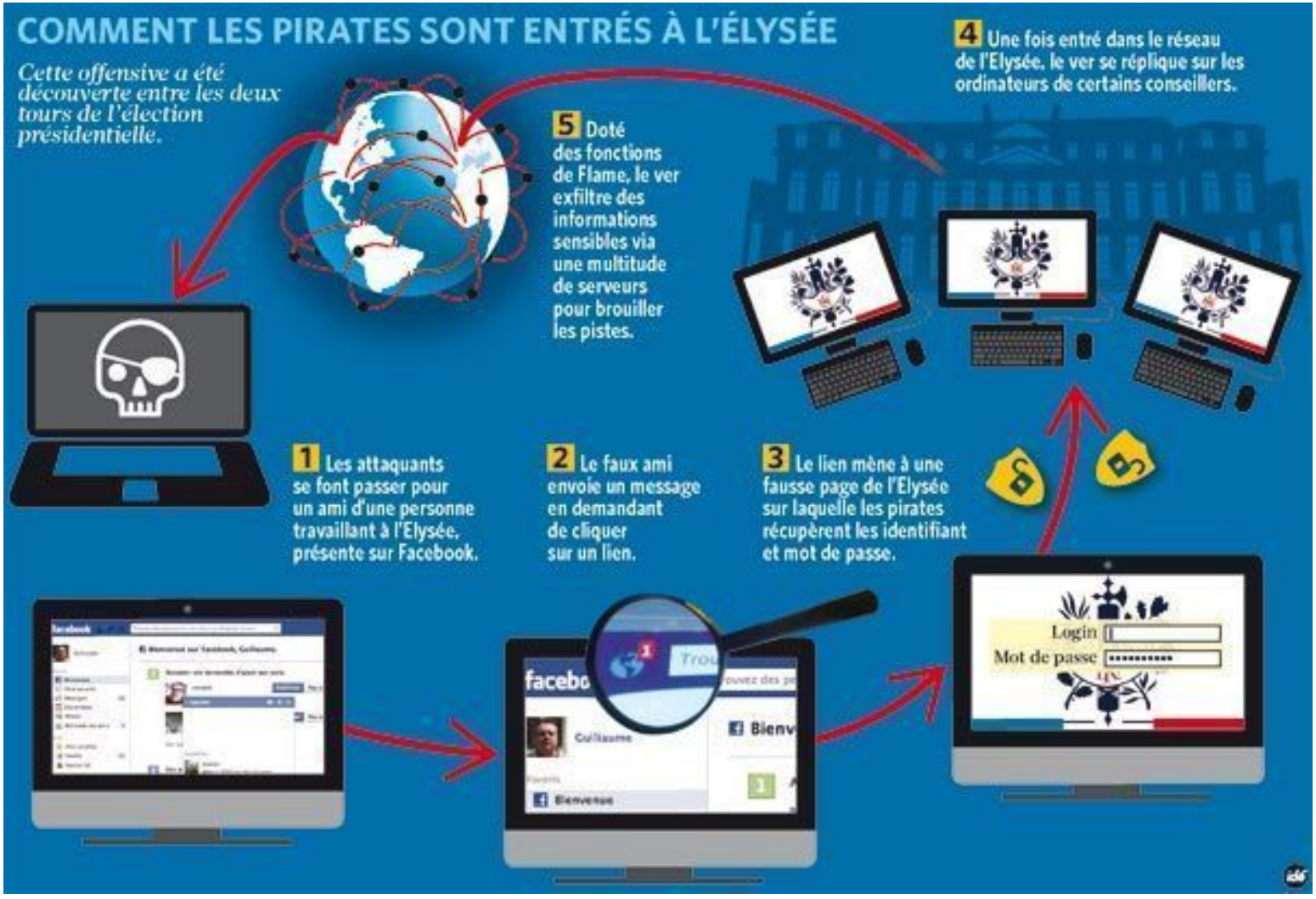
Lorsque est apparu, à l'écran, un message leur demandant leur identifiant et leur mot de passe, elles les ont donnés en toute bonne foi.

Une technique bien connue des hackers leur a permis de récupérer les clefs numériques pour se connecter en toute quiétude.

Une fois à l'intérieur, les pirates ont installé un logiciel espion basé sur Flame qui s'est propagé sur les machines des conseillers les plus influents du gouvernement et du secrétaire général, Xavier Musca.

Aspects de la sécurité

Malveillance. Attaque logique.



Aspects de la sécurité

Malveillance. Attaque logique.

Rançongiciel : *De nombreux internautes sont actuellement victimes d'un code malveillant bloquant leur ordinateur.*

Ce code affiche une page comportant notamment le logo de la Gendarmerie, de la police nationale et parfois celui de l'Office central de lutte contre la criminalité liée aux technologies de l'information et de la communication (OCLCTIC) et plus récemment celui de l'ANSSI.

Le code malveillant bloque totalement l'ordinateur infecté, en exigeant le règlement en ligne d'une somme de 70 à 100 euros.

Cette pratique, nommée "rançongiciel" (ransonware), consiste, via des bannières publicitaires, à infecter les ordinateurs ; et plus particulièrement, les ordinateurs dont les logiciels, principalement Java et Adobe Flash, ne sont pas à jour.

Aspects de la sécurité

Malveillance. Attaque logique.

Aspects de la sécurité

Malveillance. Divulgation.

M5 - Divulgation : Utilisation non autorisée des ressources du système d'information, entraînant la divulgation à des tiers d'informations confidentielles.

Aspects de la sécurité

Malveillance. Divulgation.

Distribution *: Copie du fichier fournisseur au profit d'un concurrent (collusion d'un informaticien de la société avec un concurrent).*

Ce dernier a pu obtenir des fournisseurs avec lesquels il avait de moins bonnes conditions une mise à niveau et ainsi gagner environ 0,4 point de marge.

Il a pu alors pratiquer une attaque de son concurrent sur les produits pour lesquels celui-ci était moins bien placé.

La perte en un an est estimée à près de 7 M€ et il est possible que l'entreprise ne puisse survivre (CA annuel de l'hypermarché: 60 M€).

Malveillance. Autres.

M6 - Autres : grèves, pertes ou indisponibilité de personnel, contrefaçon de progiciels, ….

Industrie *: Suite à un conflit avec la direction, départ de la presque totalité de l'équipe informatique d'un petit centre.*

Les pertes d'exploitation dues à l'impossibilité d'exploiter et de corriger les programmes par manque de documentation, même avec l'aide de personnes compétentes extérieures, ont été évaluées à plus de 300 k€ (soit le budget informatique annuel de cette entreprise).

Aspects de la sécurité

Les aspects de la sécurité

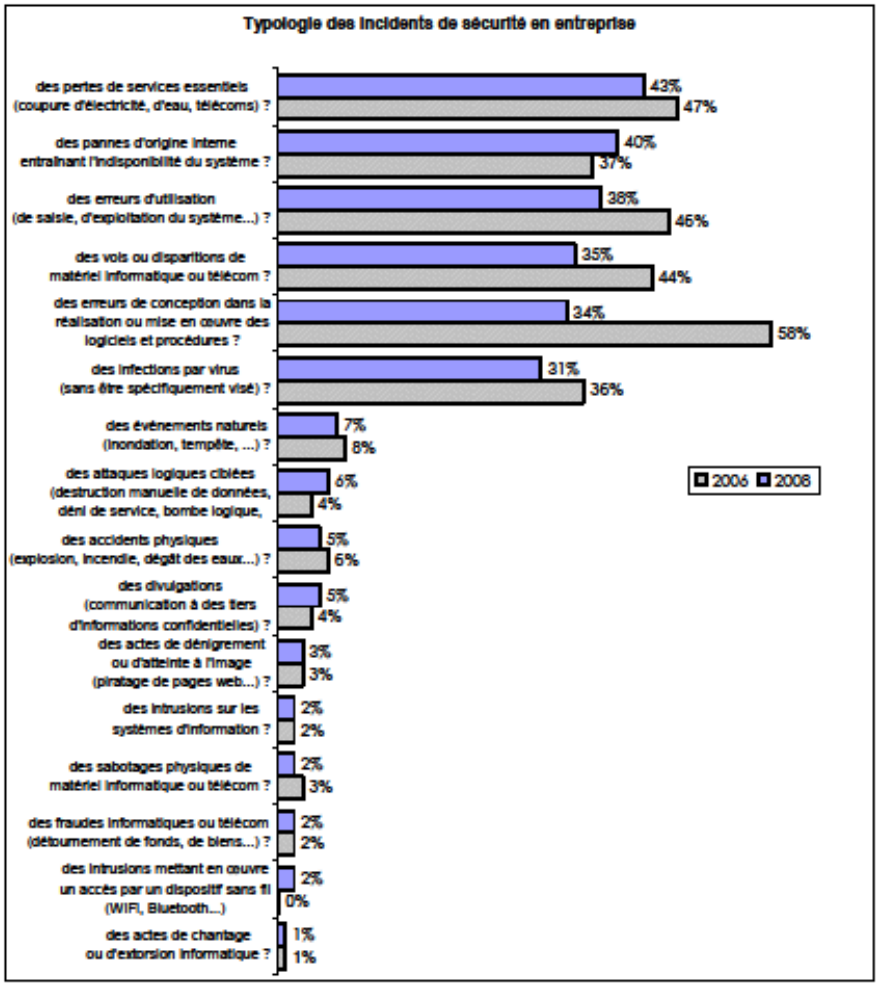


Figure 23 : typologie des incidents de sécurité en entreprise

Un exemple de répartition des causes de sinistres
Source : CLUSIF 2008

Plan

➔ A. Les principes et les enjeux

- *C01 Aspects et enjeux de la sécurité*
  - *Définitions.*
  - *Divers aspects de la sécurité. Typologie des risques. Exemples dans chaque catégorie de la typologie : nature, attaquants, impact.*
  - ***Une remise en cause face à de nouvelles menaces***
  - *Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.*
  - *Recenser les actifs à protéger.*
  - *Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)*
  - *Etude de cas : Evaluation du RMT.*

Aspects de la sécurité

De nouvelles menaces

- **De nouvelles menaces liées à de nouveaux usages :**
  - Intrusions
  - Dénis de service
  - Hameçonnage (*Phishing*)
  - Sécurité de la téléphonie mobile
  - Nouveaux risques sur IP liés à la généralisation des services
  - Ruptures de services chez les opérateurs
  - Nuages sur le « cloud computing »
  - Réseaux sociaux
  - Cartes bancaires
- **Remise en cause du concept de périmètre de sécurité.**
- **Nécessité d'une défense en profondeur.**

Intrusions

- Rappelons tout d'abord que le fait de s'introduire dans un système informatique sans y être autorisé tombe sous le coup du Code pénal (intrusions et « piratages » : articles 323-1 à -4 du Code pénal, ex-loi Godfrain).
- Pour s'introduire dans un système informatique, les intrus recherchent dans un premier temps des failles, c'est-à-dire des vulnérabilités nuisibles à la sécurité du système, dans les protocoles, les systèmes d'exploitation, les applications ou même le personnel d'une organisation !
- Les termes de vulnérabilité, de brèche ou en langage plus familier de trou de sécurité (en anglais « *security hole* ») sont également utilisés pour désigner les failles de sécurité.

Aspects de la sécurité

Intrusions

- Une fois que l'intrus a établi une cartographie du système, il est en mesure de mettre en application sa stratégie.
- Un premier accès à une machine lui permettra d'étendre son action afin de récupérer d'autres informations, et éventuellement d'étendre ses privilèges sur la machine.
- Son but ultime est d'accéder au niveau administrateur.
- L'intrus possède alors le plus haut niveau de droit sur la machine.
- La dernière étape consiste à effacer ses traces, afin d'éviter tout soupçon de la part de l'administrateur du réseau pénétré et ce de telle manière à pouvoir garder le plus longtemps possible le contrôle des machines compromises.

Dénis de services

- DDoS : *Distributed denial-of-service*"
- Le déni de service distribué est un type d'attaque très évolué visant à rendre muette une machine en la submergeant de trafic inutile en utilisant plusieurs machines à la fois.
- Exemple de l'attaque contre une administration française en mars 2009 avec 7000 « bots » impliqués.
- Parfois non lié à une malveillance (Saturation Google news lors de la mort de Michael Jackson)

Dénis de services

- L'internet et les réseaux s'entreprise reposent sur des routeurs *Cisco*
- Déni de service sur tous les équipements *Cisco* publié le 17 juillet 2003
  - Envoi de paquets dirigés vers le routeur sur certains protocoles précis de manière à ce que le paquet s'arrête sur le routeur
  - Les paquet mis dans la file d'attente n'est alors jamais traité par le routeur
  - La file d'attente se remplit après 75 paquets par défaut.
  - Le routeur n'est plus accessible et ne traite plus les paquets entrants sur cette interface.
- Concerne tous les équipements du plus petit au plus important : Les routeurs personnels comme les commutateurs ou les équipements au cœur des infrastructures des opérateurs.

Hameçonnage (*Phishing*)

- Méthode : se faire passer pour un autre.
- Objectif classique : détournement de fonds par un virement :
  - Envoi d'un message faisant croire à la victime qu'elle doit se connecter sur un site de la banque,
  - Le site n'est pas celui de la banque mais celui du pirate,
  - Le pirate récupère les informations d'identification et d'authentification,
  - Il se connecte à la banque à la place de la victime.
- La banque cible de l'attaque n'est pas directement attaquée.
- C'est le client de la banque qui est attaqué.
- Nombreux cas depuis 2004 en France.

Aspects de la sécurité

Téléphonie mobile

- Aucune sécurité sur la téléphonie mobile 2G
- A5/1 et A5/2 craqués depuis longtemps
- Récupération de la clef de chiffrement d'une conversation assez longue et décryptage en quelques minutes
- Possibilité de déchiffrer la signalisation (SMS)
- La partie la plus dure est de « sniffer » le mobile
- Réseaux 3G : passage de SIM à USIM, passage à d'autres algorithmes (KASUMI, durée de vie estimée 5 ans)

Aspects de la sécurité

Généralisation des services IP

- Surveillance et accès, climatisation et chauffage, énergie, pilotage de processus industriels, tous nouveaux services *M2M* (*Machine to Machine*) et « Internet des objets » vont reposer sur IP.
- Changement d'échelle des accès aux éléments sensibles
- Facilité d'acquisition des technologies par les agresseurs (coût, diffusion)
- Le risque informatique peut devenir un risque physique
- Equipements légers et protocoles peu résistants, vulnérabilité physiques de l'infrastructure, vulnérabilité des serveurs
- Exemple *Defcon17* : déni de service sur la caméra, puis injection d'un flux vidéo (« *Ocean's 11 attack* »)

Ruptures de service chez les opérateurs

- Les ruptures de câbles : 2008, l'année noire
  - Câble APCN2 en Malaisie;
  - Câble *Colt* GB-continent;
  - Contrôle aérien de Phoenix;
  - Sectionnement des fibres optiques de la Silicon Valley (*AT&T* offre une récompense de 100 000$)
  - Services financiers paralysés dans l'état de NY
  - Signalisation *SNCF*
- En 2005, le *FBI* a utilisé un *spyware* pour confondre une tentative de rançon contre *Verizon* et *Comcast* après coupure de 18 câbles

Nuages sur le cloud

- Les utilisateurs rêvent d'accéder de manière évolutive à de nombreux services en ligne sans avoir à gérer l'infrastructure sous-jacente, souvent complexe.
- Les applications et les données ne se trouvent plus sur un serveur identifié, mais - métaphoriquement parlant - dans un nuage (*Cloud*) composé d'un certain nombre de serveurs distants interconnectés au moyen d'une excellente bande passante indispensable à la fluidité du système.
- L'accès au service se fait par une application standard facilement disponible, la plupart du temps un navigateur Web.

Aspects de la sécurité

Nuages sur le cloud

- John Chambers, CEO de *Cisco*, reconnait qu'il est très intéressé par les opportunités que représente le « cloud » pour *Cisco*, mais il ajoute : « *It is a security nightmare and it can't be handled in traditional ways."*
- *Cloud* parfois synonyme de haute indisponibilité : exemples de *Air New Zealand, Amazon* (EC2), *Barclays*, *ebay* (*Paypa l*), *Google* (*gmail* entre autres), *Over-blog*, *RIM*, *Twitter*, …
- De multiples points à valider : valider la politique de sécurité du prestataire, maîtriser la confidentialité des information (contrats de recherche des universités avec *Google Apps Education*), identifier la chaîne de responsabilité lors d'un dysfonctionnement

Aspects de la sécurité

Réseaux sociaux

Réseaux sociaux

- Le succès des réseaux sociaux attire les pirates.
- Atteinte à la sphère professionnelle et à la sphère privée de chaque individu.
- Accroissement du risque pour les entreprises d'être victimes de vol d'informations, de campagnes de dénigrement et de désinformation.
- Pourriels sur *Twitter* en février 2009
- Campagne d'hameçonnage sur *Facebook* en mai 2009
- Le chef des services secrets britanniques en petite tenue sur *Facebook* en mai 2009
- Le protection de la vie privée serait-elle un concept dépassé ? (Oui si l'on en croit les déclarations de Eric Schmidt, CEO de *Google*, et de Mark Zuckerberg, CEO de *Facebook*)

Cartes bancaires

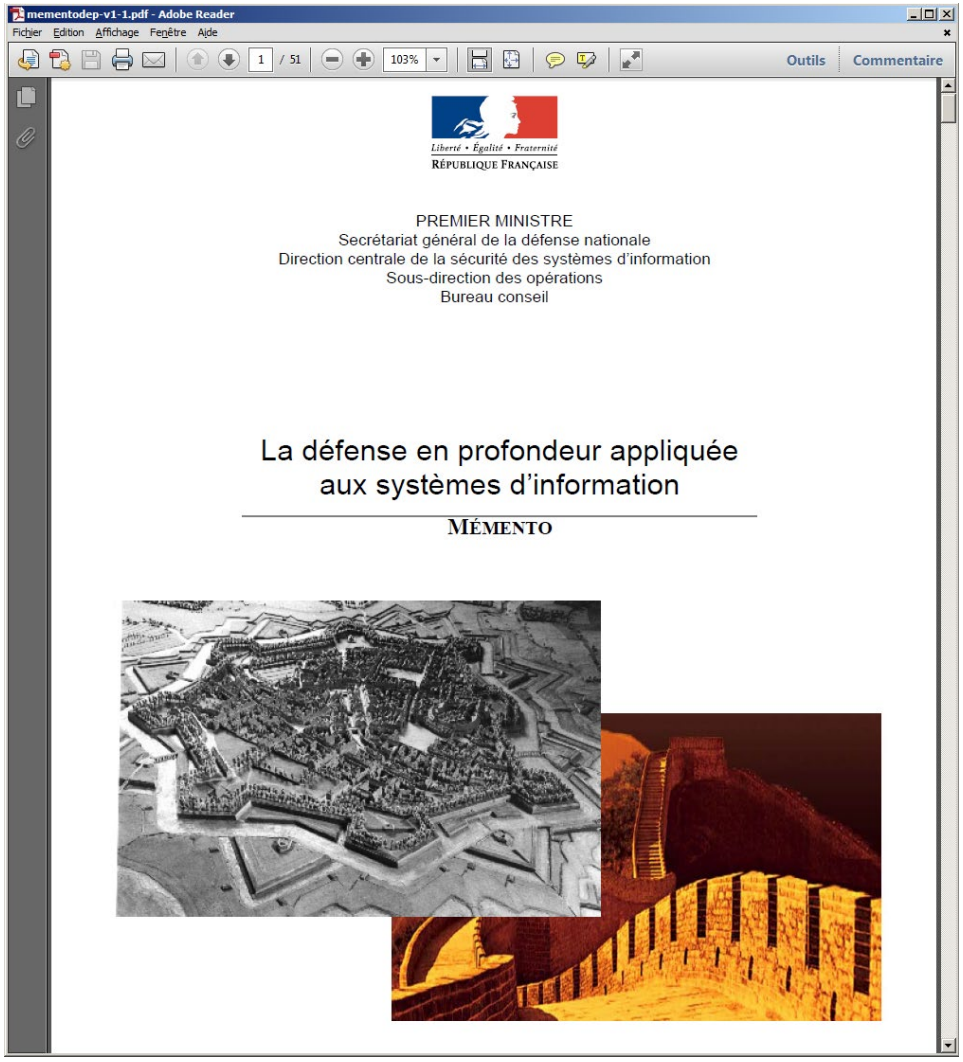
- Vols massifs de cartes bancaires.
- 9 millions de dollars de retraits frauduleux, fin 2008, au détriment de la filiale américaine de la *Royal Bank of Scotland;*
- Usage de cartes clonées, dans un délai très court, dans 2100 DAB, dans 280 villes répartis sur 8 pays (USA, Russie, Ukraine, Estonie, Italie, Honk-kong, Japon, Canada)
- Une attaque sophistiquée : Intrusion sur le réseau avec le vol de 1,5 million de Nos de cartes avec leur code PIN, décryptage des codes, création de cartes clones à piste magnétique, changement des plafonds de retrait, usage d'un réseau de « mules » rémunérées à 30-50% des sommes retirées, supervision de l'opération depuis le réseau corrompu avec effacement des traces.

Aspects de la sécurité

Remise en cause périmètre de sécurité

- La multiplication des vulnérabilités du fait de l'extension des services,
- La multiplication des points vulnérables du fait de l'extension des réseaux,
- La généralisation des dispositifs portables,
- La transformation des téléphones en véritables ordinateurs,
- L'usage de logiciels novateurs (code mobile, peer to peer, sites interactifs, téléphonie et visioconférence sur IP)
    - tendent à anéantir la notion de périmètre de sécurité comme aviation et blindés ont relativisé la notion de front.
- **La menace est partout et peut se manifester n'importe où, à n'importe quel moment.**

Défense en profondeur



- Il faut continuer à essayer d'empêcher les intrusions dans le SI de l'entreprise,
- mais le succès de la prévention ne peut plus être garanti;
- Il faut se préparer à limiter les conséquences d'une attaque réussie.

Plan

➔ A. Les principes et les enjeux

- *C01 Aspects et enjeux de la sécurité*
  - *Définitions.*
  - *Divers aspects de la sécurité. Typologie des risques. Exemples dans chaque catégorie de la typologie : nature, attaquants (menaces), impact.*
  - *Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.*
  - *Recenser les actifs à protéger.*
  - *Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)*
  - *Etude de cas : Evaluation du RMT.*

Enjeux

Enjeux de la sécurité

Enjeux de la sécurité

Démarche

- Le souci de maîtriser les risques implique une identification préventive, systématique et périodique de tous les problèmes pouvant avoir une répercussion sur le fonctionnement de l'entreprise :
  - Identifier les menaces et évaluer les risques;
  - Déterminer leurs probabilités;
  - Chiffrer leurs conséquences sur les projets (coût, délai, performances);
  - Sélectionner les risques assurables;
  - Adopter des provisions, des stocks et des marges de sécurité.

Evaluer les risques

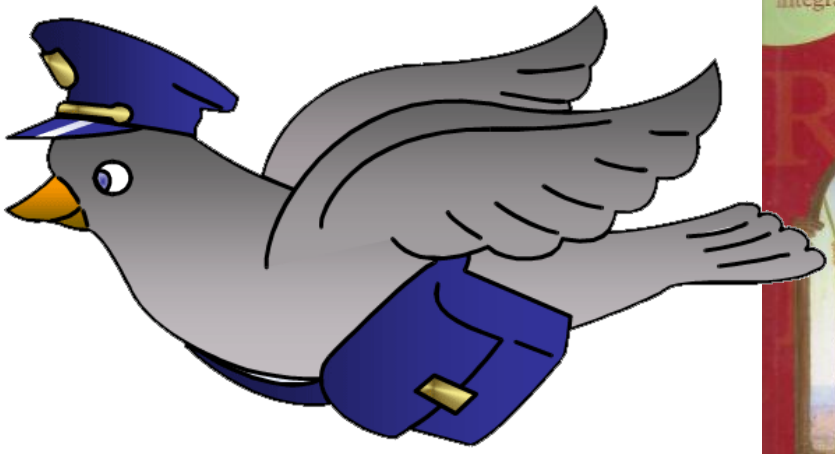
- La gestion du risque comprend l'identification, l'affaiblissement et la surveillance des menaces pour maintenir le risque à un niveau acceptable.
- Toute stratégie de gestion des risques doit tenir compte des priorités de sécurité suivantes:
  - Protection des sources de revenus;
  - Satisfaction des exigences des clients;
  - Sauvegarde de l'identité des sociétés et des marques;
  - Conformité aux réglementations et aux normes.

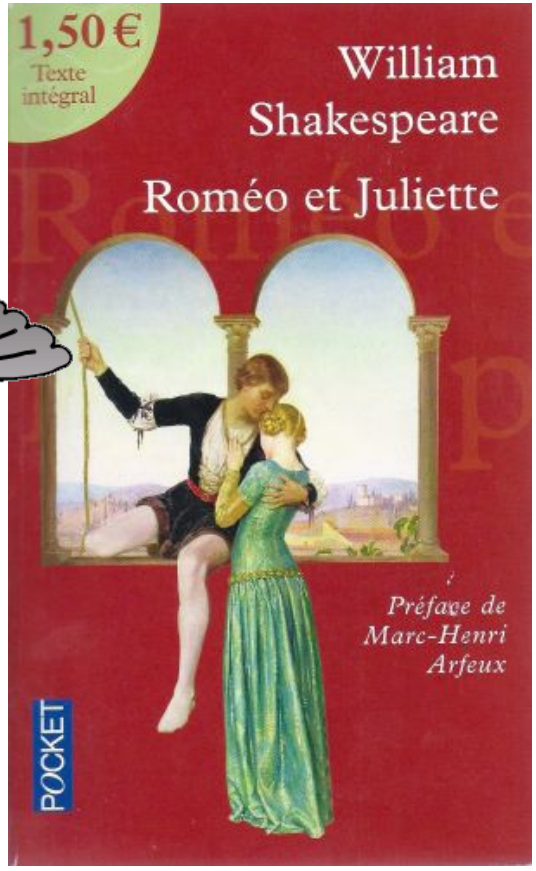
Enjeux

- Face aux menaces et risques identifiés, la sécurité des systèmes d'information repose sur 4 éléments :
  - La **disponibilité** des systèmes
  - **L'intégrité** des données et des traitements
  - La **confidentialité** des données et l'authentification des utilisateurs
  - La possibilité de **contrôle de la preuve et la non répudiation** des transactions et des échanges

Enjeux

➔ ***Roméo envoie un message à Juliette.***





Disponibilité

- ***Roméo envoie un message à Juliette.***
- Qu'est-ce qui garantit à Roméo que Juliette pourra consulter ce message dans les délais prévus ?
- Le principe de **disponibilité** vise à fournir les données ou les informations lorsque les utilisateurs en ont besoin.
- En clair : la disponibilité regroupe toutes les mesures visant à permettre un service sans interruption ou, sinon, prévue et anticipée.
- La disponibilité marque l'aptitude des systèmes à remplir une fonction –en particulier l'accès aux données de l'entreprise- dans des conditions prédéfinies d'horaires, de délais et de performances.

Disponibilité

- Assurer la disponibilité des données implique de disposer de l'accès aux données chaque fois que le besoin existe, dans des conditions de confort et de performances définies dans un contrat de service.
- Assurer la disponibilité des traitements implique de garantir la continuité du service, d'assurer les objectifs de performances, de date limite de traitement.
- Il faut disposer des ressources en matériels et logiciels nécessaires à l'ensemble des fonctions de base de l'entreprise (facturer les clients, recouvrir les créances, prendre et livrer les commandes, payer les salariés, les fournisseurs et les taxes, assurer la production, gérer les stocks ..)

Disponibilité

- Face aux menaces et risques identifiés, la sécurité des systèmes d'information repose sur 4 éléments :
  - La **disponibilité** des systèmes
  - **L'intégrité** des données
  - La **confidentialité** de l'authentification
  - La possibilité de **contrôler la non répudiation** des échanges

- Continuité de service
- Fiabilité
- Efficacité

Intégrité

- ***Roméo envoie un message à Juliette.***
- Qu'est-ce qui garantit à Juliette que ce message n'a pas été modifié durant son acheminement ?
- Le principe d'**intégrité** vise à assurer qu'une donnée est restée en l'état initial.
- Cette donnée est censée représenter l'état d'une entité, d'un système ou même d'une pensée ou idée, à un instant donné.
- Plus généralement, le principe d'intégrité vise à garantir qu'une donnée n'a pas subi de modification ou de détérioration non voulue par son administrateur.

Intégrité

- Affirmer que l'intégrité des données est assurée implique aussi que soient respectées les valeurs que peut prendre une quelconque de ces données, qu'elle soit considérée en tant que telle (un montant inscrit dans un compte ne peut être négatif) ou qu'elle soit placée en relation avec d'autres (le montant des fonds propres ne peut excéder le total du passif).
- Dans une Base de Données, les contrôles d'intégrité référentielle vérifient que pour chaque information d'une table A qui fait référence à une information d'une table B, l'information référencée existe dans la table B.
- Ceci permettra d'empêcher la saisie de commandes pour un client inexistant ou de supprimer un client pour lequel il reste encore des créances en cours.

Intégrité

- Assurer l'intégrité des données implique de respecter des critères comme exhaustivité (ne pas perdre de données), exactitude (des données qui traduisent la réalité de l'organisation) et validité.
- Assurer l'intégrité des traitements conduit à prendre des mesures pour éviter de modifier par erreur des informations.
- Elle conduit à obtenir des résultats complets et fiables quel que soit le processus (le cumul du CA sur tous les produits doit être égal au cumul du CA sur tous les points de vente).
- Elle conduit aussi à assurer la conformité de l'algorithme des traitements automatisés par rapport aux règles de gestion.

Intégrité

- Face aux menaces et risques identifiés, la sécurité des systèmes d'information repose sur 4 éléments :
  - La **disponibilité** des systèmes
  - **L'intégrité** des données
  - La **confidentialité** des données et l'authentification de
  - La possibilité de **la non répudiation** des échanges

- Exactitude
- Exhaustivité
- Inaltérabilité

Confidentialité

- ***Roméo envoie un message à Juliette.***
- Qu'est-ce qui garantit à Roméo que personne d'autre que Juliette n'a pu ou ne pourra consulter le message ?
- La **confidentialité** regroupe tous les mécanismes permettant d'assurer qu'une information ne pourrait être accessible et exploitable que par les personnes autorisées.
- Ce principe peut être considéré de manière autonome, par exemple lorsque l'on traite de cryptographie sur un système de fichiers, ou de manière combinée, au principe d'authentification.

Confidentialité

- Affirmer que la confidentialité des données est assurée implique qu'elles soient accessibles pour consultation, mise à jour ou suppression, uniquement aux personnes ayant reçu l'habilitation nécessaire.
- Authentifier un utilisateur implique de vérifier qu'il s'agit bien de lui et qu'il n'agit pas sous la contrainte.

Confidentialité

- Assurer la confidentialité des données consiste à réserver l'accès aux données par les seuls utilisateurs habilités, ce qui relie cette exigence à l'exigence d'authentification.
- Cette assurance se fait en fonction de la classification des données et du niveau d'habilitation des utilisateurs.
- En corollaire, il faut bien évidemment savoir interdire l'accès et l'usage des données par des tiers non autorisés, surtout ceux mal intentionnés.
- Assurer la confidentialité des traitements consiste à protéger les algorithmes décrivant les règles de gestion et les résultats dont la divulgation à un tiers non autorisé. C'est la protection du savoir-faire de l'entreprise.

Confidentialité

- Face aux menaces et risques identifiés, la sécurité des systèmes d'information repose sur 4 éléments :
  - La **disponibilité** des systèmes
  - **L'intégrité** des données
  - La **confidentialité** des données et l'authentification des u
  - La possibilité d **la non répudiation** des échanges

- Auditabilité

Enjeux de la sécurité

Contrôle preuve et non répudiation

- ***Roméo a reçu un message de Juliette.***
- Juliette prétend qu'elle ne l'a pas envoyé. Qui a raison ?
- Le principe de **non-répudiation** regroupe les mesures permettant d'affirmer avec certitude quel est ou quels sont les auteurs d'une opération.
- Très utilisé dans le domaine boursier, les mesures de non-répudiation permettent par exemple d'empêcher que des opérateurs se dédient de leur acquisition (ou de leur vente) en cas de chute du cours (ou de hausse).

Enjeux de la sécurité

Contrôle preuve et non répudiation

- Ne pas répudier une transaction implique de ne pouvoir nier avoir reçu ou transmis un message lorsque ceci a été effectivement le cas.
- Permettre le contrôle de la preuve au niveau d'un traitement exige de garantir la possibilité d'en reconstituer toutes les étapes.
- Permettre le contrôle de la preuve au niveau des données implique d'assurer la possibilité de reconstituer une donnée et de tracer son utilisation.

Contrôle preuve et non répudiation

- Face aux menaces et ris
  sécurité des systèmes d'inf
  4 éléments :
  - La **disponibilité** des s
  - **L'intégrité** des donnée
  - La **confidentialité** des do es et l'authentification des utilis teurs
  - La possibilité de **contrôle de la preuve et la non répudiation** des transactions et des échanges

- Confiance

Respecter les enjeux

- Le système d'information d'une organisation regroupe des données stockées sur des supports, des processus qui ont pour objet de traiter ces données et des flux qui traduisent les divers échanges de données effectués par les acteurs impliqués dans le processus.
- Nos quatre exigences de sécurité nous imposent d'agir au niveau des données, des traitements et des flux.
- La sécurité des flux renvoie au problème de la sécurité des réseaux.

Respecter les enjeux

- Pour assurer la disponibilité des systèmes;
- Pour assurer l'intégrité des données;
- Pour assurer la confidentialité des données et l'authentification des utilisateurs :
- Pour assurer la possibilité de contrôle de la preuve et la non répudiation des transactions et des échanges

Respecter les enjeux

- Pour assurer la disponibilité des systèmes;
- Pour assurer l'int rité des données ;
- Pour assurer l fidentialité des données et l'authentificati tilisateurs ;
- Pour preuv des é

- Maintenance
- Redondance
- Sauvegarde
- Capacity planning
- Procédures d'exploitation

Respecter les enjeux

- Pour assurer la disponibilité des systèmes;
- Pour assurer l'intégrité des données ;
- Pour assurer la confidentialité des données et l'authentification des utilisateurs ;
- Pour [illegible] preuve [illegible] des éc[illegible]

- Contrôle d'accès
- Contrôle d'erreur
- Contrôle de cohérence
- Activer le contrôle d'Intégrité référentielle

Respecter les enjeux

- Pour assurer la disponibilité des systèmes;
- Pour assurer l'intégrité des données ;
- Pour assurer la confidentialité des données et l'authentification des utilisateurs ;
- Pour assurer la [illegible]bilité de contrôle de la preuve et la n[illegible]ation des transactions et des [illegible]

  - Contrôle d'accès (identification et authentification)
  - Chiffrement

Respecter les enjeux

- Pour assurer la disponibilité des systèmes;
- Pour assurer l'intégrité des données ;
- Pour assurer la confidentialité des données et l'authentification des utilisateurs ;
- Pour assurer la possibilité de contrôle de la preuve et la non répudiation des transactions et des échanges.

- Certification
- Enregistrement et traçabilité
- Signature électronique

Synthèse

ENJEU	CRITERE A RESPECTER	POUR Y PARVENR
Disponibilité	Continuité de service Fiabilité Efficacité	Maintenance Redondance Sauvegarde Capacity planning Procédures d'exploitation PRI et PCA
Intégrité	Exactitude Exhaustivité Inaltérabilité	Contrôle d'accès Contrôle d'erreur Contrôle de cohérence Activer contrôle d'Intégrité référentielle
Confidentialité	Auditabilité	Contrôle d'accès Chiffrement, PKI
Contrôle de la preuve et non répudiation	Confiance	Certification Enregistrement et traçabilité Signature électronique

Plan

- **A. Les principes et les enjeux**
  - C01 Aspects et enjeux de la sécurité
    - Définitions.
    - Divers aspects de la sécurité. Typologie des risques.
    - Exemples dans chaque catégorie de la typologie : nature, attaquants (menaces), impact.
    - Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.
    - Recenser les actifs à protéger.
    - Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)
    - Etude de cas : Evaluation du RMT.

Actifs matériels

- La sécurité n'a de sens que par rapport à ce qu'on cherche à protéger.
- Le système d'information de l'entité est composé d'éléments matériels et immatériels, les premiers sont en général bien recensés dans l'inventaire, mais pas toujours !
- C'est donc un point préalable à vérifier.
- Le vol, la disparition ou le dommage à un quelconque de ces actifs devront être déclarés et justifiés par les personnels en charge de leur utilisation ou surveillance.
- Il faudra aussi étudier les polices d'assurance pour apprécier de la pertinence du contrat.

Actifs immatériels : logiciels

- Les biens immatériels composant le système d'information sont en général des logiciels, certains d'entre eux sont inscrits à l'inventaire (les logiciels acquis).
- Pour ceux qui sont développés en interne ce n'est pas toujours le cas, la procédure d'activation étant souvent jugée sans avantage économique et les commissaires aux comptes pas toujours très au fait de leur existence ou de leur importance dans la vie de l'entreprise.
- En tout état de cause, les logiciels demandent une identification bien précise et une conservation sécurisée des codes sources (si disponibles), des supports originaux des éditeurs, des licences d'utilisation, des contrats de cessions de droits ou de maintenance ou tout autre élément constitutif des droits possédés par l'entité sur les logiciels qu'elle utilise.

Actifs immatériels : données

- Les contenus des bases de données ou des fichiers ne sont pas en général valorisés dans l'actif de l'entité, mais représentent souvent des valeurs vénales importantes qui peuvent être valorisées dans certaines occasions (cession ou fusion de l'entreprise, par exemple).
- Les données concernant les clients, les contrats, les réponses aux appels d'offres, représentent souvent la valeur principale pour des entreprises qui sont de plus en plus dépendantes des informations contenues dans leur « mémoire » (concepts *ECM*, *MDM*) , constitutives de leur « savoir » et donc de leur capacité à « faire ».

Recenser les actifs à protéger

Importance de la protection des actifs

- Il est à noter l'importance cruciale de ces « actifs » dont la protection est impérative :
  - de par la loi qui protège les informations nominatives (informatique et libertés) et qui rend responsable pénalement celui qui les détient et qui ne protège pas efficacement leur confidentialité ;
  - de par la responsabilité du chef d'entreprise devant les propriétaires de l'entité ;
  - de par la prise de conscience des salariés que leur emploi en dépend.

Recenser les actifs à protéger

Normes de classification

- L'Afnor distingue trois types d'informations :
  - « L'information aisément et licitement accessible » que certains appellent « l'information blanche » est ouverte à tous. Elle se trouve dans la presse, Internet.
  - « L'information licitement accessible mais caractérisée par des difficultés dans la connaissance de son existence et de son accès ». Cette « information grise », pour la trouver, il faut d'abord savoir la chercher. Elle se rapproche davantage du renseignement.
  - « L'information à diffusion restreinte et dont l'accès et l'usage sont expressément protégés ». Il s'agit ici de « l'information noire » qui est protégée par un contrat ou une loi. Seules quelques personnes sont autorisées à y accéder.

Recenser les actifs à protéger

Normes de classification

- Il est recommandé que les informations « noires » reçoivent une mention spécifique rappelant leur sensibilité en considération de la gravité des conséquences qu'auraient leur divulgation, leur altération, leur indisponibilité ou leur destruction.
- À cette fin, une distinction est opérée par deux mentions désignant le niveau de protection qu'il faut assurer à l'information : CONFIDENTIEL et DIFFUSION LIMITÉE.
- Chacune de ces mentions de sensibilité peut être assortie d'une mention spécifique, caractéristique du domaine protégé :
  - personnel (information nominative au sens de la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés) ;
  - professionnel (protégé par l'article 226-13 du Code pénal).

Plan

➔ A. Les principes et les enjeux

- *C01 Aspects et enjeux de la sécurité*
  - *Définitions.*
  - *Divers aspects de la sécurité. Typologie des risques.*
  - *Exemples dans chaque catégorie de la typologie : nature, attaquants (menaces), impact.*
  - *Enjeux et problématiques de la sécurité. Les piliers de la sécurité : Assurer la disponibilité. Assurer l'intégrité. Assurer la continuité. Assurer le contrôle de la preuve et la non-répudiation des transactions.*
  - *Recenser les actifs à protéger.*
  - *Evaluer les risques. Classification des risques. Concept de Risque Maximal Tolérable (RMT)*
  - *Etude de cas : Evaluation du RMT.*

Evaluer les risques

Evaluer les risques

Un SI n'est jamais invulnérable

- La gestion des risques liés aux systèmes d'information repose sur une démarche globale, fondée sur l'identification des menaces potentielles, mais aussi sur l'idée qu'aucun système d'information n'est invulnérable car la sécurité repose sur des outils et sur le facteur humain.
- Les outils ne sont pas efficaces à 100% :
  - il est impossible de se protéger à 100 % des codes malveillants (virus, chevaux de Troie) ;
  - les pare-feux ne protègent pas de tous les types d'attaques ;
  - les algorithmes cryptographiques ne sont pas tous fiables ;
  - les systèmes de détection d'intrusion peuvent être trompées ;
  - il n'est pas possible de tester toutes les failles de sécurité des systèmes et les applications déployés auprès des utilisateurs dans des délais raisonnables.
- Le facteur humain est par nature vulnérable.
- La prise de conscience de l'impact des pertes possibles dues à un sinistre informatique est à mettre en balance avec les investissements souvent modestes qui peuvent protéger efficacement les actifs de l'entreprise.

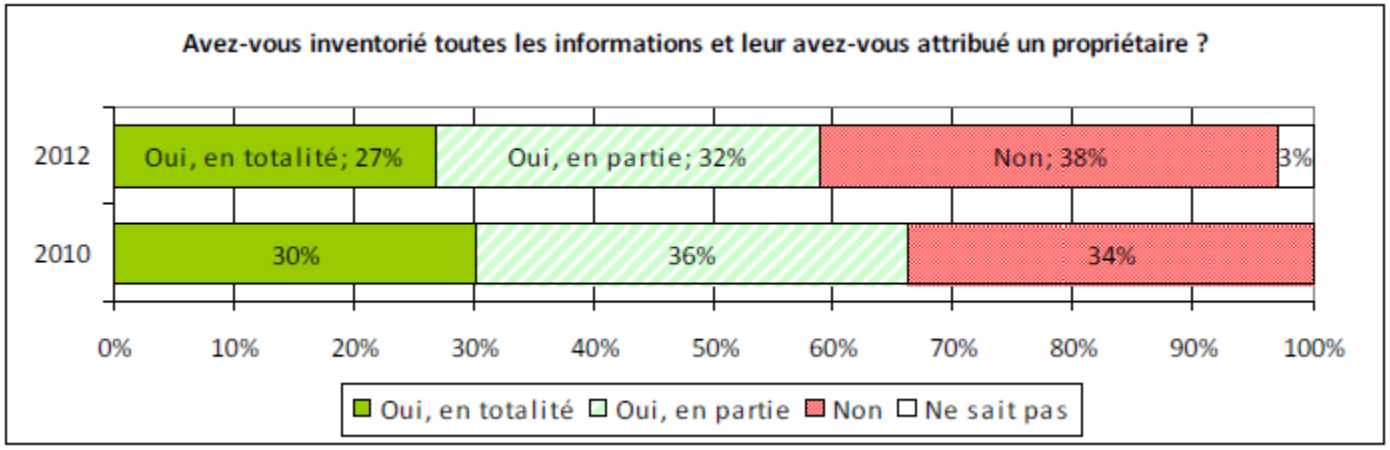
Incidences économiques

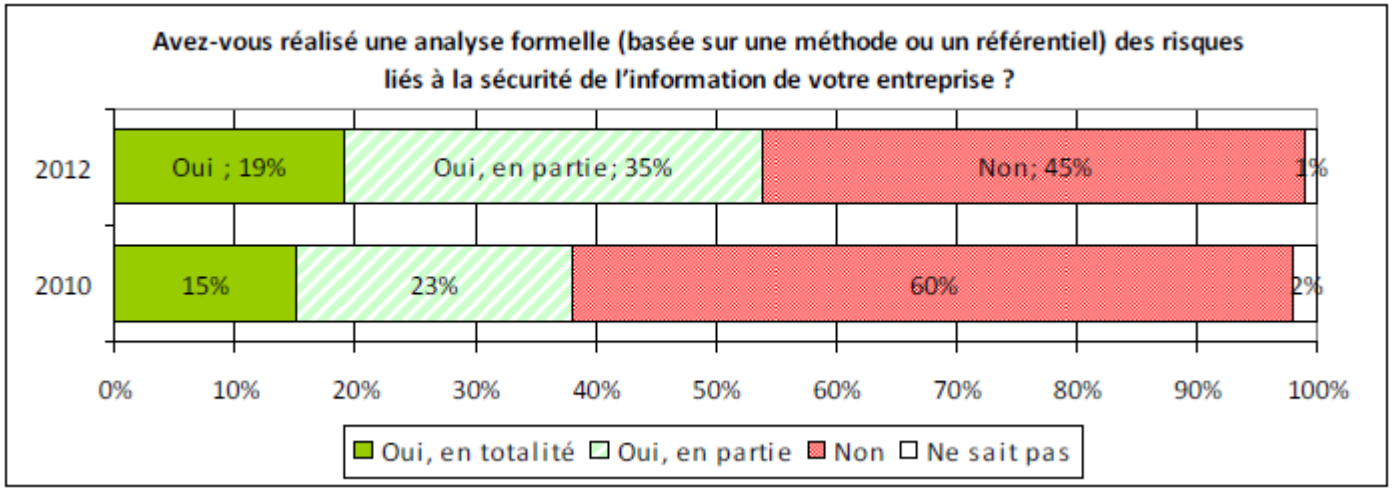
- Les incidents dus à une défaillance de la sécurité des systèmes d'information peuvent affecter l'ensemble des activités et du patrimoine de l'entreprise et peuvent conduire à :
  - des perturbations ou des interruptions des processus clés de l'entreprise ;
  - des pertes de parts de marchés (vol de technologies, de bases clients/fournisseurs…) ;
  - des pertes financières directes :
    - coûts d'immobilisation des installations de production,
    - coût du temps passé à la restauration des systèmes,
    - coûts techniques de remplacement de matériels ou de logiciels… ;
  - une perte d'image et/ou de confiance des clients, partenaires et employés ;
  - des actions contentieuses ou de mise en responsabilité liées à la fraude informatique ;
  - une remise en cause des assurances de perte d'activité.
- De manière moins visible mais plus lourde de conséquences, les actions d'espionnage industriel, relayées parfois par des moyens étatiques, vont se traduire pour les entreprises françaises par une perte de substance ou de compétitivité et au final par un effet négatif sur l'emploi.

Analyse des risques

- L'étape d'analyse des risques consiste à répertorier les différents risques encourus, d'estimer leur probabilité et enfin d'étudier leur impact.
- La meilleure approche pour analyser l'impact d'une menace consiste à estimer le coût des dommages qu'elle causerait (par exemple attaque sur un serveur ou détérioration de données vitales pour l'entreprise).
- Sur cette base, il peut être intéressant de dresser un tableau des risques et de leur potentialité, c'est-à-dire leur probabilité de se produire, en leur affectant des niveaux échelonnés selon un barème à définir, par exemple :
  - sans objet (ou improbable) : la menace n'a pas lieu d'être ;
  - faible : la menace a peu de chance de se produire ;
  - moyenne : la menace est réelle ;
  - haute : la menace a de grandes chances de se produire.

Analyse des risques





Source :
Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Risque Maximum Tolérable

- RMT : Risque Maximal Tolérable
- RMT : montant maximal du risque global que l'entreprise peut supporter sans mettre en cause la continuité de ses opérations, voire sans mettre en péril sa survie ?".
- Nous avons défini le risque :
- *Risque = probabilité d'occurrence * préjudice*
- *Risque = probabilité d'occurrence * conséquence financière si le sinistre survient*
- La somme des risques doit être inférieure au RMT

Risque Maximum Tolérable

- Considérons le cas d'une banque :
- En première analyse, le RMT est la valeur limite, en millions d'euros, imposée par la direction générale,
- de la part α des fonds propres nets désirés (considérons que la banque ait un objectif supérieur à 8 % en termes de ratio de solvabilité-Bâle II-))
- ajoutée à celle, β, de la capacité bénéficiaire prévisionnelle nette de l'année que la banque "accepte" de perdre (part des bénéfices pouvant absorber un sinistre),
- ajoutée au montant des garanties (ne sont retenues que celles dont on est sûr, ce qui explique que le facteur γ est inférieur ou égal à 1) accordées par les assurances en cas de sinistres informatiques.
- RMT = α FP + β Bénéf. + γ Garanties avec α, β, γ ≤ 1

Risque Maximum Tolérable

Etude de cas

Risque Maximum Tolérable

- *Afin d'illustrer les éléments théoriques présentés ci-dessus, nous proposons l'étude du cas d'un établissement financier.*
- *Celui-ci propose à ses clients l'achat et la vente de produits financiers (actions, options, futures (contrats à terme), warrants) uniquement sur Internet.*
- *Les achats peuvent être réglés comptant ou de manière différée (SRD).*
- *L'établissement réalise donc des opérations de crédit.*
- *Nous commençons par l'évaluation du montant du RMT.*

Etude de cas

Risque Maximum Tolérable

- ***Hypothèses*** *: L'établissement possède 15 millions d'euros de fonds propres et nous fixons, comme le recommande le Livre Blanc de la Commission Bancaire, α à 20%.*
- *L'établissement réalise 5 millions d'euros de résultats bruts. La direction générale choisit de fixer ß à 10%. C'est-à-dire que 10% des résultats d'exploitation peuvent servir à éponger les pertes en cas de sinistre.*
- *Nous considérons au démarrage un montant de l'assurance égal à 0. Ce sera notre variable d'ajustement. Nous tenterons ainsi d'en faire une évaluation afin de choisir au mieux le système d'assurance que l'établissement doit adopter.*

Etude de cas

Risque Maximum Tolérable

- ***Calculez le RMT***
- *Nous considérons que 20% des risques de l'établissement peuvent être attribués à des sinistres informatiques.*
- ***Calculez RMTi, c.a.d. le Risque Maximum Tolérable informatique***
- *Nous identifions deux risques R1 et R2.*
- *L'un est de type Intégrité et l'autre, de type Disponibilité.*

Etude de cas

Risque Maximum Tolérable

- ***Reprenons la formule du calcul du RMT :***
- ***RMT = a * Fonds Propres + ß * Bénéfices + Y * Montant de la Garantie d'Assurance***
- ***Dans notre cas :***
- ***RMT = (15 000 000 * 20%) + 5 000 000 * 10% + Y *0= 3 500 000 €***
- ***RMTi = 20%*RMT***
- ***RMTi = RMT * i= RMT * 1/5 = 700 000 €***

Risque Maximum Tolérable

- *Le risque #1 R1 : « Piratage d'un compte sur le site avec transfert frauduleux vers un compte extérieur »*
  - *Le montant maximum d'un transfert depuis le site vers un compte extérieur est de 500 000 euros. Soit V1 = 500 000 €*
  - *R1 = µ1 * V1, avec V1 = 500 000 €*
- *R2 : « Attaque Internet du site web entraînant une indisponibilité d'une journée »*
  - *La somme des pertes engendrées, pour l'ensemble des clients, par l'impossibilité de vendre ou d'acheter en fonction des variations des marchés financiers peut être très importante. Nous fixons la perte totale à 20 millions d'euros, soit V2 = 20 000 000 €*
  - *R2 = µ2 * V2, avec V2 = 20 000 000 €*
- *Reste à définir les probabilités d'occurrence µ1 et µ2 de tels sinistres.*

Etude de cas

Risque Maximum Tolérable

- *Nous considérons trois cas :*
- *Cas No 1, avec un niveau idéal de sécurité*
  - *Considérons μ1=1/1000 et μ2=1/250*
- *Cas No 2, avec un niveau moyen de sécurité*
  - *Considérons μ1=1/10 et μ2=3/100*
- *Cas No 3, avec un niveau critique de sécurité*
  - *Considérons μ1=1/10 et μ2=1/20*
- ***Déterminer la somme des risques***
- ***Comparer le résultat au Risque Maximum Tolérable informatique***
- ***Quelles décisions, dans chaque cas, vis à vis de la politique de sécurité et de la police d'assurance ?***

Etude de cas

Risque Maximum Tolérable

CAS N°1 : LE CAS IDÉAL	CAS N°2 : LE CAS RÉEL	CAS N°3 : LE CAS CRITIQUE
L'établissement **maîtrise** la sécurité de son système d'information. Les probabilités d'occurrence ***µ1*** et ***µ2*** sont donc très faibles.	La sécurité du système est **imparfaite**, mais les employés et les clients demeurent fiables. Les probabilités d'occurrence ***µ1*** et ***µ2*** ne sont pas négligeables.	Le système est vulnérable et exposé à des utilisateurs peu scrupuleux. Les probabilités d'occurrence ***µ1*** et ***µ2*** sont élevées.
Soit : $\mu 1 = 1/1000$ et $\mu 2 = 1/250$. RTMi évalué à 700 000 euros	Soit : $\mu 1 = 1/10$ et $\mu 2 = 3/100$	Soit : $\mu 1 = 1/10$ et $\mu 2 = 1/20$.
La somme des risques est alors définie comme suit : R1 + R2 = (500 000 * 1/1000) + (20 000 000 * 1/250) =**80 500** €	Nous définissons la somme des risques ($\mu 1$*V1 + $\mu 2$*V2) de la manière suivante: R1 + R2 = (500 000 * 1/10) + (20 000 000 * 3/100) = 50 000 + 600 000 = **650 000** €	La somme des risques est alors définie de la manière suivante : R1 + R2 = (500 000 * 1/10) + (20 000 000 * 1/20) = 50 000 + 1 000 000 = **1 050 000** €
80 500€ << RTMi Avec un RMTi évalué à 700 000 €, l'établissement est alors dans une situation où **la somme des risques est très inférieure au RMTi**	L'établissement est alors dans une situation où **la somme des risques est proche du RMTi.**	L'établissement est alors dans une situation où **La somme des risques est supérieure au RMTi.**
Dans le cas n°1 où R1 + R2 << RMTi, l'établissement peut choisir de réduire la part de risque informatique de sa police d'assurance.	Dans la cas n°2 où R1 + R2 ≈ RMTi, l'établissement doit renforcer sa sécurité et adapter le contrat d'assurance relatif aux risques informatiques.	Dans la cas n°3 où R1 + R2 > RMTi, l'établissement doit agir $\mu 1$ et $\mu 2$ et tenter de trouver des solutions pour réduire V1 et V2.

Corrigé
Etude de cas

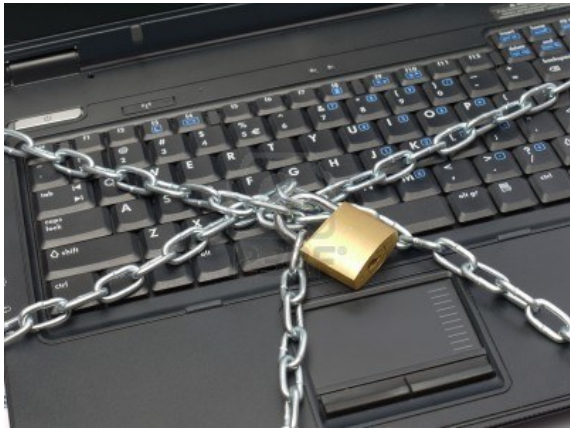
Agenda

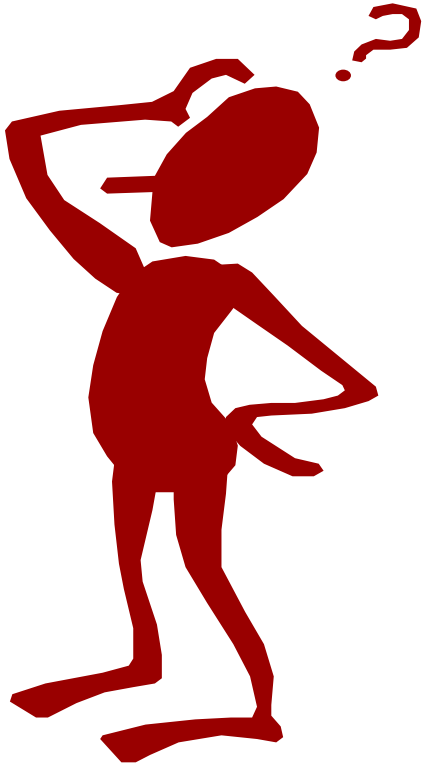
- **A. Les principes et les enjeux**
  - C01 Aspects et enjeux de la sécurité
  - **C02 Enjeux économiques et modes d'action**
  - C03 Plan de secours et plan de continuité des activités
  - C04 Sécurité et banque
- **B. Les méthodes et les outils**
  - C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité
  - C06 Renforcer la sécurité des réseaux et des systèmes
  - C07 Renforcer la sécurité des accès et des contrôle d'identités
  - C08 Renforcer la sécurité des applications et des services
  - C09 Renforcer la sécurité des dispositifs mobiles
  - C10 Evaluer la sécurité
  - C11 Manager les risques dans les projets SI
- **C. Bilan et perspectives**

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - **Enjeux économiques**
    - *Le management de la sécurité dans l'entreprise.*
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - *Assurance et financement des risques*

Enjeux économiques





Quelle solution de sécurité

Coûts

- Il n'y a pas de limites aux dépenses à engager en matière de sécurité.
- Pour éviter le vol d'un ordinateur vous pouvez :
  - l'attacher à son support par une chaîne,
  - fermer le local à clef,
  - blinder tous les accès du local (porte, fenêtre),
  - placer un gardien devant la porte,
  - mettre en place un dispositif de contrôle d'accès avec un portail électronique et des vigiles sur l'ensemble du périmètre,
  - déménager et mettre le tout sur une île déserte, entourée d'une task force de navires de guerre.

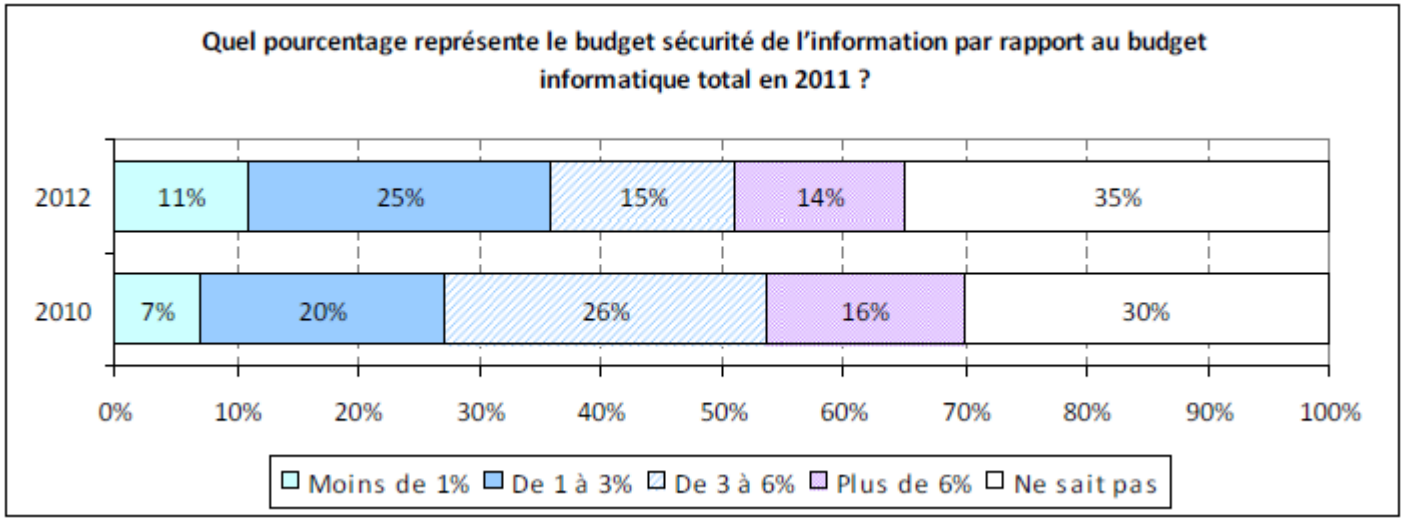
Coûts

- La vraie question est "combien dépenser par rapport au risque encouru ?".
- La dernière solution engendre des coûts qui ne sont envisageables que si l'ordinateur est un modèle unique comportant des données ultra-secrètes.
- S'il s'agit d'un simple PC, la solution No 1 suffit probablement.
- Nous avons vu que les spécialistes utilisent le concept de "**risque maximal tolérable**", défini comme la proportion des fonds propres fixée comme limite à ne pas dépasser pour ne pas remettre en cause la pérennité de l'établissement face à un sinistre informatique majeur.

Coûts

- Les études des cabinets spécialisés montrent que les dépenses en matière de sécurité des systèmes d'information représentent environ 5 milliards d'euros dans l'Union Européenne, soit 5% des investissements informatiques.
- Le **budget sécurité** représentait en 2000 1 à 3% des budgets informatiques français.
- La tendance actuelle estime cette proportion entre 5 à 8 %, ce qui montre une réelle prise de conscience.
- C'est une des rares branches du marché informatique qui a su conserver un taux de croissance à 2 chiffres.

Coûts



Source :
Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Budget informatique moyen pour les entreprises du panel : 1,6 M€
(64% < 1 M €, maxi : 40 M€)
42% des sondés ont répondu.

Coûts

- Il est beaucoup plus difficile d'évaluer le **coût de la non-sécurité** car les victimes ne sont pas très enclins à fournir des détails.
- Elle se monte probablement, pour la seule France, à plusieurs dizaines de milliards d'euros.
- Le coût moyen d'une violation/perte de données pour une entreprise : 2,55 M€ (Source : étude du Ponemon Institute commanditée par Symantec).
- Le coût moyen d'une donnée corrompue a été établie à 120 € (recherches à mener après incident, support technique pour les victimes, interruption de production, perte d'exploitation, notification aux instances réglementaires).
- On peut ainsi mieux mesurer le retour sur investissement d'une politique efficace en matière de sécurité.

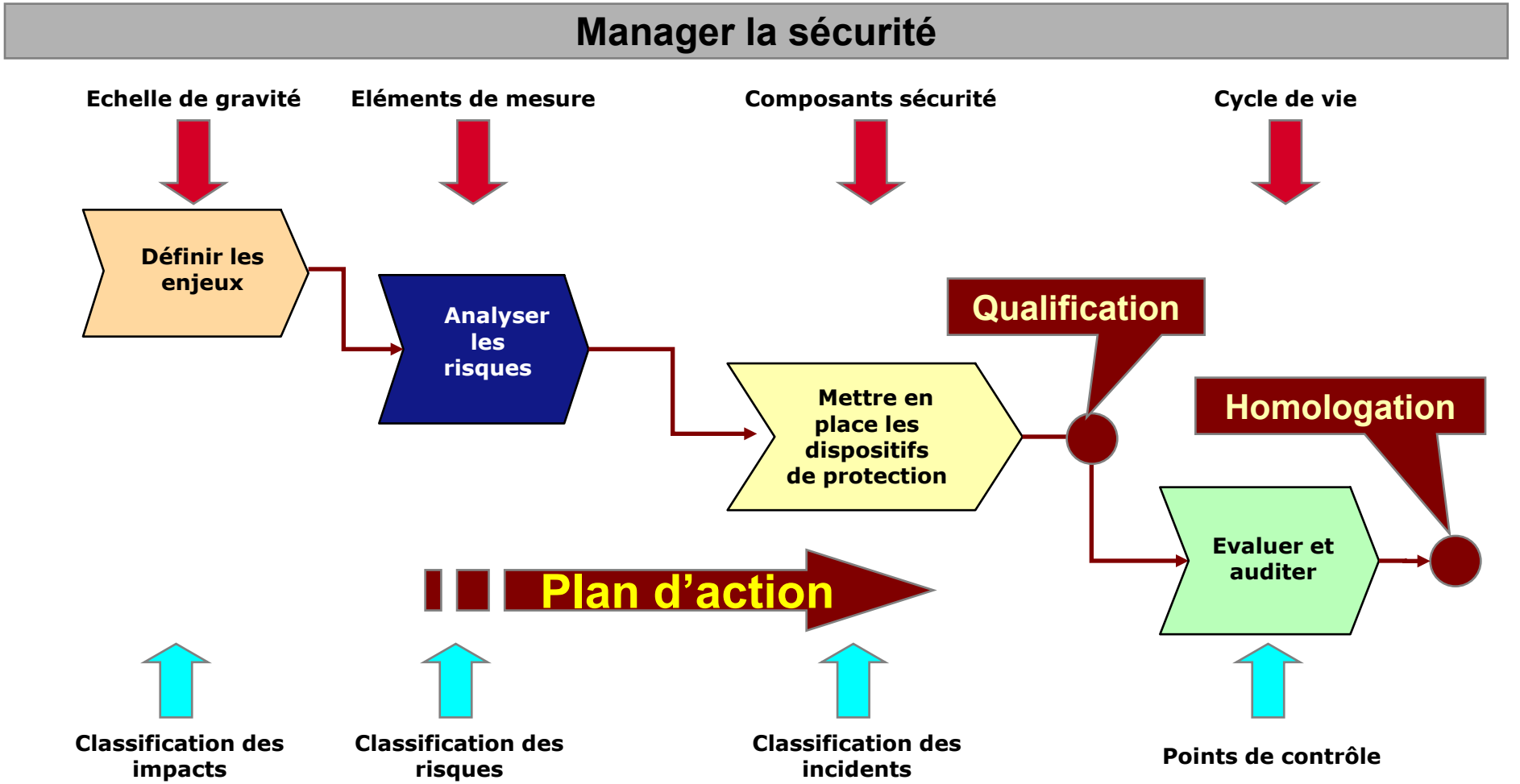
Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - ***Le management de la sécurité dans l'entreprise.***
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - *Assurance et financement des risques*

Plan d'action

- Maîtriser les risques implique la mise en place d'une **politique de sécurité**.
- Une politique de sécurité est une déclaration officielle des règles qui doivent régir le comportement des personnes auxquelles on accorde un accès aux ressources technologiques et aux actifs informationnels d'une entreprise.
- Plusieurs niveaux d'intervention sont possibles

Plan d'action



Politique de sécurité

- Pour aborder ce problème, il est essentiel de s'assurer que les processus métiers et de gestion actuels et futurs sont compris, de telle sorte que les implémentations de sécurité puissent être conçues pour les soutenir et les protéger.
- Avant de créer, d'évaluer ou de modifier toute politique de sécurité, quelques questions simples doivent être posées:
  - Les processus clefs de l'entreprise sont-ils bien compris?
  - Y a-t-il suffisamment de dispositifs en place pour protéger les données, qu'elles soient stockées, en transit, ou en usage?
  - Quelles applications commerciales, quels services, et quels changements d'infrastructure sont en cours de déploiement ou en passe d'être déployés dans les prochaines années?
  - Quels sont les risques associés à l'implantation de ces solutions ?
  - Comment réduire ces risques spécifiques, autant que possible?
  - Quels mandats de conformité réglementaire sont-ils nécessaires pour l'organisation, et quel est le plan pour les obtenir?

Plan d'action

- Des actions au **niveau physique**, relatif à :
  - la protection des locaux (qualité du bâtiment, protection incendie /dégâts des eaux), contrôle d'accès, alimentation électrique, climatisation, certification câblage, placement bornes radio, contrôle signaux en provenance et à detination de l'extérieur, etc.)
  - la protection des réseaux (pare-feux, RPV)
  - la mise en place de solutions de sauvegarde et de reprise(les fameux "*back up*")
- Des actions au **niveau logique** relatifs à la mise en place d'outils logiciels et de processus sur leur mise en œuvre (mots de passe, chiffrement, PKI, etc.)

Plan d'action

- L'amélioration du niveau de l'information et de la sensibilisation :
- **La sécurité est l'affaire de tous.**
- Il est inutile de dépenser des dizaines de milliers d'euros dans un système d'administration de la sécurité vérifiant la pertinence et le renouvellement des mots de passe si ceux-ci sont inscrits sur des petites étiquettes autocollantes placées bien en évidence sur l'écran.

Plan d'action

- L'**externalisation des risques** : Elle consiste à définir précisément quels sont les risques que l'organisation accepte d'assumer elle-même et ceux qu'elle désire transférer sur d'autres agents économiques.

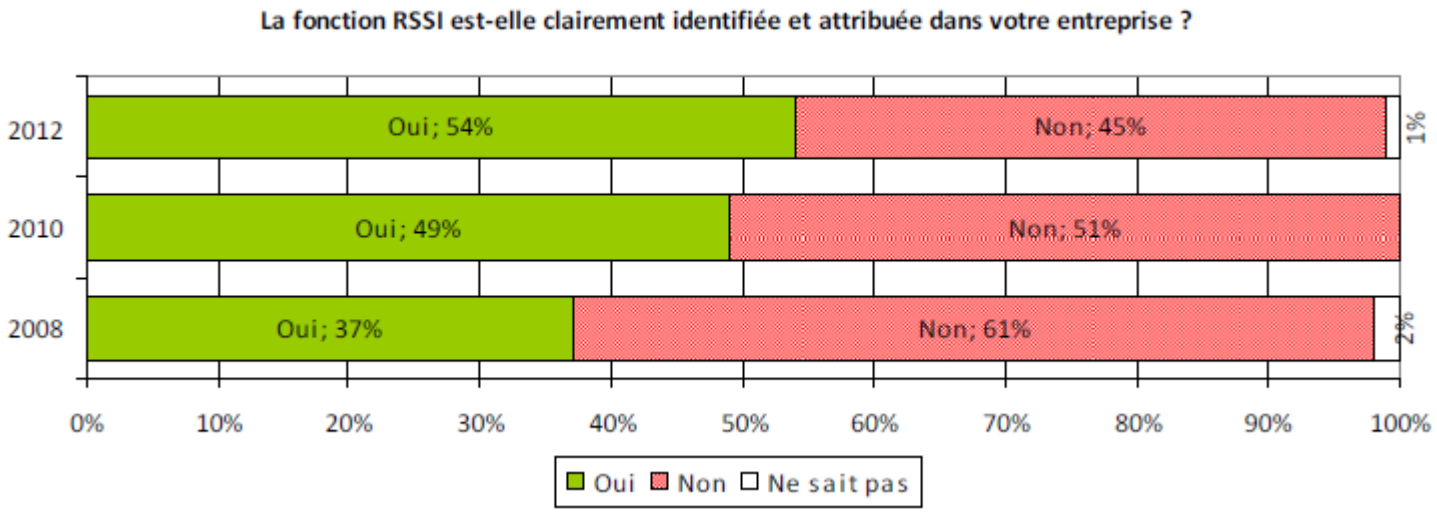
- La problématique de l'assurance entre dans le champ de cette externalisation, mais aussi le recours à des prestataires spécialisés s'engageant sur un contrat de services.

Plan d'action

- A l'image des grandes structures qui centralisent les problématiques de sécurité sur un groupe de travail animé par un **RSSI (Responsable de la Sécurité des Systèmes d'Information),** les petites structure doivent désigner un responsable qui va agir en tant que maître d'ouvrage.

- Comme il ne peut couvrir tous les champs d'expertise, il pourra s'adresser à des prestataires extérieurs spécialisés.

Plan d'action

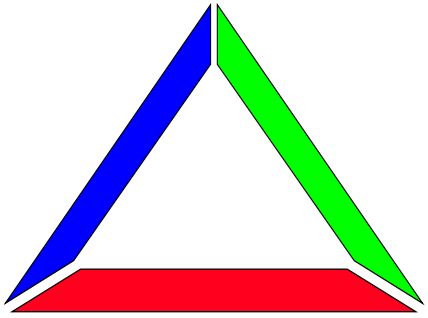


Source :
Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Sécuriser

Plans de sécurité (PSI-PCA)
Réglementation et Consignes
Sensibilisation
Formation
Responsabilisation de l'encadrement

Motivation des individus



Sécurité physique

Environnement de base
Contrôle d'accès
Risques de pollution
Risques d'incendie
Dégâts des eaux
Fiabilité du matériel

Sécurité logique

Accès au système
Système de sécurité
Gestion des mots de passe
Sécurité des télécommunications
Sécurité des données
Archivage / Désarchivage
Sauvegardes
Qualité des programmes

Evolution

- Il est important de comprendre que la sécurité est un **processus évolutif.**
- La gamme des services offerts par les technologies de l'information s'enrichit sans cesse et chaque innovation porte en elle son cortège d'opportunités et de menaces.
- Les menaces une fois identifiées, le marché offre rapidement des parades mais nous retrouvons ici aussi une loi veille comme le monde, celle de la lance et du bouclier.

Evolution

- Aucun produit ne peut, à lui seul, protéger entièrement une entreprise.
- La solution garantissant le risque zéro n'existe pas.
- La véritable sécurité émerge d'une association de produits et de services, auxquels s'ajoutent une politique de sécurité complète et l'engagement de respecter cette politique dans l'entreprise, du plus haut au plus bas de l'échelle.

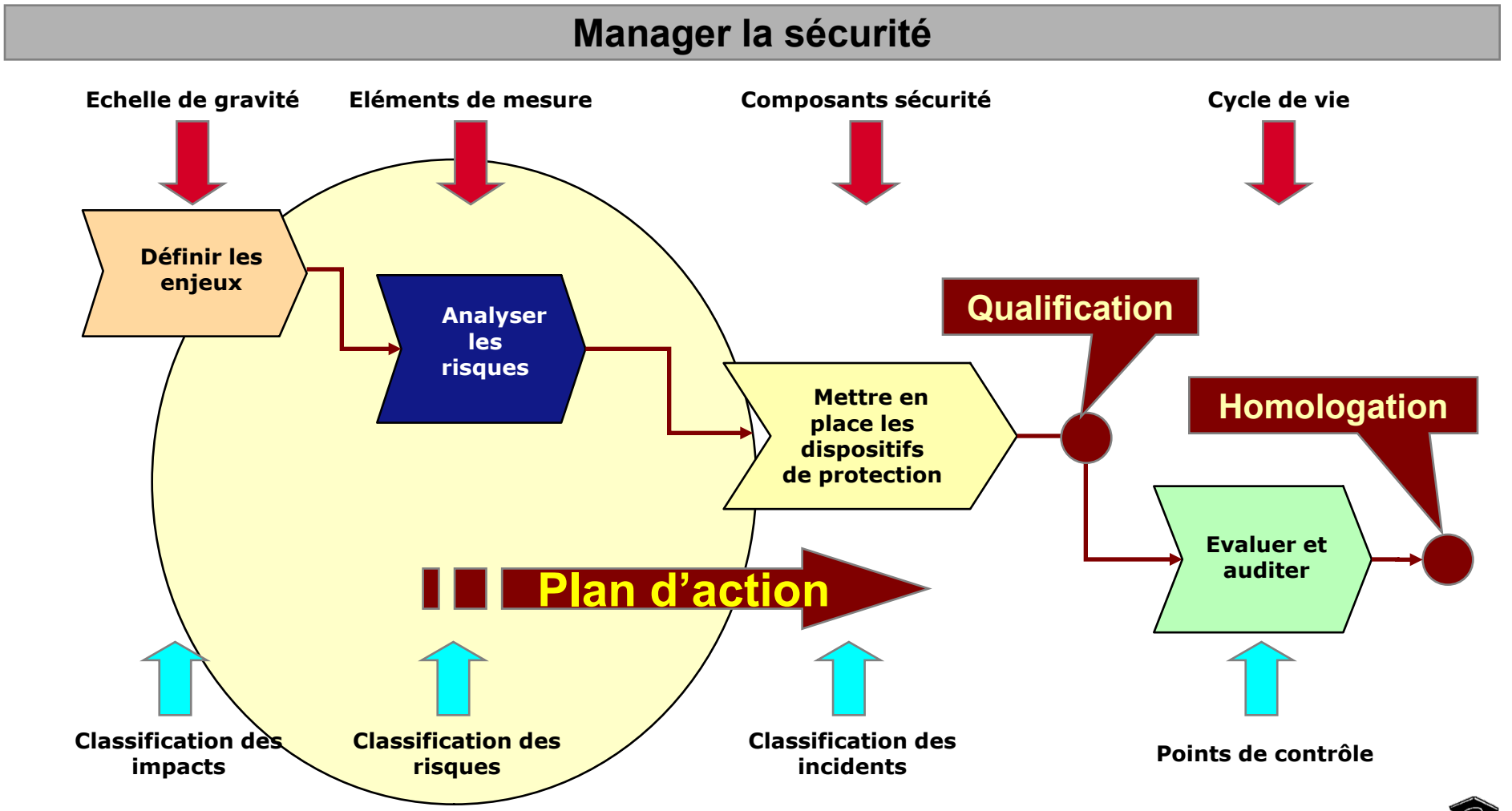
Evolution

- La sécurité des systèmes d'information, longtemps considérée comme une activité marginale à l'exception de quelques grands comptes héritiers d'une longue tradition de confidentialité, devient l'une des composantes critiques du projet d'entreprise.
- Les dirigeants d'entreprise doivent prendre conscience que celle-ci peut contribuer directement à **la création de valeur**.

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - *Le management de la sécurité dans l'entreprise.*
    - ***Comment construire un Plan sécurité. Le rôle du RSSI.***
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - *Assurance et financement des risques*

Plan d'action



Comment construire un Plan Sécurité

- Le **Plan de sécurité** est le document de référence définissant les objectifs poursuivis en matière de sécurité et les moyens mis en œuvre pour les assurer.
- Le Plan de sécurité définit un certain nombre de règles, de procédures et de bonnes pratiques permettant d'assurer un niveau de sécurité conforme aux besoins de l'organisation.
- Un tel document doit nécessairement être conduit comme un véritable projet associant des représentants des utilisateurs et conduit au plus haut niveau de la hiérarchie, afin qu'il soit accepté par tous.
- Lorsque la rédaction de la politique de sécurité est terminée, les clauses concernant le personnel doivent leur être communiquées, afin de donner à la politique de sécurité le maximum d'impact.
- Le Plan de sécurité est établi par le RSSI.

Le rôle du RSSI

- Le **RSSI** assure un rôle de conseil, d'assistance, d'information, de formation et d'alerte.
- Il peut intervenir directement sur tout ou partie des systèmes informatiques et télécoms de son entité.
- Il effectue un travail de veille technologique et réglementaire sur son domaine et propose des évolutions qu'il juge nécessaires pour garantir la sécurité logique et physique du système d'information dans son ensemble.
- Il est l'interface reconnu des exploitants et des chefs de projets mais aussi des experts et des intervenants extérieurs pour les problématiques de sécurité de tout ou partie du SI.
- Le RSSI est généralement rattaché à la direction informatique mais il peut être rattaché à la DG ou à une Direction de la Sécurité.
- D'après la définition de poste établie par le CIGREF.

Le rôle du RSSI

- Dans certains grands comptes, on voit apparaître deux missions correspondant au partage des responsabilités du RSSI entre deux interlocuteurs : l'un pour la maîtrise d'œuvre, et l'autre pour la maîtrise d'ouvrage.
  - Le CISO (*Chief Information Security Officer*), a une mission centrée sur la gestion des risques (Risk Manager) et l'organisation de la sécurité. Il participera aux réunions du Comité de Direction.
  - Le RSSI (Responsable Sécurité des Systèmes d'Information) a la responsabilité opérationnelle d'appliquer les règles à l'ensemble du domaine informatique. Il disposera d'un savoir-faire d'architecte technique de la sécurité et d'une parfaite connaissance des processus et des systèmes d'information.

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - *Le management de la sécurité dans l'entreprise.*
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - ***Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.***
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - *Assurance et financement des risques*

Les Certs

- Pas de violation de sécurité sans faille de sécurité :
  - soit par la négligence des administrateurs du système,
  - soit par des « défauts » des logiciels et matériels utilisés,
  - soit par des imprudences des utilisateurs.
- Pour lutter sur le front des « défauts », encore faut-il en être informé et en connaître les remèdes.
- La question a été jugée suffisamment sérieuse pour que les gouvernements décident de créer des organismes chargés de centraliser ces informations et d'en assurer la diffusion auprès des responsables informatiques des organisations publiques et privées.
- L'action des ***CERTs*** (*Computer Emergency Response Team*) est issue de cette volonté.
- D'autres organisations professionnelles proposent des référentiels sur le thème de la sécurité des SI.

Le CERTA

- http://www.certa.ssi.gouv.fr/
- Le ***CERTA*** (Centre d'expertise gouvernemental de réponse et de traitement des attaques informatiques) a été créé, en France, en janvier 1999, afin de renforcer la protection des réseaux de l'État face aux risques informatiques, quelle qu'en soit l'origine.
- Service du Premier ministre, rattaché à la Direction centrale de la sécurité des systèmes d'information (*DCSSI*) au sein du Secrétariat général de la défense nationale (*SGDN*), le *CERTA* est chargé d'assister les organismes de l'administration à mettre en place des moyens de protection et à résoudre les incidents ou les agressions informatiques dont ils sont victimes.
- Il participe au réseau mondial des *CERTs* et constitue le complément indispensable aux actions préventives déjà assurées par la *DCSSI* et qui se situent plus en amont dans la démarche de sécurisation des systèmes d'information.

Le CERTA

- Les deux principaux objectifs du *CERTA* sont d'assurer la détection des vulnérabilités et la résolution d'incidents concernant la sécurité des systèmes d'information (SSI) ainsi que l'aide à la mise en place de moyens permettant de se prémunir contre de futurs incidents.
- Afin d'assurer ces deux objectifs, les trois missions suivantes doivent être menées en parallèle :
  - assurer une veille technologique ;
  - organiser la mise en place d'un réseau de confiance ;
  - piloter la résolution d'un incident (si besoin en relation avec le réseau mondial des *CERTs*).
- Sur le plan international, le *CERTA* est membre du *FIRST* (*Forum of Incident Response and Security Teams*) et participe à l'activité *TF-CSIRT* (*Computer Security Incident Response Team*) qui est la coordination des *CERTs* européens.

Le CERTA

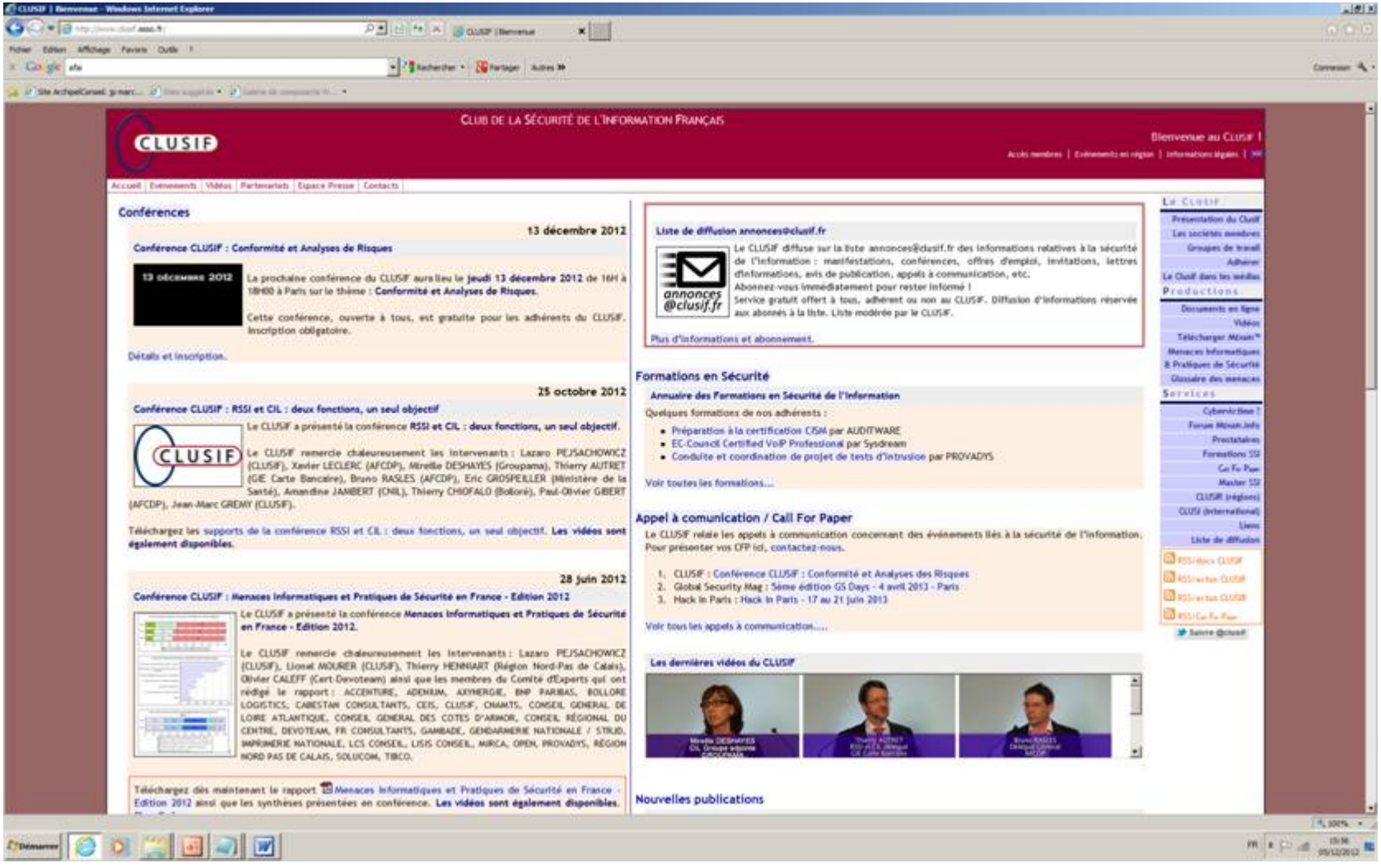
- http://www.cert-ist.com/
- Le ***CERT-IST*** (*Computer Emergency Response Team - Industrie, Services et Tertiaire*) est une association loi 1901, qui a pour vocation d'assurer à ses adhérents des services de prévention des risques et d'assistance au traitement d'incidents.
- Le *CERT-IST* est un centre d'alerte et de réaction aux attaques informatiques destiné aux entreprises françaises, membres du *FIRST* et possédant un certain nombre de partenaires, aux niveaux français et européen.
- Les activités principales sont les traitements préventifs des risques et curatifs des incidents.

Le Clusif

- http://www.clusif.asso.fr
- Le **Club de la Sécurité de l'Information Français** est un club professionnel, constitué en association indépendante, ouvert à toute entreprise ou collectivité.
- Il accueille des utilisateurs et des offreurs issus de tous les secteurs d'activité de l'économie.
- Objectif : agir pour la sécurité de l'information, facteur de pérennité des entreprises et des collectivités publiques.
- Le *Clusif* entend ainsi sensibiliser tous les acteurs en intégrant une dimension transversale dans ses groupes de réflexion : management des risques, droit, intelligence économique…
- Les groupes de travail traitent de thématiques variées en fonction de l'actualité, des besoins des membres…
- Le *Clusif* a des relais régionaux, les *ClusiR*, et des partenaires européens, les *ClusI*.
- Le *Clusif* réalise, entre autres activités, une enquête annuelle sur l'état des lieux de la sécurité informatique dans les entreprises et les administrations.

Les référentiels

Le Clusif



Le Cigref

- http://www.cigref.fr/
- Le ***Cigref***, réseau de Grandes Entreprises, est une association créée en 1970.
- Il regroupe plus de 130 grandes entreprises et organismes français dans tous les secteurs d'activité (banque, assurance, énergie, distribution, industrie, services…).
- Le *Cigref* a pour mission de :
  - Promouvoir la culture numérique comme source d'innovation et de performance ;
  - Rassembler les grandes entreprises utilisatrices de systèmes d'information afin de faire connaître les enjeux, les opportunités, contraintes et risques liés à l'usage des systèmes d'information et de communication.
  - Valoriser la fonction Systèmes d'information au sein des entreprises en favorisant auprès des DSI et de leurs collaborateurs, le partage des meilleures pratiques, les retours d'expérience et la gestion des connaissances en matière de systèmes d'information.

Les référentiels

Le Cigref

L'Afai

- http://www.afai.fr/
- **L'Association Française de l'Audit et du Conseil Informatique** a été fondée en 1982 dans le but de regrouper tous les professionnels concernés par la maîtrise des systèmes d'information et de favoriser le développement des méthodes et des techniques d'audit et de contrôle de l'informatique.
- L'AFAI a pour objectif de promouvoir l'emploi de méthodes et techniques contribuant à une meilleure maîtrise des systèmes d'information et à améliorer les compétences de tous les intervenants dans le domaine de l'audit et du conseil informatiques.
- Elle rassemble les professions de l'Audit, de l'informatique et du conseil autour de 3 pôles : la Gouvernance des SI, l'Audit et la **Sécurité**.
- L'AFAI est le chapitre français de l'ISACA, l'organisation internationale au service des professionnels de la Gouvernance des systèmes d'information.
- A ce titre, ses membres ont accès non seulement aux services de l'association AFAI, mais aussi à ceux proposés par l'ISACA.

Autres référentiels

- Le MEDEF a publié en mai 2005 un Guide de sensibilisation à la sécurisation du système d'information et du patrimoine informationnel de l'entreprise.
- http://www.ssi.gouv.fr : Agence Nationale de la Sécurité des Systèmes d'information.
- http://www.securite-informatique.gouv.fr/ : Le portail de la sécurité informatique.
- www.legalis.net : Aspects légaux de la sécurité des SI.
- http://www.ossir.org : L'OSSIR est une association du type loi 1901 existant depuis 1996 qui regroupe les utilisateurs intéressés par la sécurité des systèmes d'information et des réseaux.
- http://www.vulnerabilite.com : le portail dédié aux vulnérabilités détectées réalisé et mis à jour par la société *Isecurelabs*.

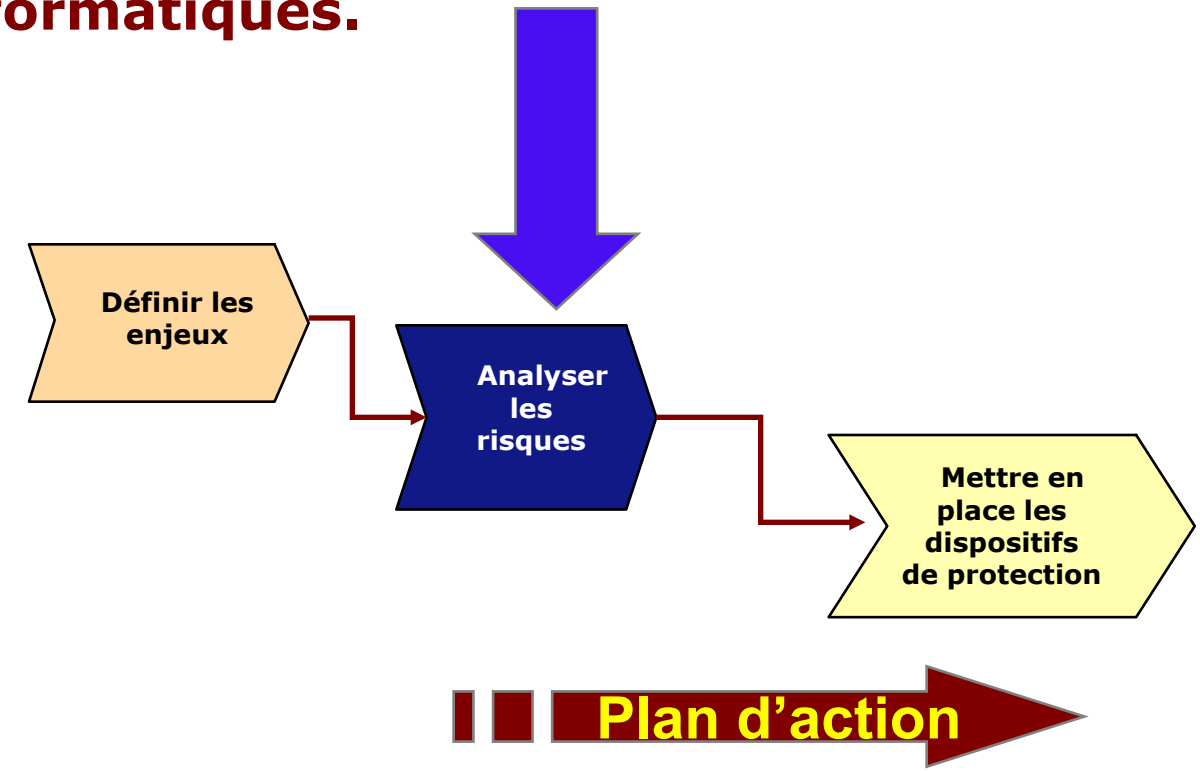
Agence Nationale de la Sécurité des Systèmes d'information

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - *Le management de la sécurité dans l'entreprise.*
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - ***Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.***
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - *Assurance et financement des risques*

Quelques méthodes

- MARION, MELISA, MEHARI et EBIOS sont différentes **méthodes d'évaluation des risques informatiques.**



Marion

- Méthode développée initialement en 1985, **Marion** est régulièrement améliorée et adaptée.
- Le risque est mesuré par sa gravité : évaluation de ses conséquence (impact) et, depuis 1993, de sa potentialité.
- 3 phases :
  - Phase 1 : analyse des risques (analyse de 17 scénarios types, mesure des risques, sélection des risques majeurs)
  - Phase 2 : analyse des vulnérabilités au travers de l'audit de 27 facteurs de sécurité (repose sur la réponse à un questionnaire de plus de 600 questions), pondération, synthèse
  - Phase 3 : définition du plan d'action, avec distinction des mesures prioritaires, secondaires de mise en cohérence, avec itérations et optimisation
- Avantages de la méthode :
  - Possibilité de se comparer aux autres entreprises d'un même secteur d'activité au travers de la note acquise
  - Existence de bases de connaissance mises à jour annuellement

Melisa

- **Mélisa** est une méthode d'auto-audit de sécurité développée initialement par la DGA (Direction générale de l'Armement) et la DCN (Direction des constructions navales) en 1985, puis étendue.
- Le risque est mesuré au travers de l'analyse des vulnérabilités grâce à l'étude d'évènements, sortes de mini-scénarios imagés et détaillés (environ 600 par base de connaissance).
- La vulnérabilité est considérée comme la résultante de la gravité des conséquences de l'évènement (impact), le risque de non détection de l'évènement, sa facilité de réalisation et du "facteur d'exposition structurelle" (c.a.d. la vulnérabilité liée aux sujets).
- Pour chaque mini-scénario, le choix d'une parade permet d'évaluer la vulnérabilité résiduelle.
- Avantages de la méthode :
  - Approche concrète,
  - Existence de bases de connaissance mises à jour annuellement, spécialisées par type de système et types de sensibilité (S : sensible, P : vitales, R : réseaux).

Méthodes d'analyse de risques

Mehari

- **Méhari** est une méthode développée par le CLUSIF (Club de la Sécurité Informatique Français) dans les années 1993 en partant des concepts de **Marion** et de **Melisa**.
- Le risque est mesurée au travers de l'étude de 6 facteurs de risques et 6 mesures de sécurité.
- La potentialité est considérée liée à 3 paramètres : l'exposition naturelle (attrait, ciblage), le niveau de risque pour l'agresseur (risque d'être identifié et sanctionné), le niveau des moyens requis (intellectuels, matériels, temporels)
- L'impact est considéré lié à 3 paramètres : l'analyse des dommages (matériels, données), les capacités de reprise (opérations, flux financiers, communication), la capacité de récupération financière.
- Les 6 mesures sont considérés comme ayant une influence sur un des facteurs : les mesures structurelles (localisation, architecture, organisation), dissuasives (identification, journalisation, sanctions), préventives (contrôle d'accès, détection, interception), de prévention (détection, intervention, non propagation), palliatives (restauration, reconfiguration, secours), de récupération (assurances, actions en justice).

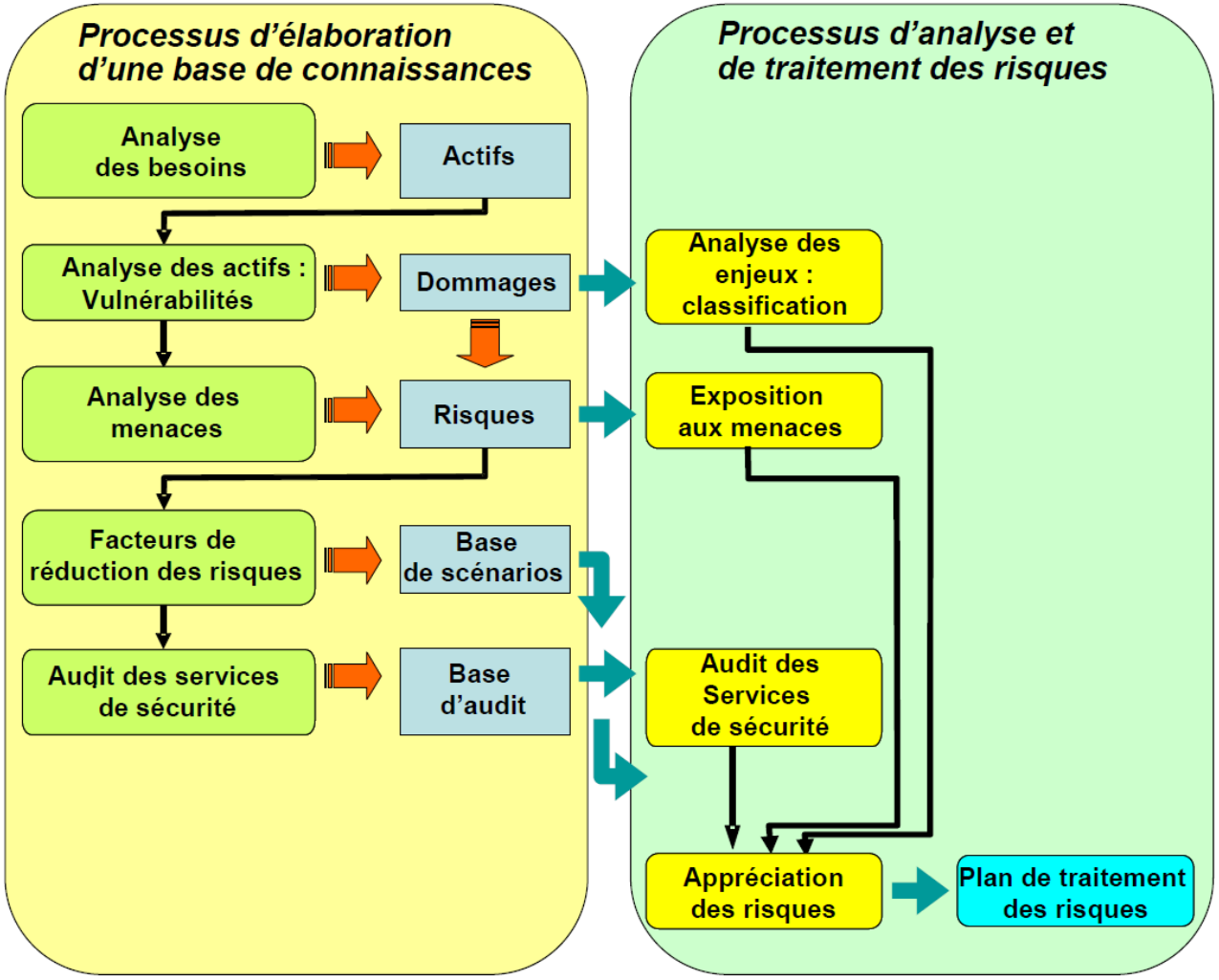
Méthodes d'analyse de risques

Mehari

- La méthode introduit 16 familles de services, décomposés en sous-service, et une base de connaissance basée sur 12 familels de scénarios de 10 scénarios chacune en moyenne
- Depuis 1995, la méthode distingue plans stratégiques et opérationnels, ce qui revient en fait à distinguer les mesures d'ordre global (mesures assurant la cohérence pour l'ensemble de l'entreprise) et local (plans réalisés par chaque entité : ressources locales)
- Avantages de la méthode :
- Depuis 1996, une approche globale, basée sur la classification des ressources, l'analyse d'un nombre limité de scénarios et l'évaluation de l'effet global des mesures a été mise en oeuvre. Elle est d'application plus rapide.

Méthodes d'analyse de risques

Mehari



Source :
Guide Mehari 2010 du clusif

Méthodes d'analyse de risques

Ebios

- EBIOS (Expression des besoins et identification des objectifs de sécurité), mise au point par la DCSSI (Direction centrale de la sécurité des systèmes d'information)
- http://www.ssi.gouv.fr/fr/confiance/ebios.html
- La méthode est compatible avec les normes internationales telles que l'ISO 13335 (GMITS), l'ISO 15408 (critères communs) et l'ISO 17799.
- Le risque de sécurité des systèmes d'information (SSI) est considéré une combinaison d'une menace et des pertes qu'elle peut engendrer.
- Chaque menace est l'objet d'un scénario qui met en jeu : une méthode d'attaque, les éléments menaçants susceptibles de l'employer (naturels ou humains, manière accidentelle ou délibérée), les vulnérabilités des entités (matériels, logiciels, réseaux, organisations, personnels, locaux), qui vont pouvoir être exploitées par les éléments menaçants dans le cadre de la méthode d'attaque.
- Les pertes sont estimées en termes d'atteinte des besoins de sécurité des éléments essentiels (le patrimoine informationnel et les processus associés) et d'impacts induits sur l'organisation.

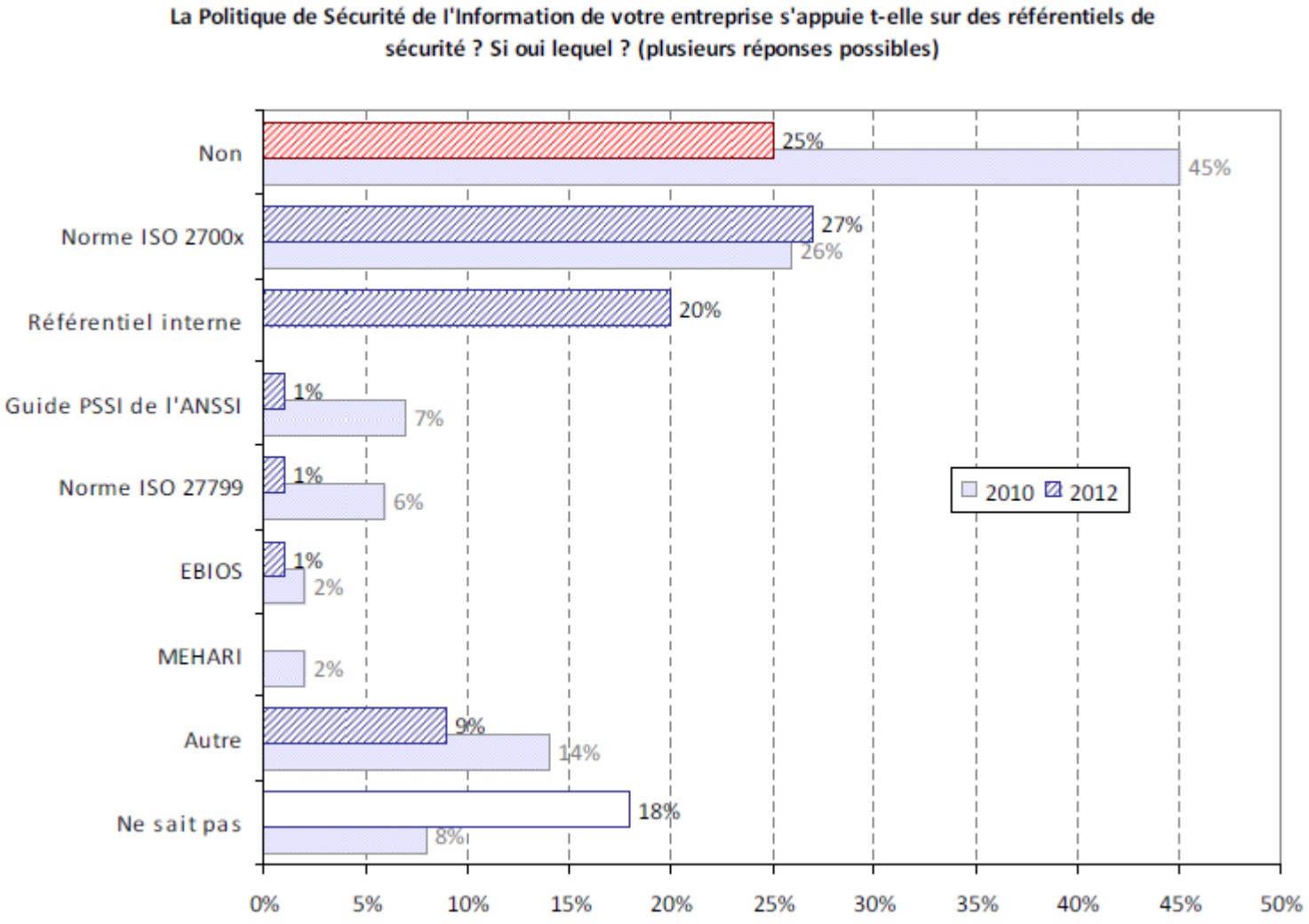
Méthodes d'analyse de risques

Ebios

- La gestion des risques SSI est considérée comme un processus continu et itératif en 4 phases :
  - Phase 1 : appréciation des risques ;
  - Phase 2 : traitement des risques ;
  - Phase 3 : acceptation des risques résiduels ;
  - Phase 4 : communication.
- Avantages de la méthode :
- Le referentiel est composé d'un ensemble d'outils pour découvrir la méthode, s'y former, la pratiquer et contribuer à son développement communautaire.
- La méthode est directement applicables à la plupart des secteurs, mais chacun peut l'adapter à son contexte particulier.
- Des éléments nécessaires à la prise de décision et à la gestion de celle-ci sont fournis (EBIOS est proposé comme un outil de négociation et d'arbitrage)
- Des formations gratuites sont assurées par la DCSSI pour les intervenants des organismes publics.

Méthodes d'analyse des risques

Répartition



Source :
Rapport Clusif 2012
Menaces informatiques et pratiques de sécurité
Enquête portant sur 351 entreprises

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - *Le management de la sécurité dans l'entreprise.*
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - ***Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.***
    - *Assurance et financement des risques*

Normes ISO pour la SSI

- *ISO 13335* : Concepts et modèles pour la gestion de la sécurité des TIC (1996),
- ***ISO 15408*** : Critères communs pour l'évaluation de la sécurité des Technologies de l'Information,
- *ISO/CEI 17799* : Code de bonnes pratiques pour la gestion de la sécurité d'information (ancienne référence de la norme *ISO/CEI 27002*).
- ***ISO/CEI 27001*** : Description des exigences pour la mise en place d'un Système de Management de la Sécurité de l'Information (SMSI).
- ***ISO/CEI 27002*** : Nouvelle mouture de la norme ISO/CEI 17799.
- *ISO/CEI 27005* : Proposition d'une méthode d'appréciation des risques (cette phase est obligatoire dans le cadre d'une certification ISO/CEI 27001).
- *ISO/CEI 27006* : Contient des informations sur le profile propre de l'auditeur 27001 et les règles de certfication.
- *ISO/CEI 27007* : Audit SMSI

Normes et réglementations

ISO 15408

- ***ISO 15408*** reprend les Critères Communs (CC) qui font la synthèse des critères à respecter en matière de sécurité pour les systèmes informatiques suivant les prescriptions européennes, américaines et canadiennes.
- Ils concernent principalement les systèmes directement impliqués dans la sécurité : anti-virus, authentification, PKI/KMI, contrôle biométrique, firewalls, IDS, systèmes d'accès, gestionnaires de réseaux, routeurs, switchs, hubs, VPN, ...voire les OS eux-mêmes.
- Les documents décrivant les Critères Communs sont disponibles sur le site de la DCSSI.
- Les CC sont structurés en trois publications:
  - Partie 1 : Introduction et modèle général
  - Partie 2 : Exigences fonctionnelles de sécurité
  - Partie 3 : Exigences d'assurance de sécurité.

Normes et réglementations

ISO 27001

- ***ISO 27001*** est une norme internationale qui traite de la gestion de la sécurité de l'information.
- Elle a été publiée en octobre 2005 et porte le titre : « Technologies de l'information - Techniques de sécurité - Systèmes de gestion de sécurité de l'information – Exigences ».
- La norme *ISO 27001* décrit comment mettre en place un Système de Gestion de la Sécurité de l'Information (SGSI) qui permet de choisir les mesures à mettre en place afin de protéger les actifs de l'entreprise.
- Elle préconise l'utilisation du modèle de qualité ***PDCA*** (*Deming*) pour : ***Plan*** (Planification de la réalisation), ***Do*** (Production, réalisation), ***Check*** (Contrôle, audit, vérification), et ***Act*** (Planification d'une nouvelle réalisation, mise en oeuvre d'actions correctrices) en vue de créer un cercle vertueux et un cycle d'amélioration continu pour établir le SGSI.
- *ISO 27001* constitue la base des règles de certification *ISO 27000*.

Normes et réglementations

ISO 27002

- ***ISO 27002*** est une norme internationale concernant la sécurité de l'information, publiée en 2005 par l'ISO, dont le titre en français est Code de bonnes pratiques pour la gestion de la sécurité de l'information .
- *ISO 27002* est un ensemble de 133 mesures dites « best practices » (bonnes pratiques), destinées à être utilisées par tous ceux qui sont responsables de la mise en place ou du maintien d'un Système de Management de la Sécurité de l'Information (SMSI).
- La sécurité de l'information est définie au sein de la norme comme la « préservation de la confidentialité, de l'intégrité et de la disponibilité de l'information ».
- Cette norme n'a pas de caractère obligatoire pour les entreprises.
- Son respect peut toutefois être mentionné dans un contrat : un prestataire de services pourrait ainsi s'engager à respecter les pratiques normalisées dans ses relations avec un client.

Les chapitres de l'ISO 27002

- Chapitre n° 01 : Champ d'application
- Chapitre n° 02 : Termes et définitions
- Chapitre n° 03 : Structure de la présente norme
- Chapitre n° 04 : Évaluation des risques et de traitement
- Chapitre n° 05 : Politique de sécurité de l'information
- Chapitre n° 06 : Organisation de la sécurité de l'information
- Chapitre n° 07 : Gestion des actifs
- Chapitre n° 08 : Sécurité liée aux ressources humaines
- Chapitre n° 09 : Sécurités physiques et environnementales
- Chapitre n° 10 : Exploitation et gestion des communications
- Chapitre n° 11 : Contrôle d'accès
- Chapitre n° 12 : Acquisition, développement et maintenance des systèmes d'informations
- Chapitre n° 13 : Gestion des incidents
- Chapitre n° 14 : Gestion de la continuité d'activité
- Chapitre n° 15 : Conformité

ISO

- Tous ces systèmes reposent sur une rationalité procédurale, basée plus sur la vérification du respect d'un référentiel que sur l'analyse de la pertinence d'un référentiel.
- Les dispositifs basés sur la rationalité procédurale ont du bon, sous réserve qu'ils ne se construisent pas au détriment de la rationalité substantielle, en l'occurrence la construction d'un système de sécurité efficient, dont la légèreté ne pénalise pas l'efficacité, et que chacun des accédants au SI ait pu se l'approprier.
- Or la lourdeur de ces dispositifs peut conduire à des « usines à gaz » inefficaces.
- Ne se contraindre à l'exercice que si :
  - L'entreprise est dans un environnement qui fait de la certification ISO 27001 une obligation légale.
  - L'entreprise noue des relations contractuelles avec un partenaire qui exige la certification ISO 27001.
  - L'entreprise recherche, par la certification ISO 27 001 un atout compétitif.

Informatique et Libertés

- La loi du 6 janvier 1978 sur l'informatique, les fichiers et les libertés a été préparée par les travaux de la commission **Informatique et libertés** créée en 1974.
- Cette loi marque une évolution notable dans les relations entre la société et l'informatique.
- La loi :
  - crée un organe veillant à son application : la Commission nationale de l'informatique et des libertés (CNIL) ;
  - assujettit à diverses formalités l'utilisation d'un fichier informatisé concernant les personnes ;
  - institue un droit d'accès en faveur des personnes concernées par un fichier.
- Après de nombreuses péripéties, la mise en conformité de la loi française avec les directives européennes de 1995 et de 2002 est effective.

Informatique et Libertés

- La loi modifiant la loi « Informatique et libertés » est entrée en vigueur dès sa promulgation.
- La loi n° 2004-801 du 6 août 2004 relative à la protection des personnes physiques à l'égard des traitements de données à caractère personnel et modifiant la loi n° 78-17 du 6 janvier 1978 relative à l'informatique, aux fichiers et aux libertés a été publiée au JO du 7 août 2004.
- Elle est immédiatement applicable, sauf pour ses dispositions nécessitant des précisions par décret comme celles sur les correspondants à la protection des données.
- Si la France était le premier pays européen à mettre en place une loi pour la protection des données, elle est aujourd'hui le dernier à transposer la directive européenne.
- Toutefois, si l'objectif assigné à l'origine visait à simplifier les procédures et à alléger les formalités, force est de constater que les entreprises sont dorénavant confrontées à des textes touffus, peu évidents à analyser, et qui, au contraire, conduisent à une multiplication des procédures.

Informatique et Libertés

- Tout traitement automatisé d'informations nominatives doit être déclaré auprès de la CNIL.
- Cette déclaration recouvre ce qu'on appelle les formalités préalables.
- Pour ce faire, il est prévu des bordereaux de déclaration que l'on trouve soit au siège de la CNIL, soit dans les préfectures et les chambres de commerce et d'industrie.
- Toute modification ou suppression de traitement doit être ultérieurement déclarée.
- La CNIL est supposée détenir de la sorte un fichier des fichiers en permanence à jour.
- Cette loi s'applique aussi bien aux entreprises privées qu'aux organismes publics.
- Dans tous les cas, la mise en œuvre du traitement doit être précédée de la déclaration qui donne lieu à l'émission d'un récépissé faisant foi.

RGPD

- À compter du 25 mai 2018, toute entreprise dans le monde traitant des données relatives à des citoyens de l'UE doit tenir compte du Règlement Général sur la Protection des Données (RGPD-GDPR).
- Ce texte ambitieux vise à standardiser les lois relatives à la confidentialité des données en Europe, à protéger la confidentialité des données des citoyens européens et à réformer l'approche des entreprises en matière de confidentialité des données.
- En cas de non-conformité, des amendes sévères, pouvant atteindre 20 millions d'euros ou 4 % du chiffre d'affaires annuel de l'exercice précédent, sont prévues (le montant le plus élevé des deux étant appliqué)

RGPD

- Le **Règlement Général de Protection des Données (RGPD)** est un texte réglementaire européen qui encadre le traitement des données de manière égalitaire sur tout le territoire de l'Union Européenne. Il est entré en application le 25 mai 2018.
- Le RGPD s'inscrit dans la continuité de la Loi française Informatique et Libertés de 1978 établissant des règles sur la collecte et l'utilisation des données sur le territoire français. Il a été conçu autour de 3 objectifs :
  - renforcer les droits des personnes
  - responsabiliser les acteurs traitant des données
  - crédibiliser la régulation grâce à une coopération renforcée entre les autorités de protection des données.
- https://www.cnil.fr/fr/reglement-europeen-protection-donnees

Plan

- **A. Les principes et les enjeux**
  - **C02 Enjeux économiques et modes d'action**
    - *Enjeux économiques*
    - *Le management de la sécurité dans l'entreprise.*
    - *Comment construire un Plan sécurité. Le rôle du RSSI.*
    - *Les référentiels : Certs, Clusif, Cigref, Afai, Portail gouvernemental de la sécurité informatique, etc.*
    - *Analyse des risques. Les méthodes (Ebios, Marion, Melisa, Mehari). Comparatif. Avantages et inconvénients.*
    - *Les aspects normatifs et la réglementation : ISO. CNIL. RGPD.*
    - ***Assurance et financement des risques***

Assurances

- En France, peu d'entreprises ont recours à des polices d'assurance pour se prémunir d'un sinistre informatique.
- Jusqu'en 2010, l'offre était quasi inexistante.
- La tendance est en train de s'inverser :
  - Couverture de l'accès frauduleux ou de l'utilisation illégale des ressources
  - Couverture du vol ou de la perte de données.
- Primes variant entre 1 et 3% du risque couvert.
- Couverture jusqu'à 100 M€.

Agenda

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - ***C03 Plan de secours et plan de continuité des activités***
  - *C04 Sécurité et banque*
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

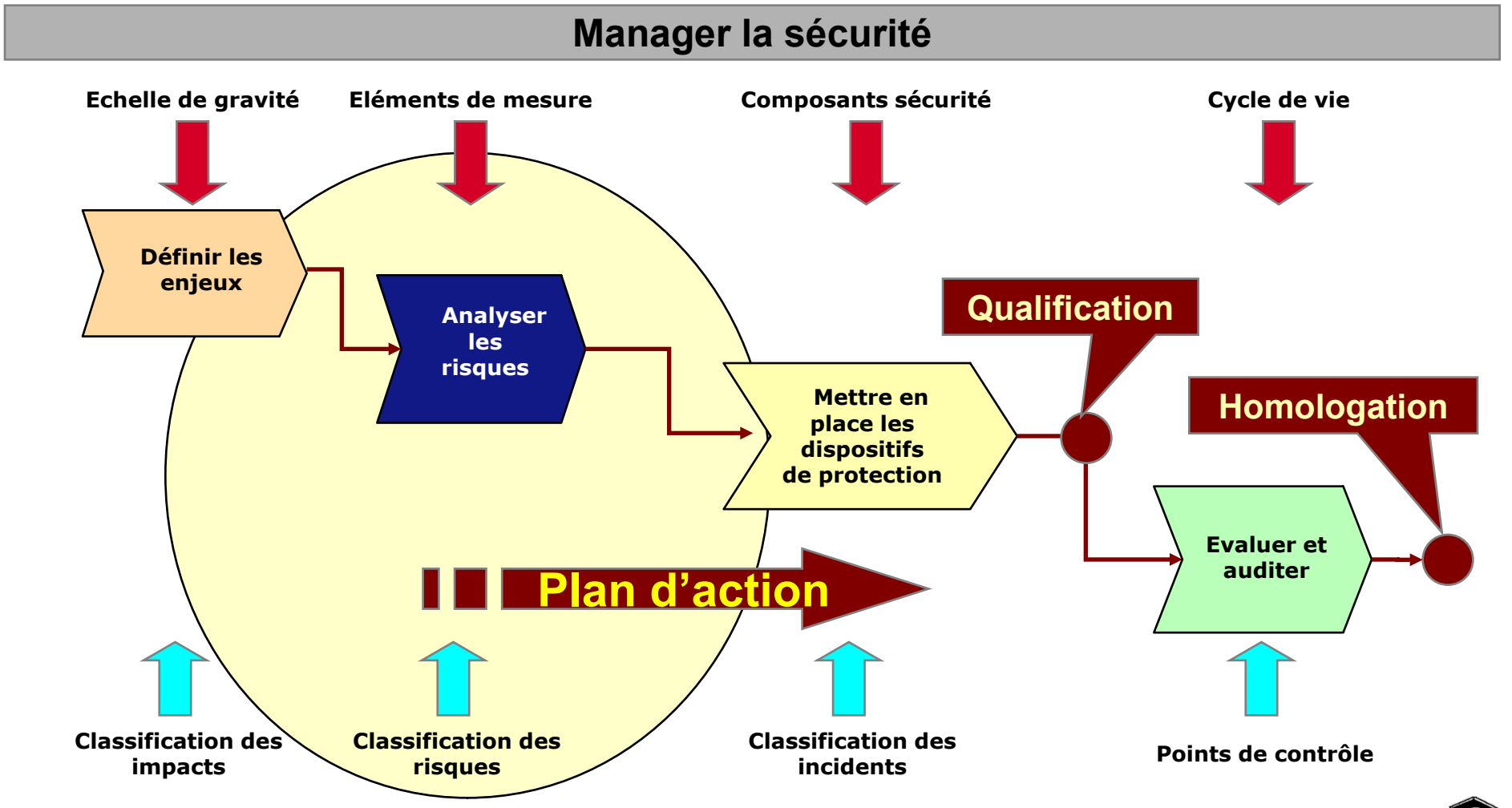
Plan

- **A. Les principes et les enjeux**
  - **C03 Plan de secours et plan de continuité des activités**
    - **Processus clefs en sécurité.**
    - *Plan de Reprise d'Activité (PRA), Plan de Secours Informatique (PSI - Disaster Recovery),*
    - *Plan de Continuité d'Activité (PCA - Business Continuity).*
    - *Etude de cas : Inondation chez GoodWater.*

Processus clefs en sécurité

- On ne peut pas éliminer tous les risques. On ne peut pas non plus les ignorer.
- Les questions clés sont les suivantes :
  - Quels sont les risques qui peuvent causer le plus de dégâts pour la société ?
  - Comment continuer les opérations courantes tout en essayant de résoudre le problème?
  - Avons-nous déjà formalisé un processus pour faire face?
- Les processus clés sont les suivants :
  - Identifier les menaces et évaluer les risques;
  - Reconnaître leur nature;
  - Evaluer leur impact potentiel;
  - Déterminer ce qui peut être fait pour atténuer leur impact;
  - Déterminer ce qui permet le meilleur ratio risques/coûts.

1 Plan d'action → Divers plans



Quels plans établir ?

- Alors que la prise de conscience sur les problèmes de reprise après incident est de plus en plus forte, les plans qui la concernent restent très limités dans leur ambition.
- De nombreux plans se limitent à préserver les moteurs du traitement de l'information et les canaux de transmission des données.
- Le périmètre de ces plans englobe normalement l'alerte, la restauration ainsi que les procédures techniques quotidiennes qui assurent la protection et le stockage des données critiques.
- Responsabilité et management restent souvent entre les mains de la DSI.

Quels plan établir ?

- Est-ce que votre programme prévoit ?
  - Un plan d'intervention d'urgence qui permette à l'entreprise de protéger ses actifs et d'atteindre ses objectifs de reprise d'activité.
  - Des activités de prévention pour réduire la probabilité et l'impact d'une perturbation.
  - Un programme permanent de sensibilisation des employés.

Plan

- ***A. Les principes et les enjeux***
  - ***C03 Plan de secours et plan de continuité des activités***
    - *Processus clefs en sécurité.*
    - ***Plan de Reprise d'Activité (PRA), Plan de Secours Informatique (PSI - Disaster Recovery),***
    - *Plan de Continuité d'Activité (PCA - Business Continuity).*
    - *Etude de cas : Inondation chez GoodWater.*

Plan de Secours Informatique

- Le "***Disaster Recovery Plan***" (Plan de Secours Informatique ou Plan de Reprise d'Activités) permet de restaurer une situation satisfaisante après un incident.
- Ce processus est essentiellement axé sur la restauration de l'infrastructure informatique et des ensembles de données.
- Contrairement à une idée communément répandue, il n'est pas indispensable de revenir directement à un niveau de disponibilité maximal.
- Une restauration séquencée dans le temps peut s'avérer plus efficace et plus économique.

Plan

- ***A. Les principes et les enjeux***
  - ***C03 Plan de secours et plan de continuité des activités***
    - *Processus clefs en sécurité.*
    - *Plan de Reprise d'Activité (PRA), Plan de Secours Informatique (PSI - Disaster Recovery),*
    - ***Plan de Continuité d'Activité (PCA - Business Continuity).***
    - *Etude de cas : Inondation chez GoodWater.*

Plan de Continuité des Activités

- C'est ici qu'intervient le concept de "***Business Continuity Plan***" (Plan de Continuité des Activités), processus anticipatif d'analyse des fonctions critiques de l'entreprise, d'identification des couples menaces/risques majeurs et d'évaluation de l'impact d'un incident éventuel.
- La continuité des activités s'inscrit dans une démarche de pérennité de l'entreprise.
- Elle consiste à mettre en place aux niveaux critiques du « business » des procédures visant à assurer le fonctionnement de ses activités clefs, ainsi que la disponibilité des ressources indispensables au déroulement de celles-ci.

Plan de Continuité des Activités

- Les organisations dépendent de plus en plus des postes de travail informatisés …
- … ainsi que des serveurs en réseau et des datacenters.
- La conséquence fut de propulser les budgets vers les sommets en y intégrant des plans de secours avec un grand nombre de ressources redondantes;
- Est-ce la bonne approche ?
- L ’assurance de la continuité des activités ne se limite pas au plan de secours et à la gestion de crise.
- Il s'agit d'un processus d'anticipation des incidents qui pourraient sérieusement affecter les fonctions et activités critiques de l'entreprise.

Plan

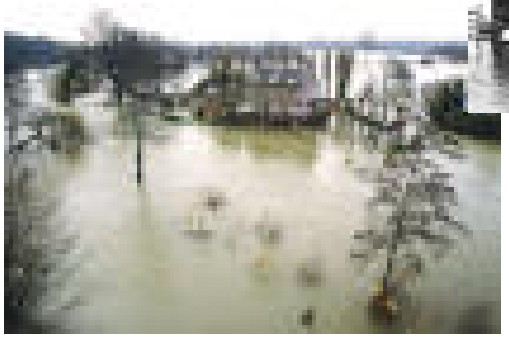
- **A. Les principes et les enjeux**
  - **C03 Plan de secours et plan de continuité des activités**
    - *Processus clefs en sécurité.*
    - *Plan de Reprise d'Activité (PRA), Plan de Secours Informatique (PSI - Disaster Recovery),*
    - *Plan de Continuité d'Activité (PCA - Business Continuity).*
    - ***Etude de cas : Inondation chez GoodWater.***

Etude de cas

- Nous considérons l'entreprise *Goodwater*, spécialiste de l'embouteillage et de la distribution d'eau minérale.

Etude de cas

Le désastre survient



Cette eau n'a rien à voir avec notre business

Etude de cas

- La plate-forme logistique de Goodwater, point central du réseau de distribution.
- Outils logistiques : magasins de stockage, quais de chargement, équipements de manutention, camions et chariots élévateurs.
- Outils informatiques : postes de travail connectés au réseau, application logistique (« supply chain ») sur les serveurs du datacenter.
- Vous êtes des managers et des partenaires impliqués dans les processus business of Goodwater.

Plan de Continuité des Activités

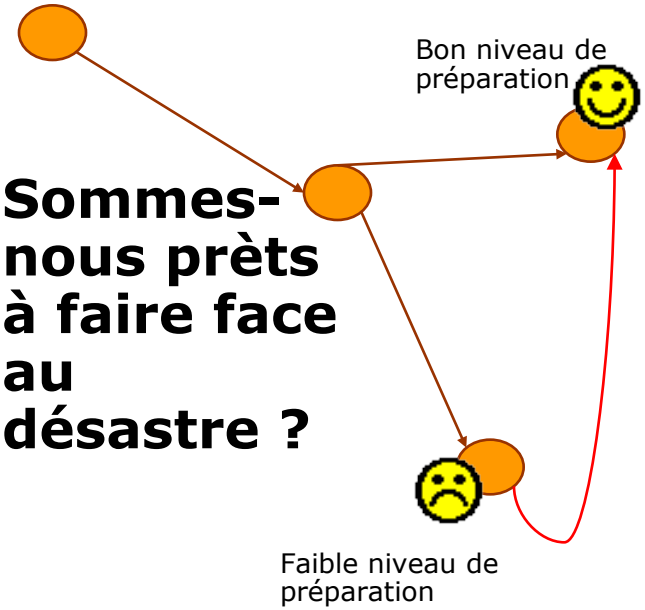
- M. A, Responsable de la plate-forme logistique, n'a pas éprouvé d'appréhension particulière lorsque la pluie a commencé, au matin du 3 juillet 2012 : « dans cette région, les fortes pluies sont une exception, même en été.
- La rivière n'était pas sortie de son lit depuis 1915, mais face à la montée continuelle des eaux, les responsables ont pensé qu'il était plus sage de prendre quelques précautions, comme de monter à l'étage quelques équipements critiques du rez-de-chaussée.
- Malheureusement, le désastre est intervenu avant que ces opérations aient pu être menés à terme, dans le courant de la nuit du 4 au 5.
- Des fortes pluies sur les collines alentour, combinées à la rupture d'une digue, ont entraîné le déferlement d'une vague d'eau et de boue sur les bas quartiers de la ville.

Etde de cas

- Nous sommes le matin du 5. Le personnel découvre le désastre.
- Le niveau d'eau dans la salle informatique est de 1,5 m.
- Dans le magasin et dans les ateliers, le niveau d'eau est de 2 m.
- Le dispositif d'embouteillage est pollué.
- Les empilements de packs de produits finis se sont effondrés. Les casiers de stockage inférieurs sont sous les eaux.
- Le niveau d'eau est si haut que, malgré les précautions prises, la totalité de l'équipement informatique est noyé.

Avons-nous un PCA ?

Le désastre survient



Nous n'avons pas de PCA

Nous avons un PCA

- ***C'est avant la catastrophe que nous nous sommes posé les questions suivantes***
- ***Qui ?***
- ***Quoi ?***
- ***Où ?***
- ***Quand ?***
- ***Comment ?***

Plan de Continuité des Activités

Qui ?

Etude de cas

Plan de Continuité des Activités

Qui ?

L'équipe (minimum) constituée en cellule de crise en charge de la continuité des activités :

- *1 représentant DRH (communication, procédures, administration, aspects réglementaires, soutien moral des équipes de secours et du personnel touché par la catastrophe),*
- *1 représentant D. Achats,*
- *1 représentant D. Production,*
- *1 représentant D. Com Ventes,*
- *1 représentant D (Com) Transport et logistique,*
- *3/4 représentants DSI (1 infra, 1 production et 1/2 SG concernés (ERP ?))*
- *1 Expert sécurité agissant en tant que coach (de préférence celui qui a piloté les « entraînements »)*

Plan de Continuité des Activités

Qui ?

- *Cette équipe « Continuité des Activités » (CA) est-elle construite ?*
- *Est-elle bien formée ?*
- *Quel est son leader ?*
- *Les responsabilités sont-elles définies ?*
- *Des entraînements sont-ils régulièrement organisés ?*

Plan de Continuité des Activités

Quoi ?

Etude de cas

Plan de Continuité des Activités

- ***Quoi ? Que doit faire la cellule de crise***
- *Mise en place d'une échelle de criticité allant de la "situation de désastre" à la "situation normale" et définition des seuils d'alerte.*
- *Evaluation des dommages et récupération de ce qui peut être récupérable (actifs SI).*
- *Relocation éventuelle sur des sites de back up.*
- *Etablissement d'une capacité SI/IT opérationnelle minimum en "**situation de désastre**" (les processus de rétablissement de la situation normale -Plan de Secours- sont tout juste démarrés).*
- *Etablissement d'une bonne capacité opérationnelle SI/IT en "**situation de crise**" ((les processus de rétablissement de la situation normale sont en régime permanent):*
  - *Comment basculer de la "situation de désastre" à la "situation de crise" ?*
  - *Modes opératoires en "situation de crise" ?*
- *Retour à la normale; le PRA est e place. ("**business as usual**"):*
  - *Comment rebasculer de la "situation de crise" à la "situation normale" ?*

Plan de Continuité des Activités

- **Quoi ?**
- *Que fallait-il faire avant pour diminuer les effets du risque (das le champ de l'analyse du risque, en amont du PCA, permettra d'allégr le PCA en éliinant certais risques (par exemple en mettant l'ensemble des actifs informatiques ?*
- *Prévoir le jour d'après ? Pour chaque situation :*
  - *Quelles applis opérationnelles ?*
  - *Quelles bases de données ?*
  - *Quelle infrastructure pour faire tourner les applis (serveurs) ?*
  - *Quels terminaux d'accès ? Pour qui ? (en liaison avec ceux qui travaillent sur les PCA prise de commandes / logistique vente/ Stocks / production / achats*
  - *Quel réseau pour accéder aux serveurs*
- *Solutions envisageables depuis le réseau local de PC avec un outil bureautique jusqu'à une version un peu allégée du SG habituel, selon l'état des actifs concernés*

Plan de Continuité des Activités

Où ?

Etude de cas

Plan de Continuité des Activités

Où ?

- *Préparer un local spécifique où sera hébergée la cellule de crise pendant la période critique.*
- *Cette cellule sera doté de moyens informatiques et de moyens de communication qui peuvent être basculés en condition opérationnelle à tout moment.*
- *Dans cette cellule on dispose de l'inventaire des moyens informatiques de l'entreprise et de leur emplacement, de manière à déterminer quelles ressources IT encore opérationnelles peuvent être immédiatement activées pour assurer les processus vitaux en situation de désastre et les processus principaux en situation de crise.*

Plan de Continuité des Activités

Quand ?

Plan de Continuité des Activités

Quand ?

- *Plan de travail de l'équipe.*
  - *1. Horaires de bureau (éventuellement étendus)?*
  - *2. H24 J7 (Nécessité d'organiser une rotation d'équipes en 3*8) ?*
- *La solution 1 est jugée suffisante, la 2 impliquant un triplement des effectifs hors de nos possibilités.*

Plan de Continuité des Activités

→ ***Comment ?***

Plan de Continuité des Activités

Comment ?

- *Disposer de documents précisant les méthodes, les procédures, les configurations et les données de références à mettre en oeuvre pendant la crise.*
- *Cette documentation est-elle correctement mise à jour ?*
- *Cette documentation sera-t-elle accessible aux membres de la cellule de crise le jour J ?*

Plan de Continuité des Activités

- ***Qui ?***
- ***Quoi ?***
- ***Où ?***
- ***Quand ?***
- ***Comment ?***

- *Les réponses à ces questions doivent être fournies avant le désastre ("Mieux vaut prévenir que guérir") dans le cadre de la stratégie et du plan "Continuité des Activités"*

Plan de Continuité des Activités

- Votre cellule de crise travaille avec le support d'une stratégie prédéterminée.
- Comment définir cette stratégie ...
- en ce qui concerne les objectifs ?
- en ce qui concerne les niveaux de décision ?
- en ce qui concerne le périmètre ?
- en ce qui concerne la flexibilité ?
- en ce qui concerne les ressources ?

Plan de Continuité des Activités

- ***en ce qui concerne les objectifs ?***
- *La stratégie doit s'assurer que l'entreprise est capable de répondre aux engagements qu'elle a pris avec ses clients.*
- *La stratégie doit s'assurer que l'entreprise est capable de protéger ses actifs et de revenir dans des délais raisonnables à une situation normale.*
- *La stratégie doit promouvoir les actions qui réduisent la probabilité et l'impact d'une interruption des activités.*
- *La stratégie doit assurer un programme de sensibilisation des employés.*

Plan de Continuité des Activités

- ***en ce qui concerne les niveaux de décision ?***
- *La stratégie doit être définie au niveau du conseil d'administration, conçue et déployée comme un élément entièrement intégré dans la structure de l'organisation.*
- *Mais la continuité des activités implique l'ensemble de la société.*
- *Les managers de rang intermédiaire (middle management) doivent être sensibilisés aux risques du niveau tactique : risques sur les prix et sur l'approvisionnement des matières premières, risques sur l'indisponibilité de compétences clefs, etc.*
- *Il est indispensable que ces managers soient régulièrement impliqués dans l'évaluation de ces risques et dans l'élaboration des processus qui visent à les réduire ou à diminuer leur impact.*
- *De la même manière, les collaborateurs sur le terrain doivent savoir évaluer les risques opérationnels qui peuvent perturber les plans les mieux établis.*
- *Il est important que cadres et collaborateurs sachent identifier les menaces qui pèsent sur la performance, la compétitivité et la pérennité de l'entreprise.*

Plan de Continuité des Activités

- ***en ce qui concerne le périmètre ?***
- *La stratégie doit être conçue à l'échelle de l'organisation.*
- *Elle doit être transverse et traverser le cloisonnement vertical des services (production, commerce, finance, ressources humaines and SI).*

Plan de Continuité des Activités

- ***en ce qui concerne la flexibilité ?***
- *La stratégie doit refléter la manière dont l'organisation interagit avec son environnement et être capable de s'adapter aux changements de celui-ci.*
- *Elle doit être capable de faire face, non seulement aux besoins exprimés explicitement aujourd'hui, mais aussi anticiper les demandes futures implicitement contenues dans l'organisation et dans son environnement.*

Plan de Continuité des Activités

- ***en ce qui concerne les ressources ?***
- *La stratégie doit pouvoir s'appuyer sur la disponibilité de ressources adéquates.*
- *La qualité de ces ressources est aussi importante que leur quantité.*
- *Elles doivent donc être sélectionnées et déployées en fonction de la nature et du périmètre du travail à fournir pendant la crise, et ce avec le meilleur ratio qualité/coût*

Plan de Continuité des Activités

- Votre cellule de crise travaille avec le support d'un plan couvrant tous les aspects d'un possible et futur désastre.
- Comment définir ce plan ...
- en ce qui concerne les concepts ?
- en ce qui concerne les acteurs ?
- en ce qui concerne les ressources ?
- en ce qui concerne les processus ?
- en ce qui concerne les indicateurs ?

Plan de Continuité des Activités

- ***en ce qui concerne les concepts ?***

Plan de Continuité des Activités

- ***en ce qui concerne les concepts ?***
- *Définir ce qu'est un désastre.*
- *Identifier le périmètre du plan (en accord avec la stratégie)*
- *Déclarer explicitement sur quelles bases, hypothèses et conjectures le plan est établi.*

Plan de Continuité des Activités

- ***en ce qui concerne les acteurs ?***

Plan de Continuité des Activités

- ***en ce qui concerne les acteurs ?***
- *Identifier les composantes de l'organisation (siège, établissements -ateliers, magasins, agences, ...-, Directions, Unités d'affaires (Business Units) concernées par la continuité des activités.*
- *Identifier les responsables et leurs adjoints*
- *Identifier les correspondants de la cellule de crise et leur back up*
- *Assigner les rôles et les responsabilités de chacun*
- *Tenir à jour un annuaire avec toutes les données nécessaires pour les contacts et échanges internes et externes*

Plan de Continuité des Activités

- ***en ce qui concerne les ressources ?***

Plan de Continuité des Activités

- ***en ce qui concerne les ressources ?***
- *Identifier et préparer deux ou trois locaux, géographiquement séparés pour ne pas être simultanément indisponibles, capables d'héberger la cellule de crise.*
- *Identifier les documents et les matériels vitaux, en incluant leurs back ups, et spécifier les modes d'accès à ces documents.*
- *Identifier les besoins en ressources diverses, préciser comment elles doivent être approvisionnées et selon quel planning.*

Plan de Continuité des Activités

- ***en ce qui concerne les processus ?***

Plan de Continuité des Activités

- ***en ce qui concerne les processus ?***
- *Formaliser le processus d'escalade dans les différents niveaux de crise, de l'incident à la déclaration de désastre.*
- *Formaliser les procédures d'alerte, de mise en sécurité et d'évacuation.*
- *Identifier, décrire et hiérarchiser les priorités pour les actions visant la continuité des activités.*
- *Identifier, décrire et hiérarchiser les priorités pour les actions visant au retour à la normale.*

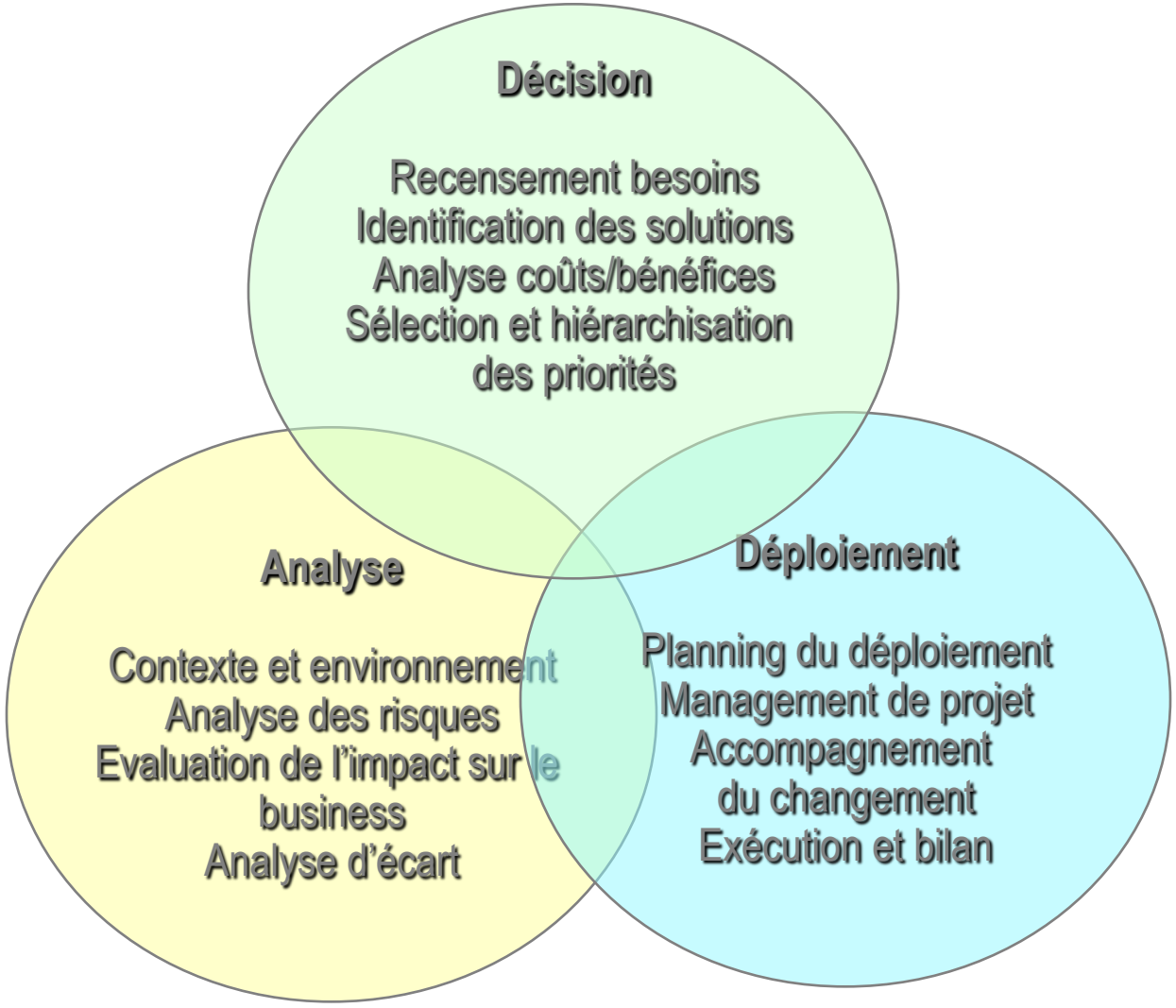
Plan de Continuité des Activités

- ***en ce qui concerne les indicateurs ?***

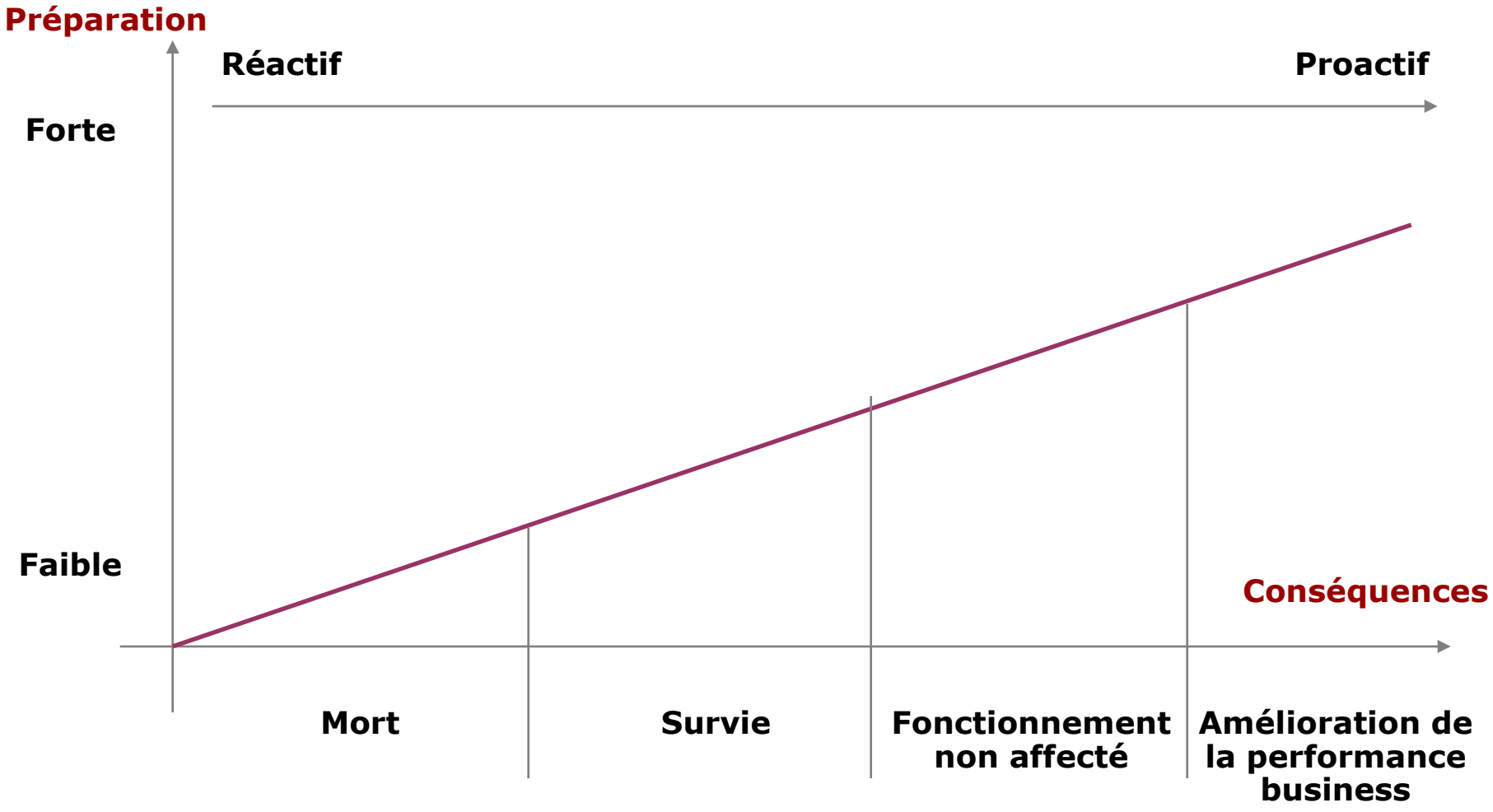
Plan de Continuité des Activités

- ***en ce qui concerne les indicateurs ?***
- *Avez-vous défini les indicateurs pour vérifier que votre plan ....*
- *permet réellement d'atteindre les objectifs de continuité définis ?*
- *permet efficacement de respecter les engagements pris vis à vis des clients ?*
- *permet de respecter les obligations fiduciaires (maintien de la valeur de la société) ?*
- *permet de minimiser l'exposition aux risques financiers, juridiques et réglementaires.*

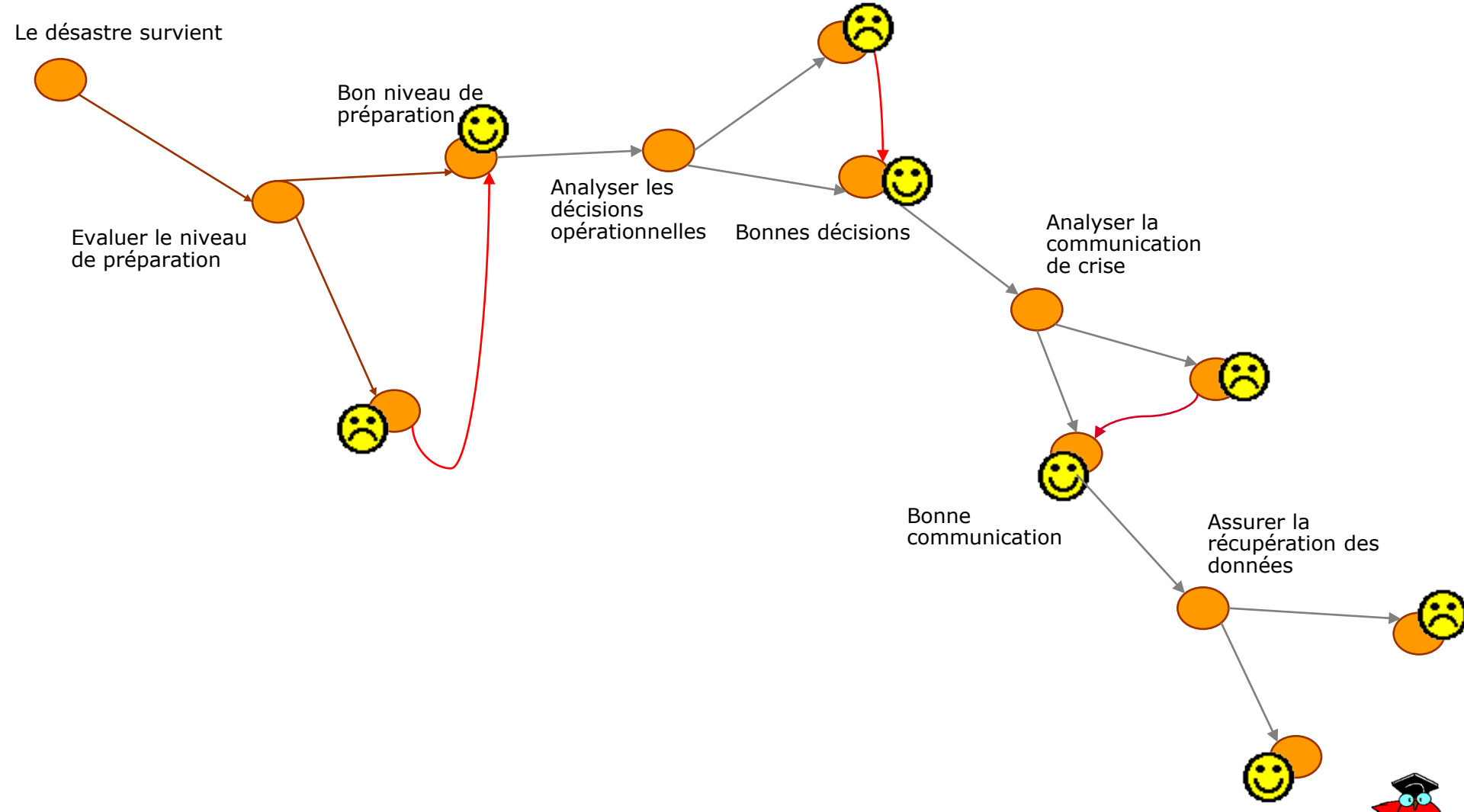
Plan de Continuité des Activités



Plan de Continuité des Activités



Plan de Continuité des Activités



Plan

- ***A. Les principes et les enjeux***
  - *C01 Aspects et enjeux de la sécurité*
  - *C02 Enjeux économiques et modes d'action*
  - *C03 Plan de secours et plan de continuité des activités*
  - ***C04 Sécurité et banque***
- ***B. Les méthodes et les outils***
  - *C05 Renforcer la sécurité des données. Cryptographie et cryptanalyse. Architectures de sécurité*
  - *C06 Renforcer la sécurité des réseaux et des systèmes*
  - *C07 Renforcer la sécurité des accès et des contrôle d'identités*
  - *C08 Renforcer la sécurité des applications et des services*
  - *C09 Renforcer la sécurité des dispositifs mobiles*
  - *C10 Evaluer la sécurité*
  - *C11 Manager les risques dans les projets SI*
- ***C. Bilan et perspectives***

Plan

- **A. Les principes et les enjeux**
  - **C04 Sécurité et commerce électronique. Sécurité et banque**
    - **Le besoin de sécurité »**
    - **Le risque SI parmi les autres risques bancaires**
    - Intranet bancaire
    - Sécurisation de la banque en ligne
    - Sécurisation des paiements (A remonter)
    - Tendances générales

Problématique SI Banque

- L'informatique joue un rôle stratégique dans les banques.
- Tout difficulté engendrée par un défaut de sécurité peut avoir des répercussions pour l'établissement et pour ses clients.
- Cas particulièrement grave si des données disparaissent ou, plus grave, si les règlements de toute nature et notamment le remboursement des dépôts sont compromis.
- Les risques induits par les défaillances informatiques sont plus élevés dans les établissements de crédit que pour d'autres secteurs de l'économie parce qu'ils peuvent également entraîner des conséquences fâcheuses pour les autres établissements qui sont en relation avec lui, et même, à la limite, avoir des répercussions pour la Place et pour l'économie nationale si l'incident était de nature à provoquer un "risque systémique".

Problématique SI Banque

- Pour les établissements de crédit, l'informatique est devenue un "outil de production" principal et "incontournable" : les valeurs monétaires, dématérialisées, sont contenues, stockées, transportées, valorisées grâce à elle.
- L'impact des problèmes que peut rencontrer une banque, lorsque la sécurité de son système d'information n'est plus assurée, est important et rapide.
- Les mouvements financiers ayant été multipliés et complexifiés par l'usage des outils informatiques et télématiques, l'effet de masse et de technicité des opérations empêche, comme par le passé, de reconstituer facilement celles-ci à partir de bordereaux papiers ou de "preuves physiques".

Problématique SI Banque

- Implications de Bâle II pour la sécurité informatique
  - PCA : Plan de Continuité d'Activité
  - Protection des données servant aux calculs règlementaires
    - Cloisonnement des applications manipulant ces données
    - Contrôles dans les transmissions : chiffrement lors des transferts et authentification des parties
    - Journalisation des incidents de sécurité
  - Sécurité dans les communication aux tiers (Commission Bancaire, CAC, ...)
  - Constitution d'une base d'incidents
  - Consolidation de la journalisation à la fois technique et fonctionnelle

Plan

- ***A. Les principes et les enjeux***
  - ***C04 Sécurité et banque***
    - *Le risque SI parmi les autres risques bancaires*
    - ***Intranet bancaire***
    - *Sécurisation de la banque en ligne*
    - *Sécurisation des paiements*
    - *Tendances générales*

Problématique Intranet Banque

- En termes de sécurité, une banque construisant son intranet a à concilier les héritages spécifiques et antagonistes des réseaux internes privés traditionnels et des réseaux IP ouverts.
- Les réseaux internes classiques étaient caractérisés par une administration structurée et un environnement de confiance.
- Les réseaux Intranet héritent de l'Internet une technologie IP ouverte et très répandue, une vulnérabilité à des accès potentiellement hostiles.
- Afin de protéger le SI supporté par ce réseau contre les menaces, il est nécessaire d'établir une démarche préliminaire d'analyse de ces nouveaux risques.
- Ensuite il convient d'adopter des solutions techniques adaptées, associées à des procédures impliquant la banque sur le long terme, permettant de contrer les attaques qui surviendrnt inévitablement dès que la valeur de l'information est importante.

Problématique Intranet Banque

- En termes de sécurité, une banque construisant son intranet a à concilier les héritages spécifiques et antagonistes des réseaux internes privés traditionnels et des réseaux IP ouverts.
- Les réseaux internes classiques étaient caractérisés par une administration structurée et un environnement de confiance.
- Les réseaux Intranet héritent de l'Internet une technologie IP ouverte et très répandue, une vulnérabilité à des accès potentiellement hostiles.
- Afin de protéger le SI supporté par ce réseau contre les menaces, il est nécessaire d'établir une démarche préliminaire d'analyse de ces nouveaux risques.
- Ensuite il convient d'adopter des solutions techniques adaptées, associées à des procédures impliquant la banque sur le long terme, permettant de contrer les attaques qui surviendront inévitablement dès que la valeur de l'information est importante.

Les risques associés

- Sur les postes de travail :
  - Les codes mobiles : Java, Active X, plugs in);
  - Les cookies;
  - Les demandes de liens ou de raccourcis;
  - Le *Netcasting* (inscription auprès d'un serveur pour recevoir des infos en *push*).
- Sur les serveurs
  - Partage des ressources sur des serveurs partagés, non dédiés;
  - Configurations inadéquates
  - Modules de scripts type CGI-BIB
  - Substitution du serveur
  - Compromission des systèmes de sécurité
  - Déni de services suite à un bombardement de trames
- Des solutions existent face à tous ces risques

Plan

- **A. Les principes et les enjeux**
  - **C04 Sécurité et banque**
    - *Le risque SI parmi les autres risques bancaires*
    - *Intranet bancaire*
    - ***Sécurisation de la banque en ligne***
    - *Sécurisation des paiements*
    - *Tendances générales*

Le besoin de sécurité

- Tout système de banque en ligne, mettant en jeu des flux financiers, doit se conformer à nos quatre exigences de base :
  - **Confidentialité** : l'information n'est accessible que par les parties autorisées.
  - **Intégrité** : les messages ne doivent pas être altérés ou modifiés
  - **Authentification** : l'expéditeur et le destinataire doivent se prouver mutuellement leur identité.
  - **Non-répudiation** : une transaction effectivement et normalement passée ne doit pas pouvoir être contestée.

Le besoin de sécurité

- Le plus gros problème concerne la sécurité des données transmises lors des transactions financières.
- Besoin de chiffrement pour empêcher le piratage d'informations confidentielles transitant sur le réseau.
- Besoin d'authentification pour certifier l'identité de l 'interlocuteur : un fournisseur de services doit être sûr de l 'identité et de la solvabilité du client, mais le client doit être certain de s 'adresser au prestataire désiré.

Le besoin de sécurité

- Les pirates ciblent particulièrement les réseaux bancaires.
- Les opérations des forces de police menées à l'échelle internationale parviennent régulièrement à démanteler des réseaux de cybercrime, démontrant, du même coup, l'omniprésence de cette menace.
- Récemment aux États-Unis, le FBI a découvert un réseaux de fraude bancaire en ligne qui a permis le détournement de 20 millions de dollars, transférés en Chine.
- À la fin de l'année dernière (2011) dans le cadre de l'Opération *Trident Breach*, les forces de l'ordre des Pays-bas, d'Ukraine, des États-Unis et du Royaume-Uni ont arrêté 150 personnes, membres d'un groupe de cybercriminels qui avait tenté de voler 220 millions de dollars via des services de banque en ligne et réussi à provoquer la perte de 70 millions de dollars.
- Enfin, une étude réalisée en 2011 par l'Institut *Ponemon* portant sur la sécurité des banques d'affaires a révélé qu'aux États-Unis, 42 % des petites entreprises ont été victimes d'une fraude bancaire en ligne l'an passé.

Plan

- **A. Les principes et les enjeux**
  - **C04 Sécurité et banque**
    - *Le risque SI parmi les autres risques bancaires*
    - *Intranet bancaire*
    - *Sécurisation de la banque en ligne*
    - ***Sécurisation des paiements***
    - *Tendances générales*

Sécurisation des paiements

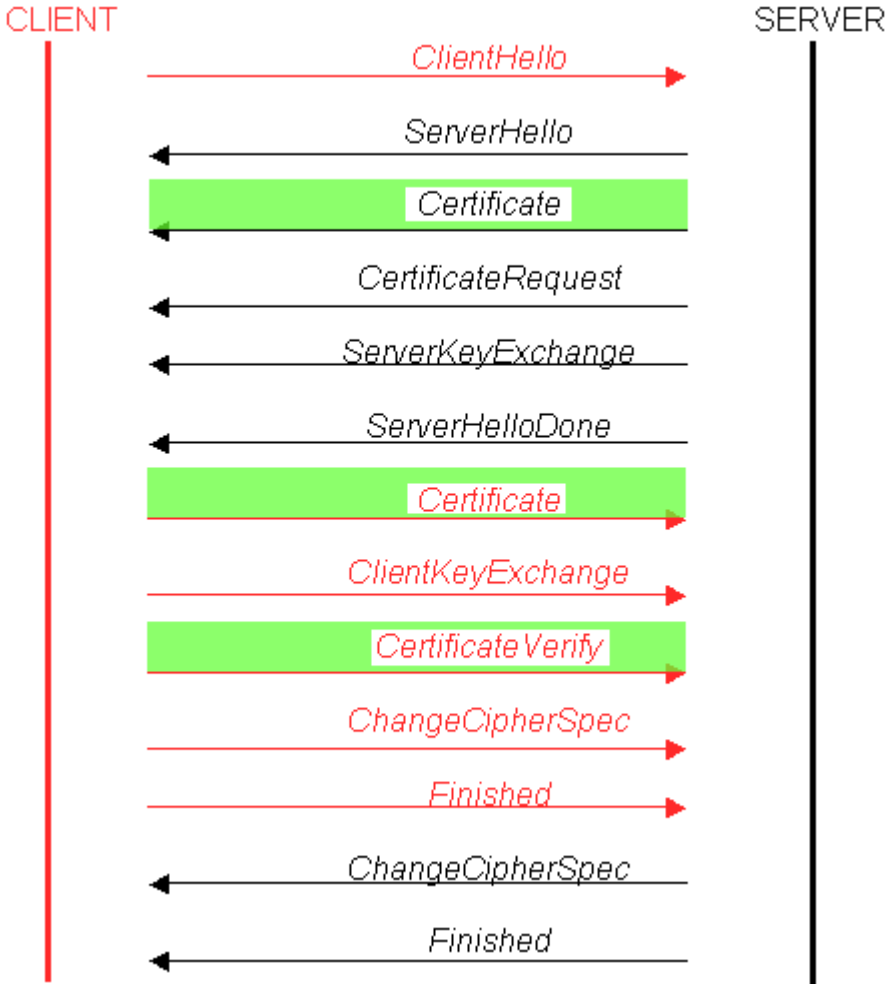
- Le client commande en remplissant sa page HTML sur le Web, mais les paiements s'opèrent de manière classique.
- Monnaie virtuelle d'un porte monnaie électronique
- L'encryptage de la page saisie.
- Les cartes de crédits couplées à des lecteurs dont le code est crypté à la base.
- Les chèques électroniques avec pour intermédiaire une banque en ligne : cas du tiers de confiance -ou « cybernotaire », exemple type de télémédiation- , secteur sur lequel les établissements financiers cherchent à se positionner.

HTTP sécurisé

- SSL (*Secure Sockets Layer*): protocole de cryptage utilisé par Netscape pour son navigateur et son serveur Web Netscape Commercial Server. Il a été adopté par Microsoft dans IIS.
- SSL crypte, authentifie et assurer l'intégrité des données transitant au travers de connexions TCP/IP..
- Algorithme RSA à clef publique.
- Cryptage des requêtes et des réponses HTTP.
- Cryptage de l'URL demandée, du contenu (No de carte de crédit), des autorisations d'accès (usernames, passwords) et de les données retournées au client par le serveur visité.
- Un serveur sécurisé a une URL https://
- Un autre protocole, S/HTTP (Secure HyperText Transfer Protocol) permet de choisir son algorithme de chiffrement.

Sécurité des paiements

HTTP sécurisé



Déroulement normal d'une transaction SSL avec une authentification mutuelle.

En noir, échanges initiés par le serveur
En rouge, échanges initiés par le client

HTTP sécurisé

- SSL a été remplacé en 1999 (RFC 2246) par TLS (IETF a acquis la licence de Netscape)
- TLS (*Transport Layer Security*) est un protocole standard de l'IETF, dont la dernière mise à jour est le RFC 5246.
- IETF (*Internet Engineering Task Force*) développe et assure la promotion des standards de l'Internet, en étroite collaboration avec les autres organisations normatives du monde de l'Internet, W3C and ISO/IEC.
- L'IETF est un groupe informel, sans statut, sans membre, sans adhésion.
- Le travail technique est accompli dans une centaine de groupes de travail.
- Tous les participants et managers sont des volontaires.

Sécurité des paiements

Norme SET (Secure Electronic Transaction)

- *Mastercard* et *Visa*, les deux principaux réseaux mondiaux de cartes de paiement, se sont associés en 1996 pour poursuivre des travaux déjà engagés sur la sécurisation des transactions et ont défini un protocole standard baptisé SET (*Secure Electronic Transaction*).
- Ce standard, qui allait plus loin que SSL (qu'il intègrait) ou S-HTTP, visait à permettre l'utilisation de la carte bancaire sur Internet en garantissant :
  - La confidentialité et l'intégrité des données transmises,
  - L'authentification du compte du porteur de la carte.,
  - L'authentification du commerçant,
  - L'interopérabilité entre les diverses plates-formes.

Sécurité des paiements

Norme SET (Secure Electronic Transaction)

- Il avait reçu le support de *Microsoft*, *IBM* et *Netscape*.
- Malgré ses atouts, SET n'a pas réussi à être massivement adopté par le marché, notamment à cause du coût et de la complexité supporté par le commerçant (comparé à l'alternative proposée par la seule protection du transport par SSL) et à cause de la logistique nécessaire à la distribution des certificats et l'installation des logiciels clients.
- Le protocole SET n'est plus opérationnel depuis le début des années 2000, *Visa* et *MasterCard* l'ayant remplacé par 3-D Secure.

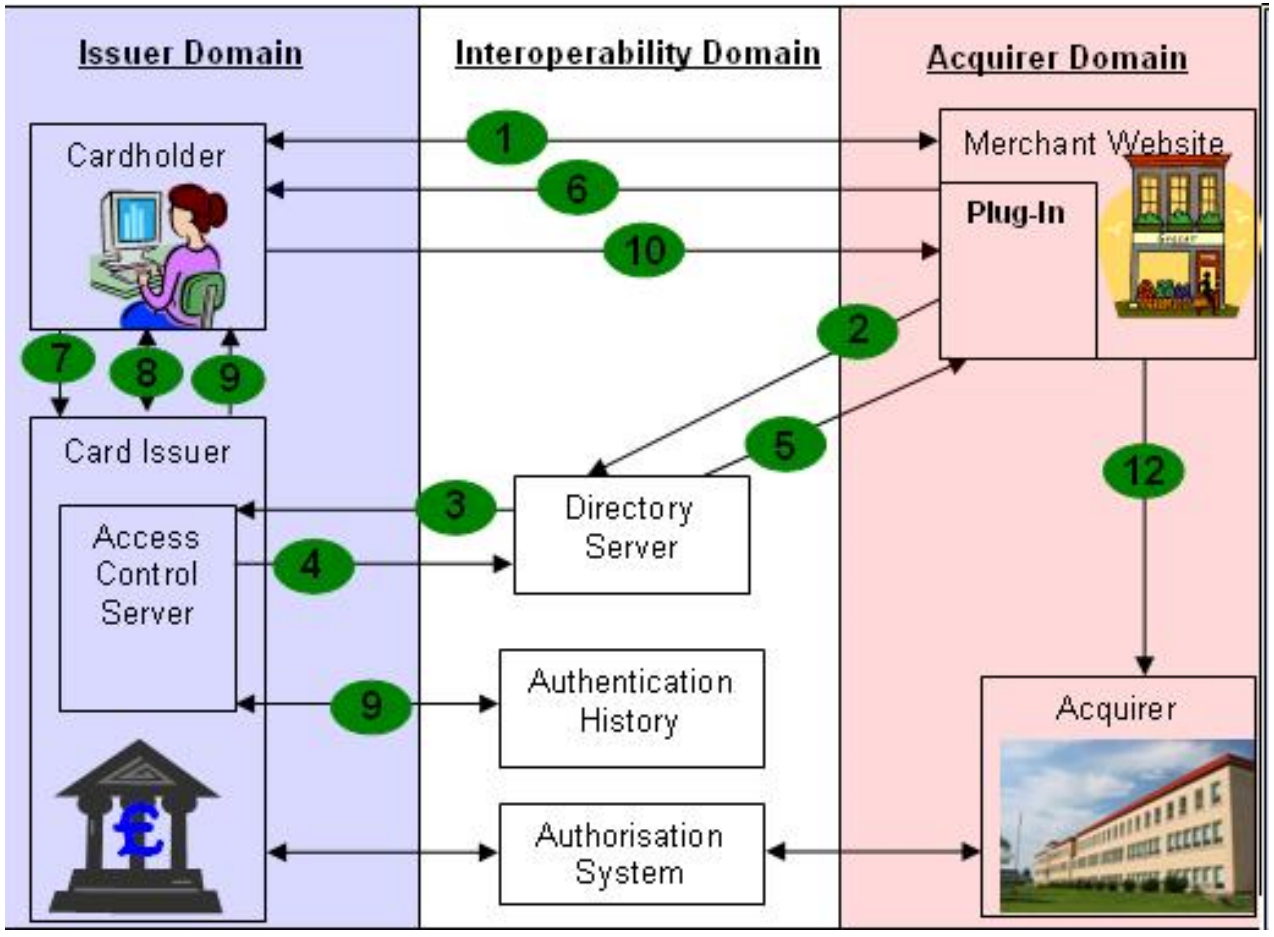
Sécurité des paiements

Norme 3-D Secure

- *3-D Secure* a été développé par *Visa* pour augmenter le niveau de sécurité des transactions, et il a été adopté par *Mastercard*.
- Le concept de base de ce protocole (basé sur XML) est de lier le processus d'autorisation financière avec une authentification en ligne.
- Cette authentification est basée sur un modèle comportant 3 domaines (d'où le nom 3D) qui sont :
  - Le commerçant (*Acquirer Domain*)
  - La banque (*Issuer Domain*)
  - Le système de carte bancaire *(Interoperability Domain)*
- Le protocole utilise des messages XML envoyés via des connexions SSL (qui garantissent l'authentification du serveur et du client par des certificats numériques).

Sécurité des paiements

Norme 3-D Secure



Sécurité des paiements

Norme 3-D Secure

Step	What Is Happening
Step 1	Shopper browses at a merchants website, adds the items to their shopping basket (or equivalent), procedes to the checkout, and enters their card details. The merchant now has all of the necessary data.
Step 2	The Merchant Server Plug-in (MPI) sends the Primary Account Number (PAN) (and user device information, if applicable) to the Directory Server.
Step 3	*The Directory Server queries the appropriate Access Control Server (ACS) to determine whether authentication (or proof of authentication attempt) is available for the Primary Account Number (PAN) and device type. *If no appropriate Access Control Server (ACS) is available, the Directory Server creates a response for the Merchant Server Plug-in (MPI) and processing continues wth Step 5.
Step 4	The Access Control Server (ACS) responds to the Directory Server.
Step 5	*The Directory Server forwards the Access Control Server (ACS) respose (or its own) to MPI. *If neither authentication nor proof of authentication attempt is available, 3-D Secure processing ends, and the merchant, acquirer, or payment processor may submit a traditional authorisation request, if appropriate.
Step 6	The Merchant Server Plug-in (MPI) sends a Payer Authentication Request to the Access Control Server (ACS) via shopper's device. *The Payer Authentication Request message may be "PAReq" (for cardholders using PCs) or "CPRQ" (for cardholders using mobile Internet devices - see 3-D Secure: Protocol Specification - Extension for MobileInternet Devices).
Step 7	The Access control Server (ACS) receives the Payer Authentication Request.
Step 8	*Access Control Server (ACS) authenticates the shopper using processes applicable to the Primary Account Number (PAN) (password, chip, PIN, etc.). Alternatively, the Access control Server (ACS) may produce a proof of authentication attempt. *The Access control Server(ACS) then formats the Payer Authentication Response message with appropriate values and signs it. *The Payer Authentication Response message is "PARes" if "PAReq" was received, or "CPRS" if "CPRQ" was received. (CPRS is created using values from the "PARes".)
Step 9	*Access control Server(ACS) returns the Payer Authentication Response to Merchant Plug-in (MPI) via shopper's device. *Access control Sercer (ACS) sends selected data to the Authentication History Server.
Step 10	Merchant Plug-in (MPI) receives Payer Authentication Response.
Step 11	Merchant Plug-in (MPI) validates the Payer Authentication Response signature (either by performing the validation itself or by passing the message to a separate Validation Server).
Step 12	*The Merchant proceeds with authorization exchange with their acquirer. *Following Step 12, the acquirer processes the authorization with the issuer via an authorization system such as VisaNet, then returns the results to merchant.

Sécurité des paiements

PCI DSS

- Le *Payment Card Industry* (PCI) est le secteur économique des moyens de paiement par carte.
- Le *PCI Security Standards Council* (PCI SSC) est une instance de ce secteur économique qui émet des recommandations de sécurité sur les paiements par carte.
- Le *Payment Card Industry Data Security Standard* (PCI DSS) est un standard de sécurité des données pour les industries de carte de paiement créé par le comité PCI SSC pour les plus importantes entreprises de carte de débit et crédit.
- Il s'agit en réalité d'un guide de 12 règlements établi par un consortium dans lequel on retrouve *Visa* et *Mastercard*, qui aident les entreprises émettrices de cartes de paiement à protéger leurs données et à prévenir les fraudes.
- PCI-DSS traite les trois dimensions de la sécurité de l'information (technologique, organisationnelle et humaine)et se focalise sur la confidentialité des données de cartes.

Le porte monnaie électronique

- *CyberCash* a déposé son bilan en 2001 et a été repris par *VeriSign*.
- *PayPal* a acquis les services de paiement de VeriSign, y compris *CyberCash* et les passerelles de paiement *Payflow Link* et *Payflow Pro*.
- *PayPal*, géré par l'entreprise américaine *Paypal Inc*., est un service de paiement électronique qui permet de payer des achats, de recevoir des paiements, ou d'envoyer et de recevoir de l'argent.
- Pour bénéficier de ces services, une personne doit transmettre diverses coordonnées financières à *PayPal*, tel que numéro de carte de crédit, transmission qui peut se faire par voie postale.
- Par la suite, les transactions sont effectuées sans avoir à communiquer de coordonnées financières, une adresse de courrier électronique et un mot de passe étant suffisant.

Le porte monnaie électronique

- Une autre forme de porte-monnaie électronique permet des paiements chez les commerçants, sur des terminaux spécialisés.
- Le dispositif se présente actuellement sous forme de cartes prépayées (type carte à puce), ou encore de comptes en ligne et peut également être intégré, par l'intermédiaire de techniques standardisées, sur une grande variété d'appareils (clés USB ou téléphones mobiles).
- La carte *Monéo* est un exemple de ce type de carte.
  - *Moneo est géré par le consortium BMS Billetique Monétique Service qui regroupe dix banques françaises (BNP Paribas, Banques populaires, Caisses d'épargne, HSBC, CIC, Crédit agricole, Crédit lyonnais, Crédit mutuel, La Banque postale, Société générale) mais également la SNCF, la RATP et France Télécom.*

Tendances sécurisation des paiement

- SSL et TLS sécurisent le transfert des informations mais ne fournissent pas à proprement parler de solution susceptible de garantir le bon déroulement d'une transaction.
- Tentatives des différents acteurs (Banques, éditeurs) pour imposer leurs propres solutions.
- Les Banques centrales craignent les risques inflationnistes liés à la création de monnaie fictive et tentent d 'élaborer une doctrine commune.
- Le développement du C.E. est lié à la disponibilité d'une solution fiable, universelle et peu coûteuse de paiement électronique à distance.
- Ceci implique des dispositifs de cryptage et le recours à des tiers de confiance.

Plan

- **A. Les principes et les enjeux**
  - **C04 Sécurité et commerce électronique. Sécurité et banque**
    - *Le risque SI parmi les autres risques bancaires*
    - *Intranet bancaire*
    - *Sécurisation de la banque en ligne*
    - *Sécurisation des paiements*
    - ***Tendances générales***

Sécurité des paiements

Tendances

- De nombreux facteurs poussent les institutions financières à repenser leurs pratiques de sécurité réseau traditionnelles et, par la même, leur fidélité envers certains fournisseurs historiques.
- Plus que jamais, elles ont besoin de trouver de nouvelles solutions pour améliorer leur couverture de sécurité, la performance et la visibilité, tout en répondant aux exigences réglementaires et de réduction des coûts.
- Face aux nouvelles menaces associées à la mobilté, à l'adoption des applications Web et cloud, et à la demande toujours plus forte en bande passante, les banques ont juxtaposé au fil du temps de nombreuses solutions de sécurité.
- Cette approche a abouti à un modèle de déploiement devenu complexe et coûteux en termes de gestion et de maintenance.

Sécurité des paiements

Tendances

- Recherche d'une stratégie de sécurité SI/IT intégrée :
  - qui permette de prendre en compte l'ensemble des exigences posées aux infrastructures par les nombreuses régulations et règles de conformité (PCI-DSS, SOX, Basel II/III, GLBA vs CNIL, etc);
  - qui permette de répondre à l'augmentation et à la complexité des menaces;
  - qui évolue de l'objectif traditionnel de simple sécurisation des actifs IT à la protection et au support des fonctions métiers, à l'adaptation à un environnement utilisateur en perpétuelle évolution;
  - qui permette le contrôle centralisé des applications – en reconnaissant le trafic par la source de l'application et par l'utilisateur, et pas seulement par le port – et la surveillance des différents terminaux connectés au réseau.
  - qui freine l'utilisation inappropriée des ressources du réseau, qui, en plus d'engorger la bande passante avec des données non-productives, exposent l'entreprise et ses mandataires sociaux à des risques de litiges et poursuites judiciaires, de fraudes et vols.

Sécurité des paiements

Tendances

- Développer la capacité d'appliquer des politiques de sécurité granulaires, adaptée spécifiquement à des groupes d'utilisateurs ou de postes, ,tout en préservant les performances de l'accès au Web et aux applications critiques.
- Développer les solutions permettant de développer à partir d'un seul code source sur de multiples plate-formes (Windows, Mac OS X, Linux, iPhone, iPad et Android)
- Remplacer les pare-feux traditionnels:
  - Répondre aux exigences de débit élevé résultant de l'utilisation des applications Web et autres nouvelles technologies,
  - Adopter des technologies ayant un impact minimal sur la latence du réseau en permettant une inspection rapide des paquets.
- Mettre en place des solutions centralisée de journalisation, d'analyse et d'édition de rapports, permettant d'offrir une vue unique et en temps réel sur l'état de la sécurité du réseau.