INGÉNIERIE DE LA SÉCURITÉ ET ASSURABILITÉ

Herbert GROSCOT

Jean-Pierre MARBAIX

En souvenir d'Hervé Lehning et de Jean-Marc Laloy

Les lundis de la cybersécurité – avril 2023

1

Le risque Cyber est un risque business fondamental

- **Purge et traitement de cheval de l'industrie de l'assurance qui dénote un manque de maturité du domaine** *Lucy 2022*

⇗ sinistralité : forte disparité S/P
ransomwares qui continuent à croître,
attaque des hôpitaux
⇗primes
⇘ garanties, franchises

Perte de confiance vis-à-vis des assureurs fin 2021

Un marché de l'assurance qui resterait marginal, malgré le besoin

Les assureurs ont un rôle à jouer en cyber

❑ **Comme cela a été le cas pour l'assurance habitation, l'automobile … : sujets matures stabilisés après des années de travail …**

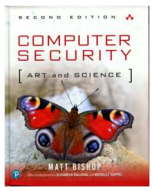
- ❖ **Rôle dans la prévention qui permet de diminuer les sinistres (nombre et charge financière) : l'assureur doit imposer de bonnes pratiques**
  - Exprimées dans un « langage commun » compréhensible par tous,
  - Pour la mise en place d'une culture de la sécurité (ce qui existe dans d'autres secteurs)
- ❖ **Rétroaction nécessaire sur les sinistres cyber, notamment les sinistres grave** (normes, pratiques, R&D)
  - Dans une hypothèse de partage des données
  - Au démarrage une activité de « data scientist »
  - Ex : l'identification de la pression artérielle comme facteur de risque cardiovasculaire vient des assureurs américains dans les années 30

⇒ Contribution à la responsabilisation des dirigeants

- ➢ … et pas seulement des RSSI ou DSI …
- ➢ Sans oublier les éditeurs de logiciels utilisés dans les entreprises
- ➢ Mais on doit les aider, on leurs fournissant les outils adéquats

3

Actuellement en cyber les recommandations sont nombreuses (ANSSI, Cyberedu, …) et bien documentées …



- ❖ **Ce que l'on trouve :**
  - Des experts qui sauraient dès aujourd'hui améliorer la sécurité d'un système,
  - Les mêmes experts qui savent dire ce qui ne va pas quand ils pénètrent dans une entreprise,
  - Des manuels qui regorgent de méthodes, techniques et recommandations pour sécuriser,
  - De nombreuses formations.
- ❖ **Peut-on affirmer que le respect des recommandations précédemment citées permettrait de réduire drastiquement la sinistralité cyber ??**
  - Les experts ont du mal à s'engager,
  - Il semble pourtant que ça marche *(Rapport LUCY et un assureur en privé)*

➢ … mais ne semblent pas structurées au sein d'une démarche globale *(ingénierie)* encourageant les dirigeant à prendre leurs responsabilités.

⇒ Il est temps de mettre de l'ordre …

4

Prévention, respect des recommandations : les responsabilités et le rôle d'un dirigeant

- **Aspects systèmes**
  - Politique de sécurité
  - Données d'importance vitale pour l'entreprise
  - Architecture
  - …
- **Organisationnels**
- **Techniques** *(mais pas seulement …)*
  - Cloisonnements
  - Sauvegardes
  - Mises à jours
  - Outils (antivirus, sondes, etc)
  - …
- **Financiers**
  - Moyens à mettre en œuvre
  - Impacts des sinistres
  - montants assurés

C'est de l'ingénierie

Appliqué couramment dans de nombreux domaines où interviennent des relations MOA/MOE… pour la réalisation de systèmes complexes

➢ Doit permettre, à terme, d'élargir le périmètre assurable, encore limité ….

➢ *En revanche, certains risques ne seront peut-être jamais assurés … ??*

5

L'ingénierie de la sécurité

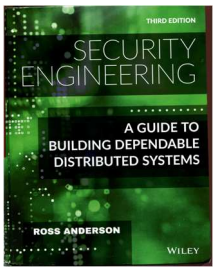
❑ **Etablissement d'une politique de sécurité prenant en compte les contraintes métier …**

❖ **Incorporation des contraintes liées à la sécurité dès la conception du Système d'Information**

❖ **Comme toute activité d'ingénierie : apporter des solutions qui satisfont des spécifications prédéfinies (la politique de sécurité)**

❖ **De plus, spécifique à la sécurité :**

- Protection vis-à-vis de l'emploi inapproprié du système
- Protection face à la malveillance

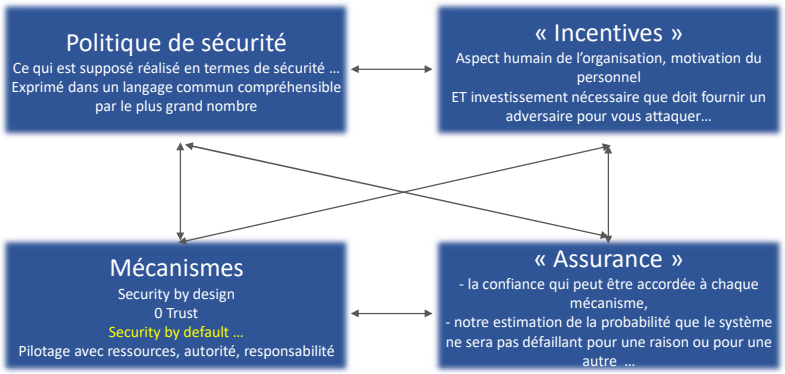


⇒ Une culture de sécurité,
ainsi que du résultat conforme et validé

6

Outre les aspects techniques (les mécanismes) …

- **sont aussi à prendre en considération les aspects métiers (politique de sécurité), humains, l'évaluation de l'efficacité des mécanismes mis en place**



D'après Ross Anderson : Security Engineering

7

… sans oublier, en amont la créativité du chef d'entreprise, et la rétroaction du côté des assureurs (et des institutionnels)

- **Penser en termes d'ingénierie en MOA, c'est bien entendu :**

Security by design *(de la responsabilité de l'entreprise)* : dès la conception prendre en compte les contraintes de sécurité ***(existe déjà)***

Security by default : exiger des fournisseurs des systèmes sûrs, et les responsabiliser ***(cf. les nouveaux textes venus des USA)***

- **Mais aussi, pour un dirigeant responsable se poser la question : « Comment faire pour que cela ne se produise pas »**
  - Un cadre « constructif » de partage d'information au lieu d'un cadre « punitif » (c'est la faute au RSSI, bien évidemment, …)
  - L'ingénierie, c'est aussi le Système D *(cf. deux exemples plus bas)*
- **Et pour un assureur et au niveau national : « Comment faire pour que cela ne se reproduise pas »**
  - Procédure de retour d'expérience, alimenté par les assureurs, les dépôts de plainte, …. : Un écosystème public/privé
  - Analogie avec le BEA (Bureau, Enquête, Analyse) …….
  - Sans oublier la R&D *(au niveau étatique et universitaire, ce qui existe depuis de décennies en informatique)*

8

Un petit mot sur les probabilités et la mutualisation du risque

- Première étape : On fait tout ce qui est possible et qui est de notre ressort pour que les incidents ne se produisent pas
  - ☺ … c'est tout simplement le bon sens
  - ☹ … encore faut-il s'en donner les moyens
- Dans ce cas, les incidents ont une fréquence suffisamment faible pour être mutualisables, et un coût suffisamment « peu catastrophique » pour que la loi des grands nombres s'applique
  - ☹ … Hélas, la loi des grands nombres n'est pas toujours vraie
- De plus, on sait alors assurer des risques coûteux
  - 😐 … car ils sont devenus suffisamment rares

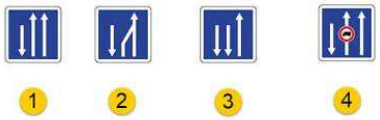
9

Un exemple : la route à trois voies

❑ **Dans les années 70 – 80, les routes à trois voies sont mortelles en France …**

En fait-on des routes à 4 voies ?
Avec ce que cela implique en termes d'investissements et de travaux …

… Ou donne-t-on un petit coup de peinture ?
Pour qu'elles deviennent des routes à 1+2 voies …



- La contre-ingénierie sociale : Le patron d'une mutuelle qui a établi une relation de confiance avec ses employés
- Détecte grâce un l'un(e) de collaborateurs(trices), un mail frauduleux potentiellement coûteux détecté à temps
- Même si l'on est dans une zone grise juridiquement (difficulté à porter plainte)

10

Un autre exemple : le Guide Michelin

❑ **Comment fait-on pour permettre à un conducteur d'effectuer le trajet Paris Nice ? Au début du 20ème siècle**

❖ En 1905, la durée de vie d'un pneu est de 100 km (sur les routes de l'époque)

➢ On fournit au conducteur un petit bouquin avec des cartes et les endroits où remplacer les pneus, manger en attendant et dormir si nécessaire

Pour la petite histoire : En 1944 les cartes Michelin ont été imprimées aux USA par les alliés avec l'accord de Michelin ….. (même si aujourd'hui ce guide est moins employé …)

➢ Le patron d'une PME qui part tous les soirs avec un disque dur externe dans sa poche, et réinstalle rapidement son système suite à une attaque

⇒ Encourager la débrouillardise et la contre-ingénierie sociale

L'exemple des ransomwares

❑ **Allier ce qui existe déjà avec la R&D**

❖ **Existe déjà**

- Quelle politique de sauvegardes pour les entreprise ?
- Prévention : anticipation de la gestion de crise, plan de continuité d'activité, …

❖ **Quelle R&D en IT ??**

- Évolution des logiciels pour qu'ils soient plus faciles à réinstaller (penser au voitures conçues dès le départ pour la faciliter le remplacement des pièces de rechange)
- Ergonomie de la cryptographie (masquer aux inconnus les données médicales sensibles …) ,
- ……

➢ La R&D une composante importante. Depuis les années 50, les réalisations IT sont spectaculaires, il faut maintenant intégrer la contrainte cyber *(avec les moyens du bord)*.

⇒ Responsabiliser les dirigeants c'est d'abords les aider à trouver des solutions, pas les punir !!!!!!

L'ingénierie de la sécurité existe déjà dans d'autres secteurs

❑ … en tant que discipline

❖ **D'autres secteurs d'activités connaissent un environnement conçu pour minimiser les accidents incluant les aspects :**

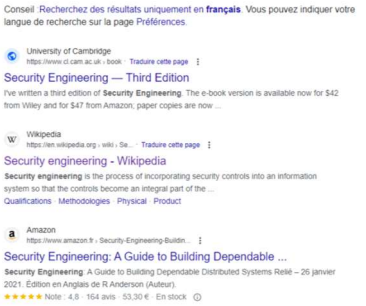
✓ Méthodologiques, Techniques, Organisationnels, Réglementaires

❖ **Recherche Google, au 10/04/2023 :**

En Français : peu de choses sur les SI

… en progrès par rapport à 2021

En Anglais : d'abords les SI



Avec des références bibliographiques

L'ingénierie de la sécurité existe déjà dans d'autres secteurs (2)

❖ **Dans ces secteurs, quand un accident se produit :**

- démarche et outils pour en analyser **les causes techniques**,
- recommandations et mesures pour que **cela ne se reproduise pas** (*ou du moins se reproduise beaucoup moins*)

❖ **Dans un tel environnement, le risque résiduel est assurable, y compris lorsqu'il porte sur de « grands risques »**

- On a imposé des procédures pour en réduire la fréquence
- Des techniques et un environnement qui en ont réduit la gravité

➢ Nous retrouvons ce que nous avons rencontré plus haut, cet ensemble cohérent :

☝ Méthodologique, Technique, Organisationnel, Réglementaire

⇒ c'est-à-dire l'Ingénierie de la Sécurité

D'autres domaines montrent qu'une ingénierie de la sécurité adaptée au domaine apporte une réponse

❑ Automobile, Habitation / Incendie, Aviation :

- **La sécurité est prise en compte dès la conception, à un niveau global (cf. slide suivant) :**
  - Ralph Nader, 1956 : "les tribunaux jugent toujours le conducteur et jamais la voiture"
  - Ralph Nader, 1965 : **"Unsafe et any Speed"**
  - une formidable campagne de presse qui mobilise l'opinion publique des États-Unis et de l'Europe.
  - Rôle des avocats, (comme dans la contre-ingénierie sociale)

Source : Olivier Barré, http://www.autocyber.fr/article/Ralph-Nader-un-avocat-qui-invente-la-s-curit-automobile

⇒ Tout doit être fait pour que le sinistre soit suffisamment rare, avec un coût maîtrisable.

Exemple : automobile

❑ Il a fallu du temps … et des combats pour diminuer la sinistralité

- **La sécurité est un objectif explicite de l'industrie**
  - Pourtant, au début du 20ème siècle, on mettait les causes des accident sur la mauvaise conduite des conducteurs *Foreign Affairs, …, février 2023*
  - Conception des véhicules
  - Infrastructures en amélioration perpétuelles

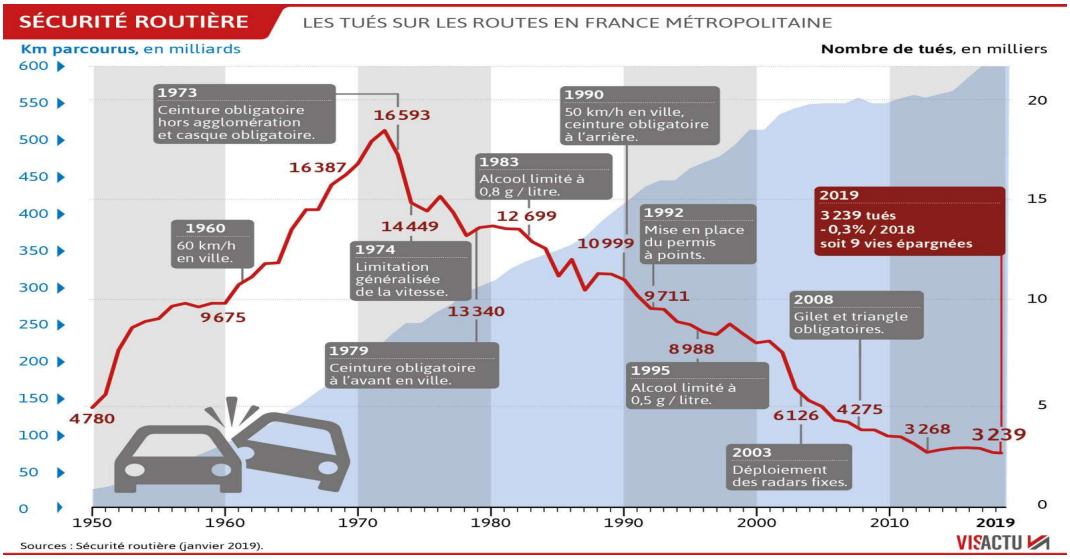
- **Permis de conduire**
- **Code de la route**
- **Police & gendarmerie qui peuvent verbaliser**
- **Dualité normes / sanctions**

➢ Assurance & responsabilisation des conducteurs

☝ Grande expérience sur la répartition des responsabilités, malus, franchise

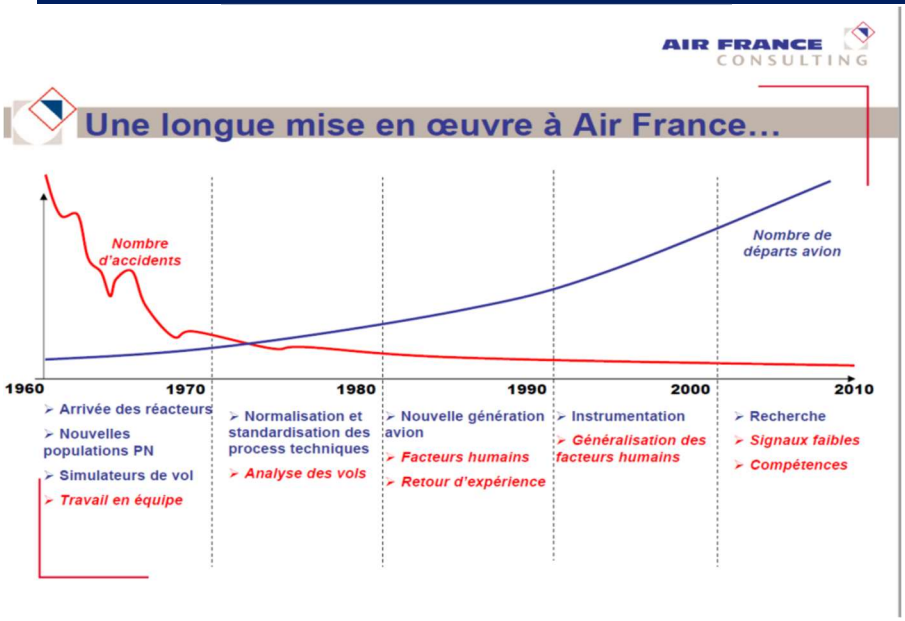
⇒ Les assureurs savent faire face aux risques extrêmes … car ils sont « suffisamment rares »

Evolution de la mortalité dur les routes depuis les années 50



Source Visactu, suggéré par Pierre-Luc Refalo

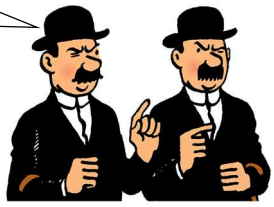
Sans oublier l'exemple de l'aviation



Fourni par JP Marbaix

Et l'Europe dans tout cela … ?

❑ **1920-1930 : 50% des voitures européennes sont belges …**



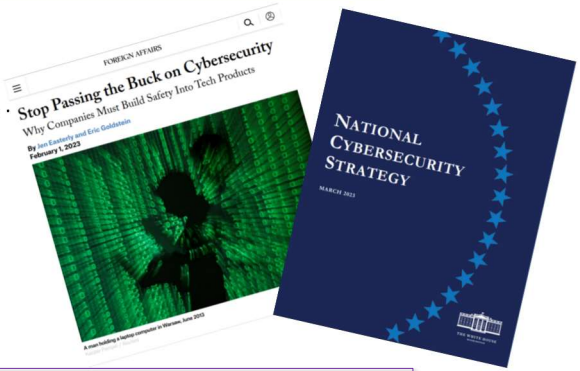
D'après la revue Foreign Affairs : ***Google***, ***Amazon*** *et* ***Salesforce*** *s'attaquent déjà au* ***« secure by default »***

On attend ***Apple, Google (Android), Microsoft***

19

Pourquoi les assureurs doivent s'approprier la discipline de « l'ingénierie de la sécurité » ?

- **Adopter un cadre qui dépasse les aspects techniques,**
  - Déjà employé dans le cas de l'incendie, l'automobile, .
- **Favoriser le partage d'information**
- **Casser des lois de probabilités « hors de prix »**
- **Améliorer la prévention**
- **Aider au lieu de punir**
- **Promouvoir la R&D**



➢ Un article et un document paru aux USA récemment

➢ L'Europe suit : « Loi sur la Cyber Résilience »

⇒ Les USA sifflent la fin de la récréation

20

Merci de votre attention

21