Gérer et sécuriser ses informations stratégiques

Introduction

✓ Objectifs

1. Vous faire réaliser l'importance du patrimoine informationnel de l'entreprise

2. Vous présenter des bonnes pratiques à adopter pour la sécurisation de vos information

Programme

Programme : Gérer et sécuriser ses informations stratégiques

✓ Les enjeux de la sécurité de l'information et du patrimoine immatériel

1. La protection de l'innovation
2. La protection de l'information stratégique

✓ Les principaux risques de fuite

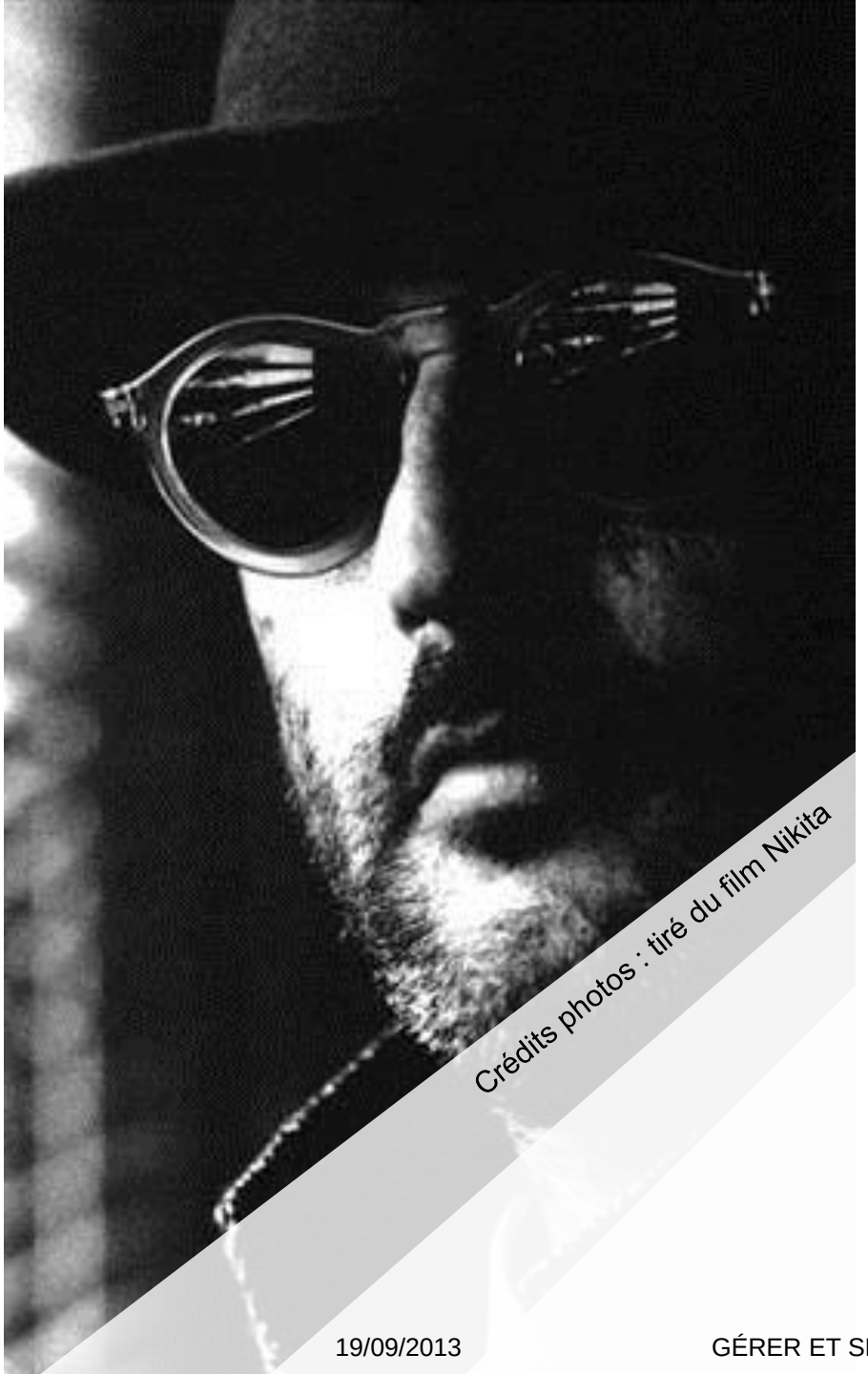
1. Les risques humains
2. Les risques liés au système d'information
3. Les risques liés aux matériels

✓ Limiter les risques

1. Sensibilisation
2. Actions concrètes à mettre en place

actulligence Consulting

Les enjeux de la sécurité de l'information et du patrimoine informationnel



- ✓ La protection de l'innovation

NDLR : Ce qui sous-entend quand même qu'avant de se protéger il faut innover…

Définition de l'innovation

✓ **Il existe plusieurs typologies d'innovation :**

1. Innovation « Recherche de base » , « Recherche appliquée », « Recherche et développement »

2. Innovations de process ou innovation produits

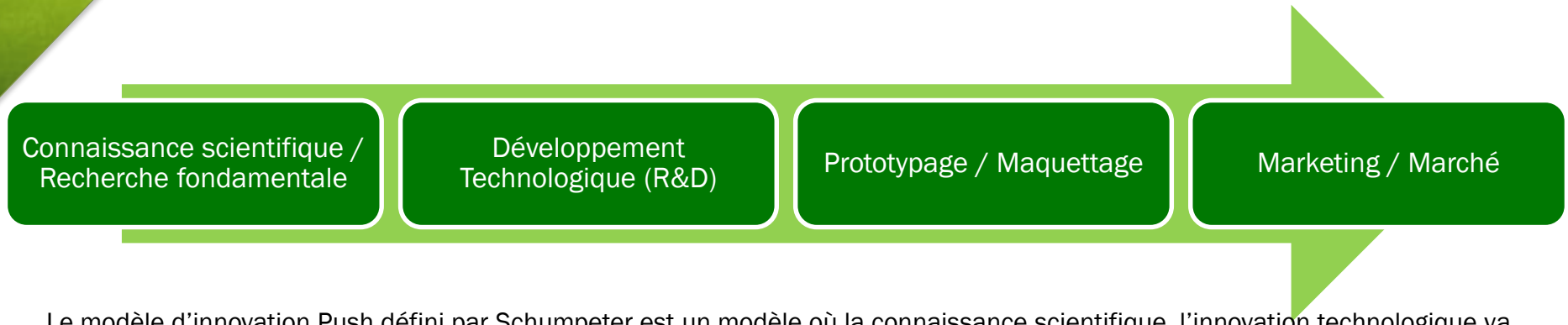
3. Innovation mineure ou innovation majeure

Exemples d'innovation (Schumpeter)

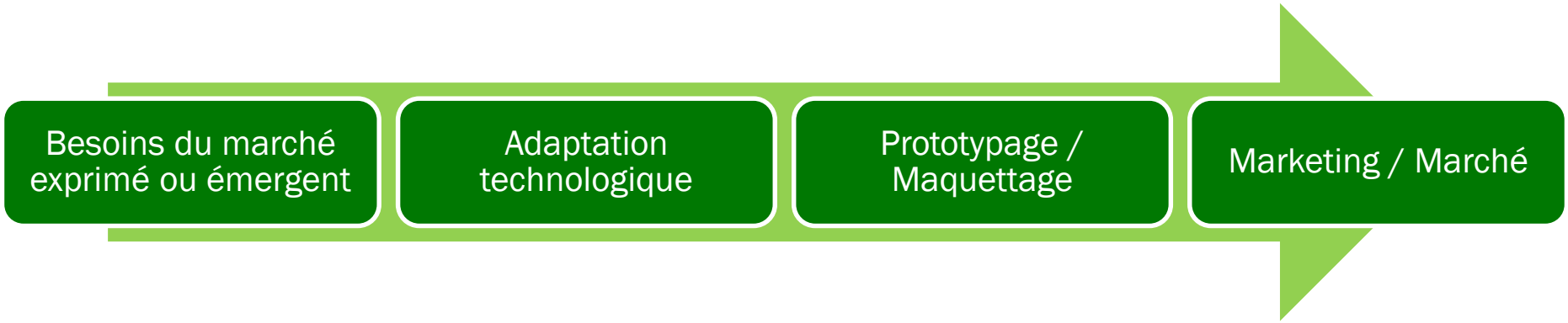
✓ **En 1931 Schumpeter liste un ensemble d'éléments innovants :**

1. Produire un bien nouveau qui n'existe pas sur le marché
2. Innover sur le procédé industriel et produire mieux de meilleure qualité, de façon plus économique
3. Découvrir de nouvelle matières premières ou matériaux
4. Se créer de nouveaux marchés (géographiquement, CSP,…)
5. Modifier l'organisation du marché (création ou destruction d'un monopole)

Modèles d'innovations



Le modèle d'innovation Push défini par Schumpeter est un modèle où la connaissance scientifique, l'innovation technologique va permettre de créer un besoin. C'est un modèle où l'innovation est plus souvent de rupture, c'est-à-dire qu'elle crée un fossé sur le marché entre celui qui innove et ses « concurrents » historiques. L'innovation lui permet d'acquérir un monopole ou quasi-monopole temporairement.



Le modèle d'innovation Pull défini par Schmookler est un modèle dans lequel le marché exprime un besoin. Ce type d'innovation, poussé par les consommateurs, donnera plus souvent lieu à des innovations de type incrémentales.

Niveaux de création de connaissance et d'innovation

- ✓ **La connaissance qui donne lieu à l'innovation n'est pas que technologique et n'est pas que « produit ».**
- ✓ **Il y a plusieurs champs de création des connaissances qui mènent à l'innovation et cette dernière peut être mesurée selon des indicateurs.**

Domaine	Activité	Résultats	Indicateurs
Science	Recherche (fondamentale, spéculative ou finalisée)	Découverte scientifique	Publications et communications scientifiques
Technologie	Recherche appliquée, D de R&D	Invention	Brevets
Economie / Société / Marché	Développement industriel et commercial, organisation et productions	Innovation	Chiffre d'affaires, Marge, activité, emplois

Innovation et coopération

✓ **Pourquoi des pôles de compétitivité ? Pourquoi la coopétition ? Pourquoi des alliances productives ?**

1. L'innovation est presque toujours un phénomène de réseau

2. L'innovation implique souvent une coalition d'acteurs qui trouvent un intérêt mutuel dans la mise en commun de leurs ressources pour innover

Innovation ≠ Invention

✓ **L'innovation est l'expression d'une forme de créativité non forcément liée à la science ou à la technologie.**

- Définition de l'innovation par le Manue d'Oslo (OCED) : « Une innovation est la mise en œuvre (*implementation*) d'un produit (bien ou service) ou d'un procédé (de production) nouveau ou sensiblement amélioré, d'une nouvelle méthode de commercialisation ou d'une nouvelle méthode organisationnelle dans les pratiques d'une entreprise, l'organisation du lieu de travail ou les relations extérieures », déclinées en 4 catégories :
  - de produit ou de prestation (quand il s'agit d'une entreprise du commerce ou des services) : création d'un nouveau produit ou offre d'une nouvelle prestation commerciale ou de service
  - de procédé : mise en œuvre de nouvelles techniques pour la production de biens ou la réalisation de prestations de services
  - d'organisation : les cercles de qualité en sont un exemple
  - de marketing : par exemple la mise en franchise ou la promotion sur Internet.

Innovation ≠ **Invention**

- ✓ **L'invention est plus restrictive que l'innovation dans le sens où une invention doit avoir un caractère « nouveau » (innovant) et doit pouvoir être matérialisée par un « produit »**
- ✓ **L'office européen des brevets dit ainsi qu'une invention pour être brevetée doit :**
  1. Avoir un caractère nouveau
  2. Avoir un caractère technique
     - Mais la règle n'est pas la même pour tous les offices de brevets.
- ✓ **Il n'y a pas de consensus international sur ce qu'est une invention et de fait sur sa brevetabilité.**

L'invention brevetable en France

✓ Elle doit être nouvelle

non comprise dans l'état de la technique, ne doit pas avoir été rendue accessible au public avant la date de dépôt (même par l'inventeur)

✓ Impliquer une activité inventive

ne découle pas de manière évidente pour un homme du métier de l'état de la technique

✓ Susceptible d'application industrielle

peut être fabriquée ou utilisée dans tout genre d'industrie y compris l'agriculture

Source : Les brevets – Jean-Pierre Cardo

Exclusions de brevetabilité en France

✓ Ne sont pas considérées comme des inventions Art.L611-10 CPI:

- **Les découvertes, théories scientifiques et méthodes mathématiques**
- **Les créations esthétiques**
- **Les plans, principes et méthodes dans l'exercice d'activités intellectuelles ou dans le domaine d'activités économiques**
- **Les règles de jeu**
- **Les programmes d'ordinateurs**
- **Les présentations d'informations**

✓ Ne sont pas brevetables Art.L611-17 CPI:

- **Les inventions contraires à l'ordre public et aux bonnes mœurs, notamment au vu de considérations bioéthiques**
- **Les obtentions végétales protégées par un C.O.V (Certificat d'Obtention Végétal)**
- **Les races animales et procédés essentiellement biologiques d'obtention d'animaux**

✓ Ne sont pas brevetables du fait de leur application ***Art L.611-16 CPI:***

- **Les méthodes de traitement chirurgical ou thérapeutique du corps humain et méthodes de diagnostic appliquées au corps humain et animal**

Que peut-on protéger ?

✓ Le produit

- Protégé en soi -même par procédé différent et quelle que soit l'application
- Défini par sa composition, structure ou constitution

✓ Le moyen

- Protégé dans sa forme et dans sa fonction mais si seulement pour l'application

✓ L'application nouvelle

- Couvre la seule utilisation nouvelle du moyen connu

✓ La combinaison nouvelle

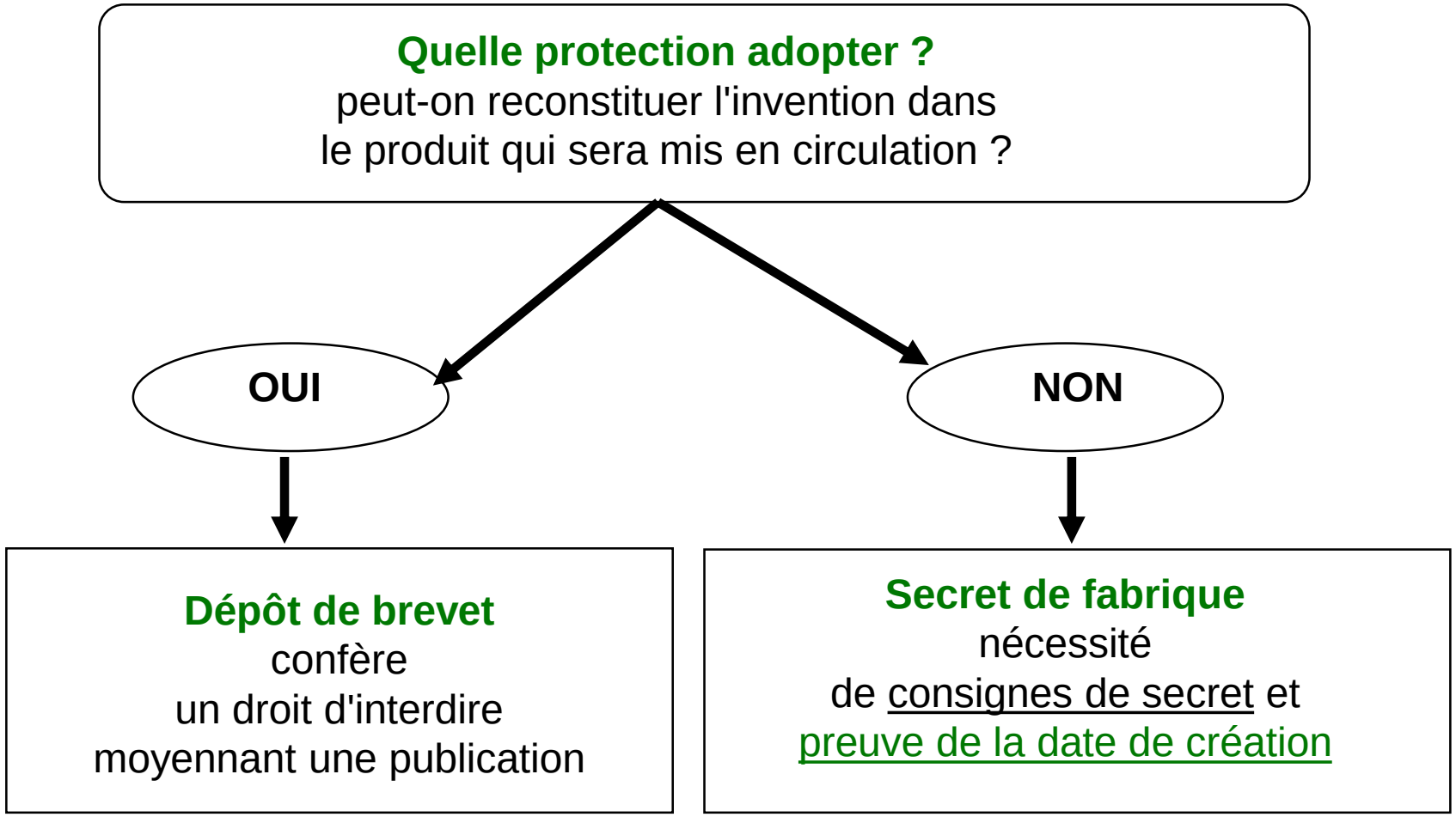
- Protégée contre tout agencement identique avec mêmes moyens pour 1 même résultat

Source : Les brevets – Jean-Pierre Cardo

ATTENTION !!!

« Une invention divulguée sans protection appartient de fait au domaine public : son exploitation est libre de droits. »

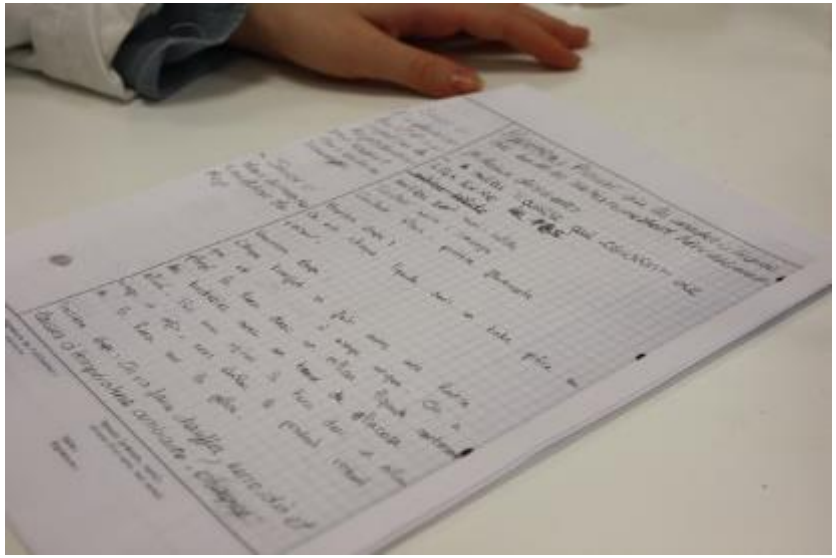
Se passer de brevets ?



Protéger l'antériorité : cahiers de laboratoires

✓ Le cahier de laboratoires :

- « Le cahier de laboratoire national est un outil de traçabilité des travaux de recherche pour les laboratoires et les PME innovantes. Elaboré par le ministère de l'Enseignement supérieur et de la Recherche et le Réseau Curie, en collaboration avec l'INPI et en concertation avec les organismes de recherche publics, il est destiné à laisser une trace écrite des travaux de recherche, pouvant également servir de preuve matérielle sur l'antériorité d'une invention. »
- Source : inpi.fr



Source : http://www.lyc-marseilleveyre.ac-aix-marseille.fr/spip/spip.php?article248&id_document=228

Protéger l'antériorité : l'enveloppe Soleau

✓ **« L'enveloppe Soleau est un produit de l'INPI qui, sans être un titre de propriété industrielle, vous permet de dater de façon certaine la création de votre œuvre et vous identifier comme auteur. »**

- Source : inpi.fr

✓ **L'enveloppe Soleau permet pour une somme « modique » de déposer des documents papiers actant d'une innovation**

✓ **Les documents déposés n'ont pas de contrainte de formalisme.**

✓ **« Elle ne permet pas à son propriétaire d'interdire à d'autres personnes l'exploitation de l'invention concernée ou le dépôt d'un brevet portant sur cette invention. »**

Le bon équilibre

- ✓ **Vous devrez toujours dévoiler de l'information stratégique à des collaborateurs ou partenaires pour avancer**
- ✓ **Il vous faudra toutefois veiller à :**
  1. Sécuriser ces partages
  2. Ne dévoiler que le nécessaire

« En protection de l'information stratégique il ne faut être ni paranoïaque ni naïf… »

- ✓ La protection de l'information stratégique

NDLR : Ce qui sous-entend quand même qu'avant de protéger de l'information stratégique il faut avoir une stratégie

Définition : Information stratégique

✓ Information stratégique :

- « Information contenant des éléments susceptibles de contribuer à la définition, l'infléchissement ou la remise en cause de la stratégie de l'organisation. On parle d'information critique lorsque celle-ci a un impact fort sur la stratégie. »
  - Définition ADBS

✓ Se traduit par :

1. « faire gagner du temps » sur l 'échiquier de la compétition «(offre, position géographique)
2. Réduire son incertitude sur son environnement (connaissance de projets, d'interactions entre des acteurs)
3. Un caractère exceptionnel qui va bouleverser des postulats, des rapports
4. Doit se traduire en événements probables
5. L'évaluation d'un potentiel

Source : FB Huygue

Les spécificités de l'information stratégique

- ✓ **L'information stratégique est multiforme : projets, budgets, recrutements, investissements.**

- ✓ **L'information stratégique est diffuse : dans votre système informatique, dans la tête de vos collaborateurs, dans votre tête, sur Internet**

- ✓ **L'information stratégique est mobile : téléphones portables, ordinateurs, tablettes**

- ✓ **Sa protection est complexe :**
  1. Elle doit être partagée avec certains collaborateurs ou partenaires
  2. Elle doit être sécurisée de ses adversaires

Quelques informations à protéger

✓ **Les projets :**

1. De fusion / acquistion
2. D'évolution de son réseau de distribution
3. De construction d'infrastructures (usines)

✓ **Les programmes de recherche et développement prévisionnels ou en cours**

✓ **Les sous-traitants ou fournisseurs ayant une compétence unique ou rare**

✓ **Les modes de production ou recettes de production lorsqu'elles n'ont pas été rendues publiques**

✓ **Les données financières lorsque cela n'est pas nécessaire**

Le cadre juridique autour de l'information : Se prémunir

✓ Le droit du travail :

1. La clause de confidentialité s'impose à tous, « même en l'absence de stipulation expresse et même après la rupture du contrat de travail »
2. Elle peut expressément être rappelée et se trouve parfois nommée : obligation de confidentialité ou obligation de discrétion

✓ Le droit de la propriété intellectuelle :

1. Qui régit les inventions faites par le salarié dans le cadre de son contrat de travail (article L 611-7)
2. Qui régit la protection des bases de données, de leur structure et de leur contenu (article L.341-1 du CPI)

✓ Les relations contractuelles avec ses sous–traitants et partenaires :

- Clause de confidentialité qui se doit d'être explicite dans le cas des partenaires et sous-traitants et qui pourra fixer les sanctions financières en cas de non respect

Le cadre juridique autour de l'information : Se défendre

✓ **En cas de fuite l'on pourra invoquer plusieurs cas de figures et orienter sa défense selon plusieurs axes :**

1. La corruption (art 445-1 du code pénal)
2. Révélation des secrets de fabrique (art. L 1227-1 du code du travail
3. Abus de confiance (Cass. Crim. 22/09/2004 | Fimag Groupe Ertop contre Roger X.)
4. Vol d'information accompli au moyen du vol de son support (Cass Crim 04/03/20013)
5. Vol de données immatérielles (TGI de Clermont-Ferrand 26/09/2011)
6. Violation du secret professionnel qui n'est pas forcément limitatif à certaines professions (art. 226-13 du code pénal)
7. Accès et maintien frauduleux dans un système de traitement automatisé de données (art. 323-1 et s. Code pénal)
8. Le parasitisme économique, article 1382 du Code civil jurisprudence vente-privee.com entre autre, 22/6/2012 – Tribunal de commerce de Paris

Les principaux risques de fuite de l’information et du patrimoine immatériel

Les risques de fuites sont…

Humains

Manque de discrétion, manque de réflexes sécuritaires, non respect de règles de sécurité élémentaires …

Informatiques

Mauvaise sécurisation du système informatique, mauvaises prestations informatiques, …

Matériels

Oubli ou pertes de téléphones portables, clés USB, ordinateurs portables

Quelques anecdotes…

- ✓ **En 2009, un prestataire informatique travaillant pour le gouvernement britannique, Daniel Harrington, égare une clé USB contenant des mots de passe permettant d'accéder UK Government Gateway system et en février 2012, un salarié d'EDF, britannique, égare une clé USB non chiffrée contenant des détails techniques sur la centrale nucléaire d'Hartlepool**

- ✓ **De nombreuses « agences privées de renseignement » travaillant pour les entreprises réalisent une part conséquente de leur chiffre d'affaires en faisant les poubelles :**

  1. En 2008, une plongée dans les poubelles des ménages d'Ile-de-France montrait que 80 % recelaient au moins un document personnel (feuilles de paye, de sécu, relevé bancaire) – Etude du Credoc
  2. Dans la même étude, il est apparu que les deux tiers des poubelles de PME analysées contenaient au moins un papier confidentiel. En moyenne, chaque bac recélait 8,5 documents intéressants

- ✓ **En 2009, 4 000 ordinateurs portables ont été volés dans les principaux aéroports européens dont 700 à Roissy (source Baromètre KPMG du vol et de la perte d'informations.)**

CRÉDITS PHOTOS : L'ASSOCIÉ DU DIABLE

- ✓ Les risques humains

Diversité des intentions

✓ **Les risques humains sont nombreux :**

1. Intentionnels :
   - Revente d'information confidentielles
   - Fuite d'information organisée visant à nuire à l'employeur
   - Désobéissance aux protocoles et règles de protection de l'entreprise menant
   - …

2. Inadvertance :
   - Utilisation de mots de passes trop simples
   - Utilisation de moyens tiers non sécurisés pour faire transiter de l'information
   - En dire trop
   - …

✓ **Les risques intentionnels peuvent pour la plupart trouver une réponse juridique, il n'en est pas de même des inadvertances qui sont tolérées (droit à l'erreur)**

✓ **Problème : prouver l'intention**

Les risques humains et le social engineering

✓ **Social engineering :**

1. Celui qui veut de l'information va utiliser des interactions humaines pour les obtenir ou pour compromettre ces informations (clé d'accès)
2. Celui qui essaie d'obtenir cette information se présentera sous son meilleur jour et pourra même donner des références :
   - Nouvel employé
   - Réparateur
   - Service informatique
3. Son objectif sera de recouper et réunir assez d'informations pour pénétrer le système d'information de l'entreprise
4. Ce danger est renforcé par l'utilisation des réseaux sociaux sur laquelle l'on peut plus aisément qu'auparavant trouver des informations personnelles.

✓ **La technologie seule ne peut pas résoudre les problèmes de Social Engineering**

Le cas Robin Sage / Thomas Ryan

Robin Sage

From Wikipedia, the free encyclopedia

For the training exercise, see United States Army Special Forces selection and training.

Robin Sage is a fictional American cyber threat analyst. She was created in December 2009 by Thomas Ryan, a security specialist and White hat hacker from New York. Her name was taken from a training exercise of United States Army Special Forces.[1]

Contents [hide]

1 Fictional biography
2 Security problems revealed
3 "Getting in bed with Robin Sage"
4 References

"Robin Sage" as she appeared on social networking pages.

Fictional biography [edit]

According to Sage's social networking profiles, she is a 25-year-old "cyber threat analyst" at the Naval Network Warfare Command in Norfolk, Virginia. She graduated from MIT and had allegedly 10 years of work experience, despite her young age.[2] Ryan created several accounts under the name Sage on popular social networks like Facebook, LinkedIn, Twitter etc. and used those profiles to contact nearly 300 people, most of them security specialists, military personnel, staff at intelligence agencies and defense contractors.[1] Her pictures were taken from a pornography-related website in order to attract more attention.[2]

Despite the completely fake profile and no other real-life information, Sage was offered consulting work with notable companies Google and Lockheed Martin[2] and received dinner invitations by several of her male friends.[1]

Not everyone was fooled by Sage's profiles, though. Ryan admitted that his cover was already blown on the second day, when several of those she tried to befriend tried to verify her identity using the phone number he provided, checking email addresses outside the social networking sites or using the MIT alumni network to find her. Others recognized the fake identity of Sage based on her implausible profiles. Yet no central warning was issued about the profile, and users continued to connect with Sage despite warnings not to do so.[1]

Security problems revealed [edit]

Using those contacts, Ryan befriended men and women of all ages during a short time period between December 2009 and January 2010. Almost all of them were working for the United States military, government or companies (amongst the only organizations that did not befriend Sage were the CIA and the FBI[1]). Using these contacts, Ryan gained access to email addresses and bank accounts as well as learning the location of secret military units based on soldiers' Facebook photos and connections between different people and organizations.[2] She was also given private documents for review and was offered to speak at several conferences.[3]

"Getting in bed with Robin Sage" [edit]

Ryan presented his findings[4] as a speaker at the "Black Hat" conference in Las Vegas with a presentation he called "Getting in bed with Robin Sage".[2][3] He explained that his short experiment proves that seemingly harmless details shared via social networking pages can be harmful but also that many people entrusted with vital and sensitive information would share this information readily with third-parties, provided they managed to capture their interest. He concluded that his findings could have compromised national security if a terrorist organization had employed similar tactics.[5]

En 2009, Thomas Ryan, un expert en sécurité informatique créa plusieurs faux profils Facebook, Twitter, LinkedIn de Robin Sage, une jeune femme de 25 ans, soi disant analyste sur les cyber-menaces avec des photos « correctes » mais attirantes tirées d'un site pornographique. Elle ajouta alors 300 contacts principalement militaires, spécialistes de la sécurité, … En l'espace de quelques semaines on lui proposa des missions de consultant chez Google on bien encore Lockheed Martin et elle reçut de multiples invitations à dîner de contacts masculins.

Source : Wikipedia et divers articles de presse

Les leviers du renseignement humain

✓ **Money, Ideology, Coercicion, Ego**

1. Si une personne n'est pas assez payée dans son entreprise il sera facile de la corrompre
2. Un autre des leviers et de menacer de dévoiler les convictions idéologiques
3. Menace physique ou chantage
4. Jouer sur l'ego des personnes, leur manque de reconnaissance, les valoriser

✓ **Bien évidemment, utiliser ces leviers est illégal toutefois certains sont plus risqués que d'autre :**

- Il est ainsi assez facile de flatter l'égo de quelqu'un et d'arriver à se livrer plus ouvertement sur les projets qu'il dirige professionnellement

✓ **La politique salariale est globalement une arme d'acquisition des savoirs et savoir faire extérieurs. C'est aussi un mécanisme de défense permettant de limiter le turn over…**

- ✓ Les risques du système informatique

Le risque informatique

✓ **Il doit être appréhendé selon les points de vue suivants :**

1. Risque de perte d'information de valeur / d'information d'exploitation
2. Risque de dysfonctionnement du système productif entraînant un ralentissement de l'activité
3. Fuite d'information confidentielle

✓ **Aucun de ces aspects ne doit être négligé !**

Risque de perte / destruction d'information

✓ Cela constitue un risque majeur et crédible car :

1. Une partie importante de l'activité commerciale, financière, comptable voire même de la production des biens ou des services repose sur de l'information
2. Les supports de stockage sont faillibles (panne, durée de vie limitée, …)
3. Les utilisateurs sont faillibles

✓ L'entreprise doit :

1. Sauvegarder ses données de façon sûre en conformité avec la réglementation (traçabilité, obligations comptables) et ses clauses d'assurance (souvent sauvegarde existante à l'extérieure de l'entreprise)
2. S'assurer que ses sauvegardes fonctionnent (tester la remontée de sauvegardes régulièrement)
3. Disposer d'un plan de reprise d'activité (organiser le redémarrage de toute ou partie des activités en cas de panne / perte de données)
4. Former ses utilisateurs à la bonne utilisation des outils informatiques

Risque de dysfonctionnement / ralentissement

✓ **En dehors de la perte d'information, le système de transfert de l'information peut dysfonctionner et entraîner un ralentissement de l'activité**

1. Panne de CRM
2. Dysfonctionnement d'un EDI (Echange de Données Informatisée) entre ses lieux de production et / ou sous-traitants
3. Dysfonctionnement comptabilité

✓ **Il est important d'anticiper les panne sur les endroits les plus critiques du SI et de planifier les solutions en cas de :**

1. Cessation des transactions d'interaction entre les applicatifs
2. Perte temporaire des données

✓ **A prévoir :**

1. Solutions et organisation temporaire
2. Plan de reprise
3. Modes de résolution des principaux dysfonctionnements prévisibles

Fuite d'information confidentielles

✓ **Les fuites d'information liées au SI sont nombreuses et plusieurs points essentiels sont à prendre en considérations :**

1. Résistance du système aux attaques extérieures
   - Virus
   - Spywares
   - Tentatives d'accès au réseau interne
2. Verrouillage des sorties documentaires
3. Gestion des accès aux documents confidentiels / Gestion des droits
4. Sécurisation des périphériques mobiles :
   - Clés USB
   - Téléphones portables
   - Ordinateurs portables
   - Disques durs amovibles

Crédits photo by Ross Larocco

- ✓ Les risques liés au matériel

Constat

- ✓ **Le salarié est de plus en plus mobile.**
- ✓ **L'information est de plus en plus disponible sur des terminaux ou périphériques mobiles destinés à voyager à l'extérieur de l'entreprise.**
- ✓ **Le risque de fuites d'information lié aux terminaux mobiles et aujourd'hui un point critique d'autant plus que parfois les terminaux n'appartiennent pas à l'entreprise (BYOD : Bring Your Own Device).**
- ✓ **Le développement du télétravail augmente ce risque.**

Les risques de fuites d'informations liés aux terminaux mobiles

✓ **Exposition de l'information consultée dans les lieux publics :**

1. Train
2. Avion
3. Lieux de travail extérieurs

✓ **Vol des terminaux mobiles à l' extérieur de l'entreprise**

✓ **Piratage des réseaux publics Wifi ou 3G et des échanges de documents**

✓ **…**

- ✓ Sensibilisation

Une action indispensable

✓ **Un des points essentiels dans la prévention contre les fuites d'information est de sensibiliser les personnels sur plusieurs points :**

1. Rappel des obligations de discrétion / confidentialité

2. Mise en place et communication de règle d'utilisation des ressources informatiques :
   - Matériel
   - Logiciel

3. Mise en place d'une charte d'utilisation des réseaux sociaux

4. Sensibilisation générales aux risques du social engineering

5. Sensibilisation aux risques d'utilisation de terminaux mobiles / supports amovibles et à leur bonne utilisation

Rappel des obligations des discrétion

✓ **Bien que le droit du travail soit explicite et opposable il pourra être nécessaire de :**

1. Rappeler explicitement dans le contrat de travail l'obligation de confidentialité vis-à-vis de son employeur

2. Formaliser contractuellement les terminaux mobiles remis à l'utilisateur et les obligations inhérentes à leur utilisation

Mise en place et communication de règles d'utilisation des ressources informatiques

✓ **De plus en plus les entreprises se dotent de chartes de bonnes utilisation des ressources informatiques qui peuvent comprendre :**

1. L'interdiction d'aller sur certains types de sites
2. L'obligation de n'utiliser que son email professionnel sur son lieu de travail
3. L'interdiction de faire transiter ou héberger, y compris temporairement, des documents professionnels sur des ressources externes :
   - DropBox
   - Google Docs
   - …
4. L'interdiction d'installer des logiciels tiers sur ces outils de travail
5. L'obligation d'utiliser le matériel fourni par l'entreprise pour travailler

✓ **Plus généralement la charte pourra rappeler les règles pratiques et de bon sens liés à l'utilisation des outils informatique dans un cadre professionnels**

✓ **Il est possible de prévoir des sanctions en cas de non respect des ces règles**

✓ **La charte peut être intégrée au règlement intérieur**

Exemple de charte informatique

2. Accès aux ressources informatiques et services Internet

L'utilisation des ressources informatiques et l'usage des services Internet ainsi que du réseau pour y accéder sont destinés à l'activité professionnelle des utilisateurs conformément à la législation en vigueur. L'activité professionnelle doit être entendue comme celle définie par les textes spécifiant les missions du CNRS.

L'utilisation des ressources informatiques partagées de l'entité et la connexion d'un équipement privé et extérieur (tels qu'un ordinateur, commutateur, modem, borne d'accès sans fil…) sur le réseau sont soumises à autorisation du responsable de l'entité et aux règles de sécurité de l'entité. Ces autorisations sont strictement personnelles et ne peuvent en aucun cas être cédées, même temporairement, à un tiers. Elles peuvent être retirées à tout moment. Toute autorisation prend fin lors de la cessation de l'activité professionnelle qui l'a justifiée.

L'entité peut en outre prévoir des restrictions d'accès spécifiques à son organisation (certificats électroniques, cartes à puce d'accès ou d'authentification, filtrage d'accès sécurisé,…).

3. Règles d'utilisation et de sécurité

Tout utilisateur est responsable de l'usage des ressources informatiques auxquelles il a accès.

L'utilisation de ces ressources doit être rationnelle et loyale afin d'en éviter la saturation ou leur détournement à des fins personnelles. En particulier :

BNP PARIBAS

Cette utilisation ne doit pas porter atteinte à l'exécution normale de son contrat de travail ou de sa mission, ni aux intérêts de l'entreprise, de sa clientèle ou de ses salariés.

Il s'engage à respecter les présentes règles.

3.2.2. Règles d'utilisation

3.2.2.1 - Matériels - programmes - logiciels - données…

L'utilisateur s'interdit de modifier les moyens informatiques mis à sa disposition, notamment par ajout de matériels ou de logiciels qui ne lui auraient pas été fournis ou autorisés par les services techniques compétents de l'Entreprise ; il s'engage à n'utiliser que les seuls programmes autorisés par ces services.

L'utilisateur s'engage à ne pas faire de copies des logiciels mis à sa disposition en dehors de sauvegardes pour nécessités de service.

En toute circonstance, quel que soit l'endroit où il se trouve, l'utilisateur doit veiller à la bonne conservation des moyens informatiques mis à leur disposition ainsi qu'à celle des données qu'ils contiennent et de leurs moyens d'accès.

3.2.2.2 - Mesures de sécurité

L'utilisateur ne doit pas chercher à contourner les procédures et les mécanismes de sécurité mis en œuvre par l'Entreprise (antivirus, chiffrement, sauvegarde, signature, mot de passe…).

En particulier il se doit :

- d'utiliser des moyens d'authentification qui ne doivent pas être communiqués,
- de ne jamais prêter à des tiers son identifiant ou mot de passe,
- de ne pas utiliser ou tenter d'utiliser les moyens d'accès d'autres utilisateurs,
- de ne pas quitter son poste de travail en laissant accessible une session en cours.

L'utilisateur contribue à son niveau à la sécurité générale des outils informatiques de la Banque, il se doit à ce titre de signaler tout dysfonctionnement ou tout événement lui apparaissant anormal. Il met en application les règles et recommandations établies par les administrateurs des systèmes informatiques et les services techniques compétents de l'entreprise.

Charte d'utilisation des réseaux sociaux

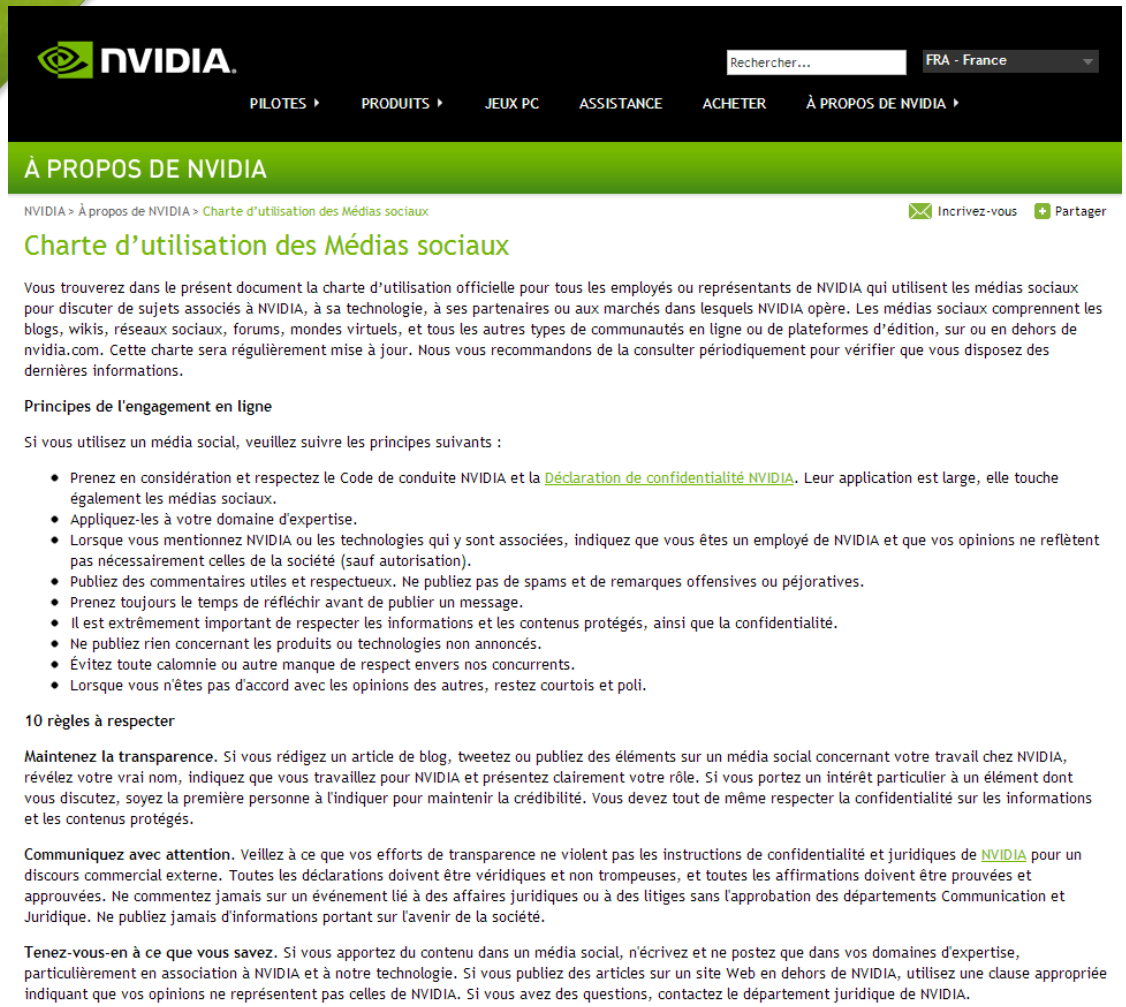
- ✓ **Sujet complexe car chaque salarié est libre de s'exprimer librement en respectant l'obligation de confidentialité.**
- ✓ **L'obligation de confidentialité n'interdit pas à un salarié de dévoiler son employeur et sa fonction.**
- ✓ **Il est facile de recouper des profils personnels et professionnels de salariés.**
- ✓ **Les informations collectées et les profils sociaux peuvent permettre d'amorcer des démarches de social engineering aisément.**
- ✓ **Voire de pirater des comptes mails.**

- ✓ **Par ailleurs il peut être intéressant que certains salariés soient toutefois actifs sur les réseaux sociaux.**

- ✓ **La charte d'utilisation des réseaux sociaux devra donc :**

1. Rappeler le devoir de confidentialité
2. Sensibiliser aux risques de dévoiler des informations personnelles sur les réseaux sociaux
3. Mettre en garde sur les associations pouvant être faites entre informations publiées à titre personnel et celles publiées à titre professionnel
4. Encadrer les publications faites sur les médias sociaux par les salariés et mentionnant la marque.

Exemples de social media policy



NVIDIA

Rechercher...

FRA - France

PILOTES ▸ PRODUITS ▸ JEUX PC ASSISTANCE ACHETER À PROPOS DE NVIDIA ▸

À PROPOS DE NVIDIA

NVIDIA > À propos de NVIDIA > Charte d'utilisation des Médias sociaux

Inscrivez-vous Partager

Charte d'utilisation des Médias sociaux

Vous trouverez dans le présent document la charte d'utilisation officielle pour tous les employés ou représentants de NVIDIA qui utilisent les médias sociaux pour discuter de sujets associés à NVIDIA, à sa technologie, à ses partenaires ou aux marchés dans lesquels NVIDIA opère. Les médias sociaux comprennent les blogs, wikis, réseaux sociaux, forums, mondes virtuels, et tous les autres types de communautés en ligne ou de plateformes d'édition, sur ou en dehors de nvidia.com. Cette charte sera régulièrement mise à jour. Nous vous recommandons de la consulter périodiquement pour vérifier que vous disposez des dernières informations.

Principes de l'engagement en ligne

Si vous utilisez un média social, veuillez suivre les principes suivants :

- Prenez en considération et respectez le Code de conduite NVIDIA et la Déclaration de confidentialité NVIDIA. Leur application est large, elle touche également les médias sociaux.
- Appliquez-les à votre domaine d'expertise.
- Lorsque vous mentionnez NVIDIA ou les technologies qui y sont associées, indiquez que vous êtes un employé de NVIDIA et que vos opinions ne reflètent pas nécessairement celles de la société (sauf autorisation).
- Publiez des commentaires utiles et respectueux. Ne publiez pas de spams et de remarques offensives ou péjoratives.
- Prenez toujours le temps de réfléchir avant de publier un message.
- Il est extrêmement important de respecter les informations et les contenus protégés, ainsi que la confidentialité.
- Ne publiez rien concernant les produits ou technologies non annoncés.
- Évitez toute calomnie ou autre manque de respect envers nos concurrents.
- Lorsque vous n'êtes pas d'accord avec les opinions des autres, restez courtois et poli.

10 règles à respecter

Maintenez la transparence. Si vous rédigez un article de blog, tweetez ou publiez des éléments sur un média social concernant votre travail chez NVIDIA, révélez votre vrai nom, indiquez que vous travaillez pour NVIDIA et présentez clairement votre rôle. Si vous portez un intérêt particulier à un élément dont vous discutez, soyez la première personne à l'indiquer pour maintenir la crédibilité. Vous devez tout de même respecter la confidentialité sur les informations et les contenus protégés.

Communiquez avec attention. Veillez à ce que vos efforts de transparence ne violent pas les instructions de confidentialité et juridiques de NVIDIA pour un discours commercial externe. Toutes les déclarations doivent être véridiques et non trompeuses, et toutes les affirmations doivent être prouvées et approuvées. Ne commentez jamais sur un événement lié à des affaires juridiques ou à des litiges sans l'approbation des départements Communication et Juridique. Ne publiez jamais d'informations portant sur l'avenir de la société.

Tenez-vous-en à ce que vous savez. Si vous apportez du contenu dans un média social, n'écrivez et ne postez que dans vos domaines d'expertise, particulièrement en association à NVIDIA et à notre technologie. Si vous publiez des articles sur un site Web en dehors de NVIDIA, utilisez une clause appropriée indiquant que vos opinions ne représentent pas celles de NVIDIA. Si vous avez des questions, contactez le département juridique de NVIDIA.

Une liste très complète de social media policies ou social media guidelines peut être trouvé à l'adresse : http://socialmediagovernance.com/policies.php

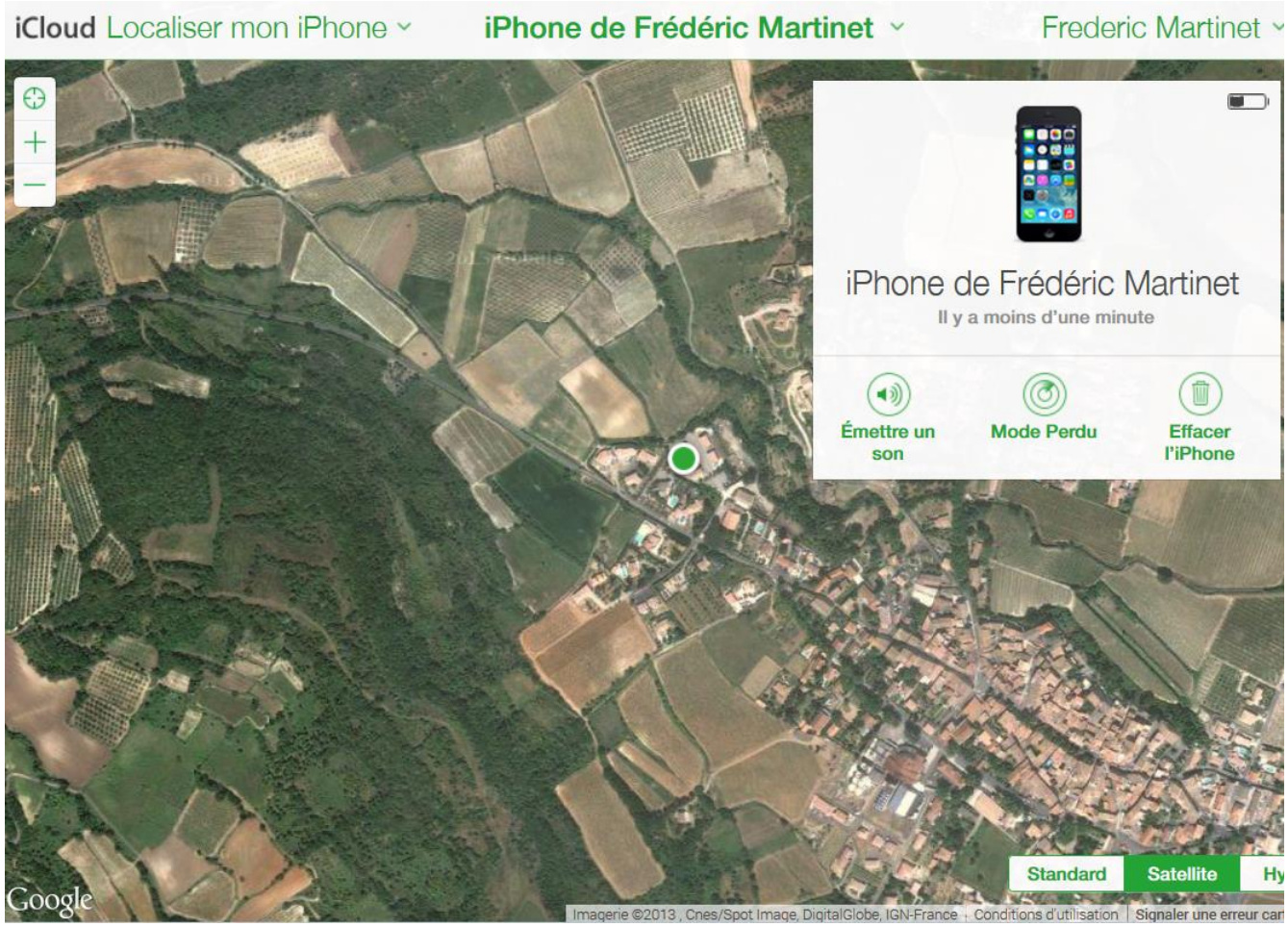
Ci-contre la charte d'utilisation des médias sociaux proposée par Nvidia.

Sensibilisation des risques liés aux terminaux mobiles

✓ **Il est important de sensibiliser tous les salariés aux risques liés aux terminaux mobiles et l'on pourra fixer certaines règles :**

1. N'utiliser des clés USB et disques mobiles uniquement lorsque cela s'avère nécessaire
2. Crypter si possible ces supports mobiles et les fichiers stockés
3. Sécuriser son téléphone portable et ses différents terminaux comportant des données pros par un mot de passe solide
4. Activer les fonctionnalités d'effacement à distance des supports et terminaux mobiles lorsque cela est possible
5. Activer les options de tracking des supports mobiles
6. Pousser à l'utilisation de filtres d'écran

Smartphone égaré, réagissez vite

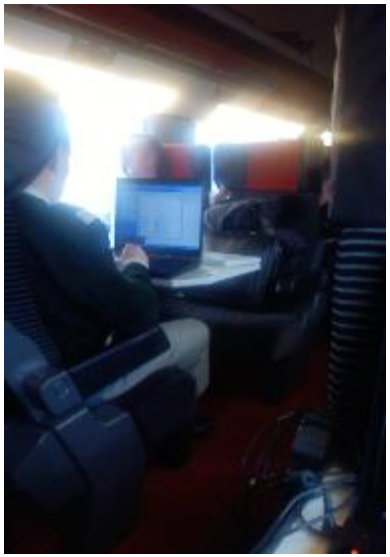


Le site Web iCloud.com permet à tout moment de détecter l'iPhone, l'iPad ou bien l'ordinateur Mac auquel votre compte est associé à partir du moment où celui-ci est allumé et connecté à Internet.

Il permet également de le verrouiller et si besoin était d'effacer toute donnée présente sur ce dernier.

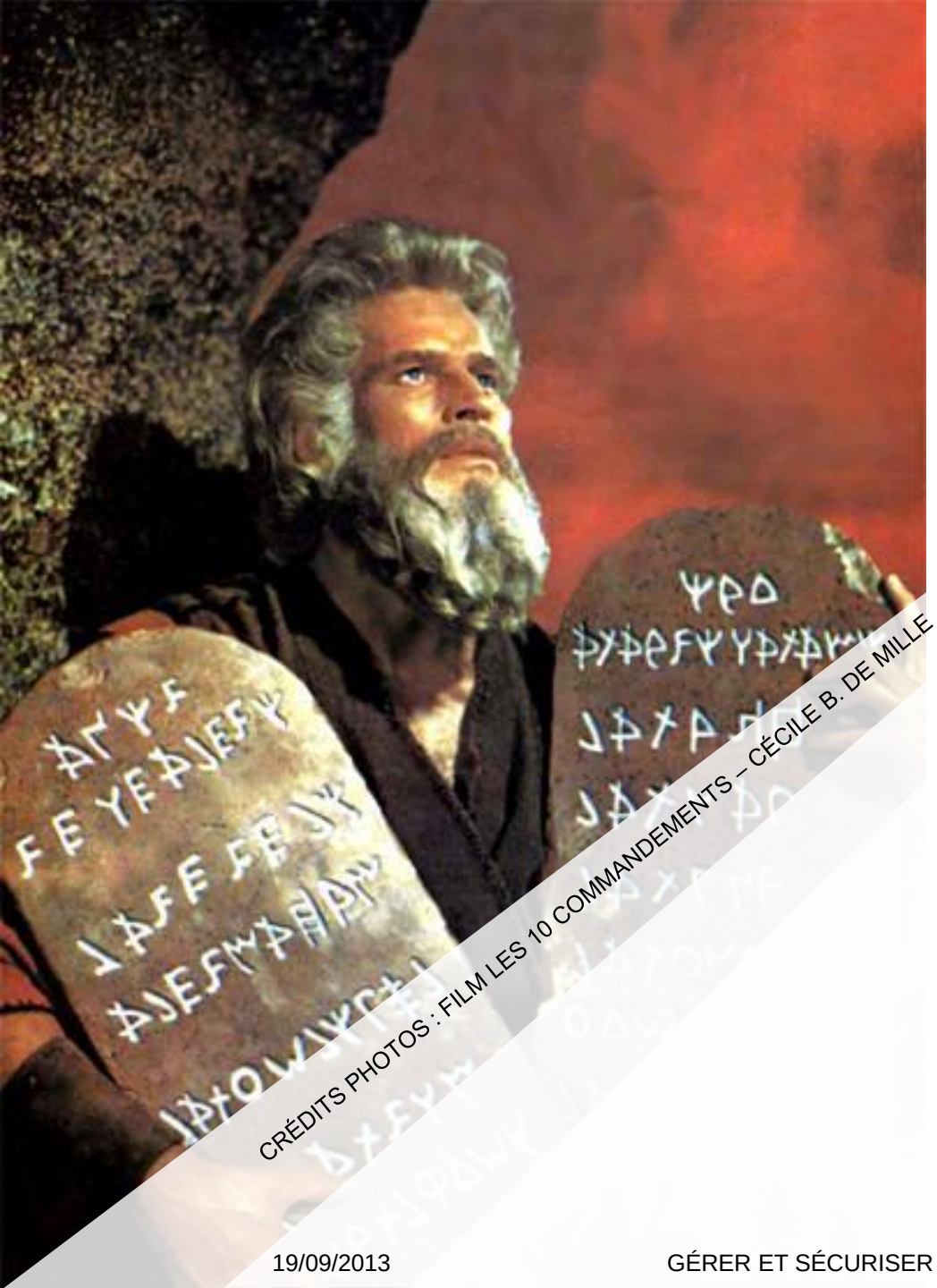
De telles solutions existent aujourd'hui quasiment pour les smartphones de toutes les marques.

Quelques exemples de fuites de tous les jours



Colonel offrant une vue sur son écran et diffusant une présentation d'une intervention du Commandement des opérations spéciales sur les drones
http://fjb.blogs.com/weblog/2009/03/train-%C3%A0-grande-visibilit%C3%A9-.html
François Jeanne-Beylot – Troover

Audit de la réputation digitale de la société Maggi trouvé dans une poubelle du métro parisien
http://twitpic.com/304svq / Séverine Godet / www.twitter.com/tamala75



CRÉDITS PHOTOS : FILM LES 10 COMMANDEMENTS – CÉCILE B. DE MILLE

- ✓ Actions concrètes à mettre en place

L’audit de sécurité

- ✓ **L’audit de sécurité de l’information est essentiel car il permet de manager le risque**
- ✓ **Il devra :**
  1. Identifier les actifs (matériel, physique, logiciel, humain, documents, immatériel)
  2. Identifier le responsable pour chacun de ces actifs
  3. Identifier les vulnérabilités pour chacun des actifs
  4. Identifier les menaces pour chacun des actifs
  5. Identifier les impacts pour chacun des actifs en cas de compromission selon 3 notes :
     - Confidentialité
     - Intégrité
     - Disponibilité
  6. Evaluer la vraisemblance
  7. Estimer le niveau de risque [note finale]
- ✓ **Ce premier audit permettra de déterminer les actions à mener entre : accepter le risque, éviter le risque, transférer le risque, réduite le risque**
- ✓ **Certaines normes (27001 et 27002) détaillent précisément les démarches de sécurité de l’information**

La sécurisation des locaux

✓ **Une des actions afin de limiter le risque de perte des informations vise à minimiser ou couvrir le risque lié aux intrusions physiques dans l'entreprise :**

1. Risque contre les intrusions :
   - Périmètre fermé et sécurisé autour des locaux
   - Alarmes
   - Surveillance / gardiennage
   - Caméras vidéos
   - etc

2. Encadrement des visites :
   - Traçabilité des visites
   - Badges
   - Zones interdites au public
   - Consignes remises aux visiteurs
   - Confiscation des téléphones portables,
   - etc

La sécurité informatique

✓ **Elle est importante mais ne doit pas focaliser toute l'attention de la sécurité de l'information.**

✓ **L'entreprise devrait mettre en place par ordre décroissant de priorité :**

1. Sauvegarde systématique des documents de travail
2. Sécurisation des réseaux informatiques :
   - Vis-à-vis des connexions Web
   - Vis-à-vis des connexions sans fil
3. Traçabilité des matériels informatiques
4. Gestion des droits d'accès à l'information
   - Bases de données
   - Applications métiers
   - Serveurs

✓ **Selon la nécessité elle pourra mettre en place :**

1. Verrouillage des ordinateurs contre l'installation de logiciels tiers
2. Verrouillage des ports USB
3. Contrôle des accès Internet
4. Surveiller le trafic Web (en informant les salariés)

Actions de sensibilisation

✓ **La sensibilisation requiert un aspect essentiel car le principal vecteur de l'information dans une entreprise est l'humain.**

✓ **Il est possible de :**

1. Détailler les obligations du salarié dans les différents documents :
   - Contrat de travail
   - Lettre de mission
   - Charte informatique
   - Règlement intérieur
   - Social Media Policy
2. Rappeler certains risques liés à l'utilisation d'Internet, de l'informatique et des terminaux mobiles
3. Intégrer une étape « sensibilisation informatique » dans le parcours d'intégration
4. Réaliser régulièrement de piqûres de rappel sur ces sujet

Le matériel de sécurité

✓ **L'entreprise peut par ailleurs opter pour certains mécanismes de sécurité peu onéreux et généraliser leur utilisation :**

1. Risques contre les fuites d'information :
   - Périphériques mobiles cryptés (clés USB biométriques)
   - Imprimantes à déclenchement sur place par code
   - Broyeur de documents
   - Filtres de confidentialité pour les terminaux mobiles
   - …

2. Risques contres les destructions d'information :
   - Réseau électrique sécurisé
   - Onduleurs
   - Serveurs mirorés
   - …

Exemple : clé USB biométrique

Exemple de clé USB biométrique permettant de sécuriser son contenu avec son empreinte digitale. Le système biométrique existe aussi pour les ordinateurs (démarrage, mots de passe, etc)

La meilleure solution étant toutefois d'éviter de transférer des fichiers sensibles sur clé USB. Il faut également savoir que de nombreux utilitaires permettent d'accéder à des fichiers qui ont été effacés sur une clé USB tant qu'un autre fichier n'a pas été réécrit par-dessus.

Conclusion

Conclusion

✓ **La préservation du patrimoine immatériel de l'entreprise passe par :**

1. Une vraie stratégie de protections des actifs immatériels par le brevet, la marque
2. Une prise en compte des risques liés à la fuite d'information
3. La mise en place d'une démarche globale et cohérente de sécurité de l'information sur :

- Les locaux
- Les matériels
- Les personnels

✓ **Sécurité ne veut pas dire paranoïa.**

1. Une sur-sécurité peut mener aux effets inverses de ceux désirés : les salariés chercheront à contourner une sécurité trop forte
2. La gestion du risque doit être faite de façon rationnelle en attribuant des ressources (temps et budget) sur les points les plus critiques

Annexe
Grille de mini-audit des risques

Sécurité générale

Critère	Notation (0 à 5)	Commentaires
L'entreprise dispose t-elle d'un Risk Manager ou d'une personne exerçant cette responsabilité même à temps partiel?		
L'entreprise a-t-elle des contacts avec les services officiels (DCRI, DPSD, police, gendarmerie, sapeurs pompiers…) ?		
Existe –t-il des procédures pour les visiteurs (demandes de pièces d'identités, badges, circuits de visite « balisés »…)?		

Sécurité des locaux

Critère	Notation (0 à 5)	Commentaires
Centralisation des clés ?		
Codes d'accès aux bâtiments ?		
Gardiennage ?		
Alarmes ?		
Systèmes anti-incendie ?		

Protection du patrimoine

Critère	Notation (0 à 5)	Commentaires
Les documents sensibles ont-ils été systématiquement repérés ?		
L'entreprise dépose-t-elle des brevets, marques, dessins, enveloppes Soleau ou modèles ?		
Des clauses de confidentialité ont-elles été insérées dans les contrats de travail ?		
Des clauses de non concurrence ont-elles été insérées dans les contrats de travail ?		
Le personnel est-il sensibilisé à la protection (conférences, formation, affichage, règlement intérieur…) ?		
L'entreprise a-t-elle prévu un plan de continuité d'activité ?		
Des scénarii de situation d'urgence sont-ils envisagés ?		
L'entreprise dispose-t-elle d'une charte de sécurité / sûreté ?		
L'entreprise dispose-t-elle d'un schéma directeur de sécurité / sûreté (investissements annuels et pluriannuels…) ?		
L'entreprise utilise-t-elle la « délégation de pouvoir » pour limiter la responsabilité pénale des dirigeants ?		
L'entreprise dispose-t-elle d'une cellule de crise (même virtuelle…)?		
L'entreprise emploie-t-elle ses propres personnels de sécurité ?		
L'entreprise sous traite-t-elle la sécurité / sûreté de ses locaux et sites ?		
L'entreprise organise-t-elle la formation sensibilisation de ses personnels?		

Sécurité du système informatique

Critère	Notation (0 à 5)	Commentaires
Existe-t-il un RSSI à temps plein ou partiels ?		
Gestion des droits d'accès ?		
Mots de passe systématiques ?		
Périodicité dans les changements des mots de passe ?		
Logiciels de protection (anti-spam, antivirus, firewall + leur mise à jour…) ?		
Cryptage des données ?		
Sauvegardes ?		
Existe-t-il une charte TIC (usages et responsabilités définis pour les collaborateurs…)		

Les risques managériaux

Critère	Notation (0 à 5)	Commentaires
L'entreprise anticipe t elle une défaillance de solvabilité de ses clients? (renseignement commercial…)		
L'entreprise a-t-elle pris conscience des risques de rupture d'approvisionnement (télécommunication, matières premières, énergie etc….) ?		
Anticipe-t-elle les risques psychosociaux (stress, harcèlement…) ?		
A-t-elle pris conscience du risque d'externalisation de ses données (cloud computing…)		
Dispose-t-elle d'analyses risque pays à l'exportation ?		
A-t-elle conscience des contrefaçons dont elle serait victime ?		
Envisage-t-elle la contrefaçon dès la création de nouveaux produits/services ?		
A-t-elle pris des mesures contre l'espionnage économique ?		
L'entreprise anticipe t elle les rumeurs malveillantes par de la contre information ?		
A-t-elle pris des mesures pour la protection de ses employés expatriés ?		
Dispose-t-elle d'une contre intelligence économique ?		
Edulcore-t-elle sa publicité et ses messages sortants ?		
L'entreprise a-t-elle pris conscience des risques financiers « fonds propres » et « taux de change » ?		
L'entreprise anticipe t elle une défaillance de solvabilité de ses clients? (renseignement commercial…)		
L'entreprise a-t-elle pris conscience des risques de rupture d'approvisionnement (télécommunication, matières premières, énergie etc….) ?		

Scoring des risques

Actif	Responsabilité	Valorisation			Vulnérabilités	Menaces	Vraisemblance	Risque
		Confidentialité	Intégrité	Disponibilité				

Cette grille permet de scorer le risque lié à chaque actif véhiculant ou donnant accès à de l'information.

Par exemple on mettra dans actif « téléphone portable dirigeant. »

La responsabilité sur l'actif qui peut parfois être partagée. (par exemple potentiellement dans cet exemple Dirigeant et DSI).

La valorisation côté de 1 à 5 donne une échelle du risque financier encouru si les informations de cet actif n'étaient plus confidentielles, si leur intégrité était compromise ou si elles étaient perdues.

Les vulnérabilités (dans ce cas précis le fait qu'il soit mobile).

Les menaces (le vol par exemple).

La vraisemblance notera de 1 à 5 la probabilité que le cela survienne (ici si le dirigeant est souvent en déplacement, le mobile n'est pas protégé par un mot de passe et ne dispose pas d'un effacement à distance, le risque sera majeur).

Enfin le risque est égal au plus élevé des trois critères de valorisation que multiplie la vraisemblance.

www.facebook.com/actulligence

www.twitter.com/actulligence

fr.linkedin.com/in/fmartinet

Frédéric Martinet
Consultant Intelligence Economique, Veille stratégique et e-réputation
Actulligence Consulting
+33 (0) 6 19 05 41 37
frederic.martinet@actulligence.com
www.actulligence.com