douhenri@yahoo.fr

La sécurité globale
des entreprises, institutions et territoires

Résumé de l'intervention du Professeur Henri Dou
Arts et Métiers – Aix en Provence
3 Février 2020

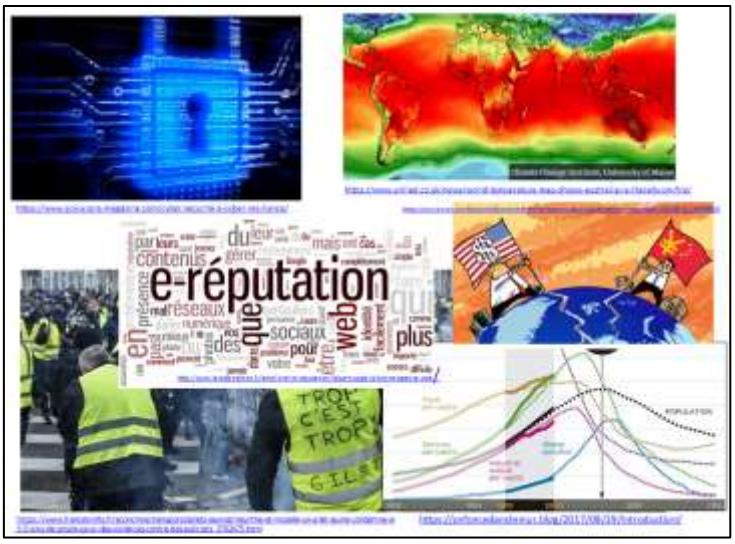
La première étape dans la notion de sécurité globale, est qu'il ne fait pas **masquer la réalité** : dans le monde actuel (et à venir), les menaces de toutes natures augmenteront, qu'elles soient cybernétiques, climatiques, concurrentielles, géopolitiques, politiques, terroristes, prédatrices, etc. **Eviter le « cela n'arrive qu'aux autres ».**

La meilleure attitude est alors d'acquérir la « résilience » nécessaire, ce qui implique :

- Avoir en fonction de son activité une perception des menaces possibles : **état des lieux**
- Développer des scénarios et envisager les attitudes et mesures à prendre en cas de menaces : **prospective et prévention**
- Acquérir le jugement et les réflexes nécessaires à une action rapide lorsque la menace se réalise : **réaction et rapidité**

Tôt ou tard, dans votre activité, vous serez confronté à une crise, plus ou moins grave, **mais inattendue,** c'est la résilience acquise par la pratique d'exercices de sécurité globale qui vous permettrons de répondre le mieux possible à cet état de fait. **Evitez d'être surpris !** Il est possible que dans les années proches les changements climatiques fassent apparaître des menaces nouvelles potentiellement dangereuses selon votre type d'activité.

Les menaces sont multiples, la figure suivante en présente quelques-unes : la Cyber – sécurité, l'e-réputation, les désordres politiques et sociaux, l'affrontement USA – Chine, le réchauffement climatique (World3 2000), etc.



On présentera rapidement quelques cas liés à des types de menaces :

- protéger votre patrimoine matériel et immatériel (comportements, législation, etc.) **NDA (Non Disclosure Agreement), marque, enveloppe Soleau**
- acquérir des réflexes informationnels endogènes (mutation épigénétiques des organisations)
- cyber sécurité : **quel que soit votre niveau de protection, vous pouvez être attaqué efficacement !** (les menaces sont multiples : communication, comportement humain (protocoles), intrusion (analyse des informations vitales et protection, attention aux clouds, etc.), **Dernière en date le Face Morphing ou deepfake** (contraction de deep learning et fake)

Conclusion

il faut s'organiser faces aux menaces potentielles, visant les membres de l'entreprise et l'entreprise elle-même. Les **procédures** robustes sont un des meilleurs moyens pour arriver à cet objectif. **Attention, la sécurité globale a un coût**.

Quelques règles simples :

- Codifiez vos informations afin de protéger l'essentiel (loi de 2018 sur le secret des affaires). On ne peut pas tout protéger, donc connaissez ce qui doit l'être et qui constitue le cœur stratégique de vos activités (Facteurs Critiques de Succès)
- Connaissez les informations qui sont divulgables et celles qui ne le sont pas
- Mettez en place des procédures de dialogue entre le personnel et les dirigeants, formez vos collaborateurs
- Soyez au courant des « arnaques classiques », ceci implique une veille sur « les menaces potentielles » attention, elles évoluent rapidement en fonction de l'imagination des « escrocs », mais aussi des avancées technologiques.
- Sensibilisez vos collaborateurs à l'usage des réseaux sociaux, ne mélangez pas vie familiale et vie de l'entreprise. S'il existe dans votre entreprise un réseau social interne, sachez le maîtriser.
- Suivant vos activités, surveillez les réseaux sociaux, sauvegardez votre e-reputation
- Protégez vos ordinateurs par des anti-virus efficaces. Ne vous contentez pas de la protection minimale gratuite.
- N'ayez aucune donnée sensible sur votre ordinateur
- Mais attention aux clés USB ou disques durs externes qui doivent être testés afin de ne pas contenir de virus

- Analysez les processus critiques de vos activités et évitez de les monitorer par réseau Internet ou autre, revenez à des procédures manuelles
- Méfiez-vous des « clouds », pas de données critiques (par exemple fichier client) sur ces derniers
- Ne croyez surtout pas votre système informatique inviolable
- Prenez toutes les précautions si vous travaillez sur des projets critiques ou confidentiels en réseau. Partager les informations à distance peut constituer un risque
- Attention à votre téléphone portable et à vos emails. Pas de transmission de données sensibles par un même canal (exemple protocole d'accord par e-mail, mais noms chiffres et dates via SMS)
- Ayez un téléphone « familial » et un téléphone professionnel, et ne les perdes pas. Un téléphone se garde toujours dans sa poche !
- Sécurisez votre entreprise physiquement, virtuellement, humainement
- Analysez vos activités et envisagez le pire et les moyens de réponses appropriés, développer des scénarios « d'attaque » et envisagez les réponses les plus pertinentes
- Ne parlez pas de projets ou d'informations critiques en public (entre autre dans les transports, les conférences, les expositions)
- Protégez vos créations (mais faites l'effort de comprendre le système de protection par brevet, par certificat d'utilité, par antériorité en France (enveloppe Soleau)
- Si vous utilisez des prestataires, exigez chez eux un bon niveau de sécurité (entre autre de cyber-sécurité)
- Certaines entreprises utilisent des services particuliers qui vérifient les e-mails (pièces jointes, etc.) avant qu'ils vous soient transmis. (sas de sécurité)
- Etc. car il y de nombreux autres points concernant la sécurité

Références :

Dou Henri, Juillet Alain, Clerc Philippe, Strategic Information for the Future, part 1. A New Strategic and Operationnal Approach, Wiley, 2019

Dou Henri, Juillet Alain, Clerc Philippe, Strategic Information for the Future, part 2. A New Information Function Approach, Wiley, 2019

Dou Henri, Du métabolisme de l'Information à l'Intelligence Economique: le rôle de la fonction information dans le changement épigénétique des individus et des organisations, R2IE Revue Internationale de l'Intelligence Economique, 10/1, 2018, pp.7-11

http://www.ciworldwide.org intelligence économique et stratégique

http://cybermalveillance.gouv.fr

https://www.economie.gouv.fr/files/dgsi-special-cybersecurite.pdf

https://competitivite.gouv.fr/fileadmin/DOCUMENTS/Actualites/Flash_DGSI_42_Manoeuvres_Ingenierie_Sociale_Avril_2018.pdf

douhenri@yahoo.fr

https://scholar.google.com/citations?hl=en&user=TiDDrHcAAAAJ
https://www.amazon.fr/l/B00AWD21WU?_encoding=UTF8&redirectedFromKindleDbs=true&rfkd=1&shoppingPortalEnabled=true