Version réservée aux membres du club TILT 85
Ne pas diffuser

ESPIONNAGE ET CYBERCRIMINALITÉ EN ENTREPRISE

Risques, enjeux et solutions

Éric Filiol

https://www.ericfiliol.site

efiliol@netc.fr

EXPÉRIENCE & SOURCES

- Expérience professionnelle
  - Formation scientifique (mathématiques et informatique) : Ing. – PhD – HDR
  - 22 ans dans la Défense et dans l'opérationnel dont 15 passés dans le domaine du renseignement technique opérationnel (+ qualifications OTAN)
  - De 2009 a 2019, direction d'un laboratoire de R&D (laboratoire de cryptologie et de virologie opérationnelles) dédiées à l'analyse, l'étude et la conception d'attaques
    - De la doctrine aux outils
  - Consultant en sécurité de l'information et des systèmes, techniques de renseignement
  - Expertise entreprises, ministères de la Justice et de la Défense
  - Étude de cas concrets (audits entreprises, missions opérationnelles…)
  - Recherche scientifique et technique (professeur associé ENSIBS, Universités Moscou [MGU, MSU HSE])
  - Appartenance à la communauté hacker ouverte et réseau personnel
- Littérature scientifique et technique
- Littérature généraliste, news
- Information à chaque fois croisée et vérifiée !

Le contexte et les acteurs

LES MENACES

LES ACTEURS

- Essentiellement trois catégories d'acteurs
  - Les Etats et en particulier ceux bénéficiant d'une position économique dominante et prédatrice

    - Contexte géostratégique de la souveraineté des états
    - Cas Huawei et industrie chinoise (attaque BGP)
    - Sociétés de « mercenaires numériques » (0Dium – NSO Group – Dark Matter)
  - Les entités mafieuses et la criminalité organisée
    - L'essentiel des attaques
    - Devenue une économie mondiale de premier plan
  - Les entités économiques mondiales (GAFAM, BATX, data brokers, autres)

- Ils peuvent collaborer selon pratiquement tous les patterns possibles
- **Environ 1 500 groupes répertoriés dont 50 de type « APT »**


Le Monde

ACTUALITÉS · ÉCONOMIE · VIDÉOS · OPINIONS · CULTURE · M LE MAG · SERVICES

Le Monde Afrique

La France et ses intérêts en Afrique sous surveillance

Plusieurs ambassades françaises ou encore Médecins du Monde ont été visées par la surveillance des agences britanniques et américaines.

Par Joan Tilouine et Simon Piel

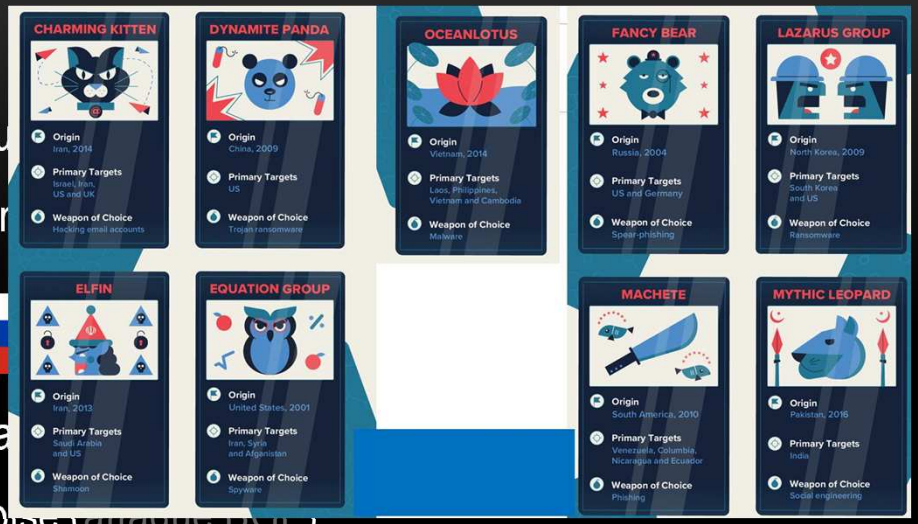
Publié le 08 décembre 2016 à 11h01 · Mis à jour le 09 décembre 2016 à 10h37 · Lecture 5 min.

Article réservé aux abonnés

L'ambassade française à N'Djamena, en 2008. PASCAL GUYOT / AFP

Si les services secrets britanniques privilégient les interceptions massives en Afrique anglophone, ils ne s'interdisent pas de lorgner sur le pré carré français, à commencer par le ministère des affaires étrangères dont la ligne fixe du standard figure dans les rapports d'écoute, comme celles de la Direction générale de la coopération internationale et du développement (DGCID, devenue Direction générale de la mondialisation, du développement et des partenariats). Autant de portes d'entrée électroniques vers les différents services de la diplomatie française.

English version : Britain spied on companies, diplomats and politicians in French-speaking Africa



ories d'acteu

lier ceux bér

égique de la

dustrie chinoise (attaque DOT)

- Sociétés de « mercenaires numériques » (0Dium – NSO Group – Dark Matter)

la criminalité organisée

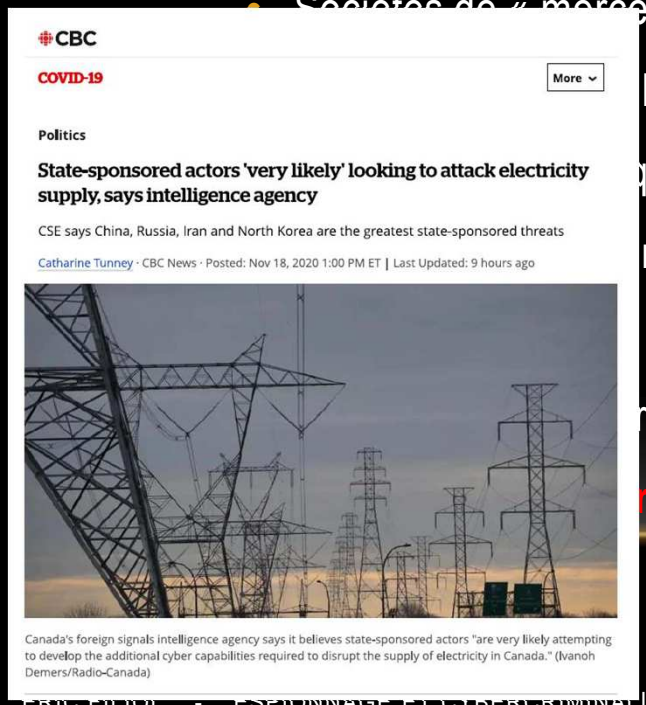
ques

mie mondiale

mondiales (

ratiquement t

rtoriés dont


CBC

COVID-19

More

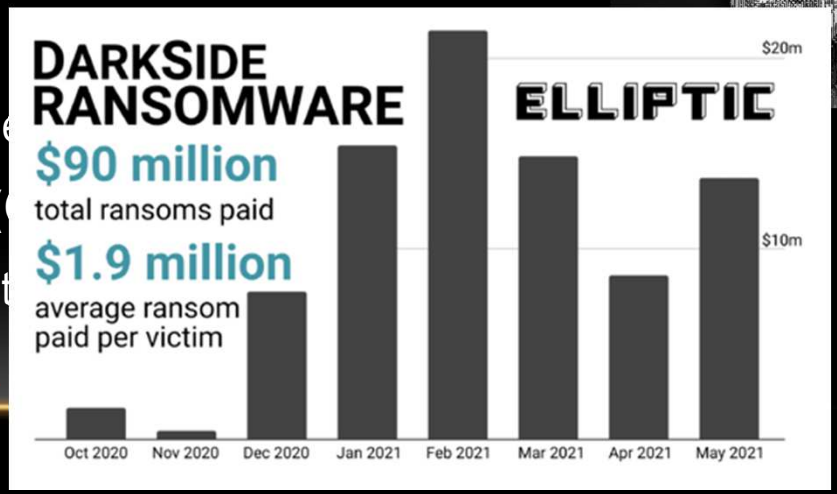
Politics

State-sponsored actors 'very likely' looking to attack electricity supply, says intelligence agency

CSE says China, Russia, Iran and North Korea are the greatest state-sponsored threats

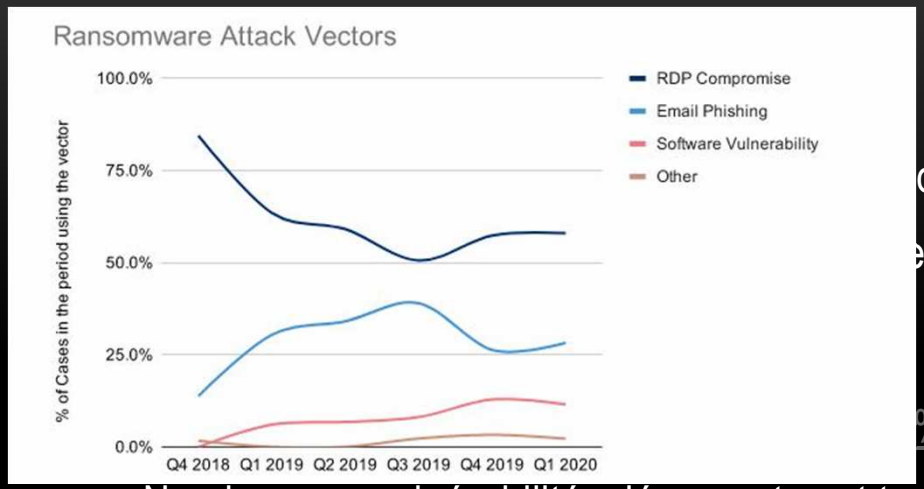
Catharine Tunney · CBC News · Posted: Nov 18, 2020 1:00 PM ET | Last Updated: 9 hours ago

Canada's foreign signals intelligence agency says it believes state-sponsored actors "are very likely attempting to develop the additional cyber capabilities required to disrupt the supply of electricity in Canada." (Ivanoh Demers/Radio-Canada)



SITUATION 2020 - 2021

- La crise COVID-19 a accéléré une tendance déjà forte
- Multiplication par 5 des attaques en particulier contre les protocoles VNC, ransomware, accès en mode RDP
- Plus de 600 000 serveurs de type VNC en accès non protégés https://www.shodan.io/search?query=%22rfb%22
- Nombreuses vulnérabilités découvertes et traitées moins rapidement
- Les entreprises ont ouvert beaucoup (trop) de ressources d'entreprises sans la sécurité nécessaire
- Environnements de travail à domicile souvent calamiteux
- Explosion des attaques par ransomware (ex. Garmin) et des modes opératoires (cas Tesla et autres)
- Augmentation des attaques contre les grandes infrastructures (énergie, finances, santé, transports…)
- Décembre 2020 – Attaque Solarwinds



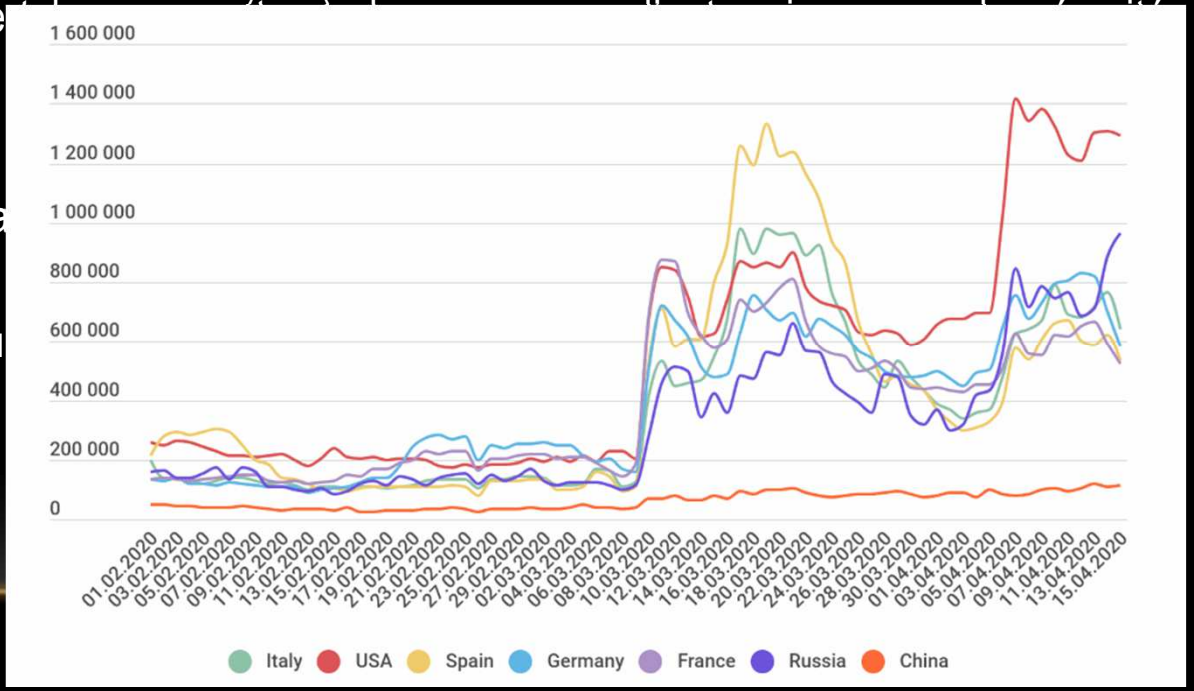
déjà forte

er contre les protocoles VNC, ransomware, accès

type VNC en accès non protégés

%22

- Nombreuses vulnérabilités découvertes et traitées moins rapidement
- Les entreprises ont ouve
  nécessaire
- Environnements de travail
- Explosion des attaques pa
  autres)
- Augmentation des attaqu
  transports…)
- Décembre 2020 – Attaque



SITUATION 2021

- Février 2021 Attaque Stormshield et Centreon
- Le problème des vulnérabilités devient ingérable
  - https://www.comparitech.com/blog/information-security/cybersecurity-vulnerability-statistics/
  - https://www.zdnet.com/article/more-than-12500-vulnerabilities-disclosed-in-first-half-of-2021-risk-based-security/#:~:text=The%20other%20report%20found%20from,by%202.8%25%20compared%20to%202020.
  - Voir rapport RedScan
  - En 2020, plus de 18000 failles découvertes
  - En 2021, 12,500 failles découvertes au premier semestre
- En conséquence, les attaques critiques se multiplient :
  - Attaques contre des banques centrales européennes
  - Attaque Kaseya Juillet 2021
  - Cloud Microsoft et bases Cosmos DB Aout 2021
  - Septembre 2021 attaques contre l'Etat français venant de Chine

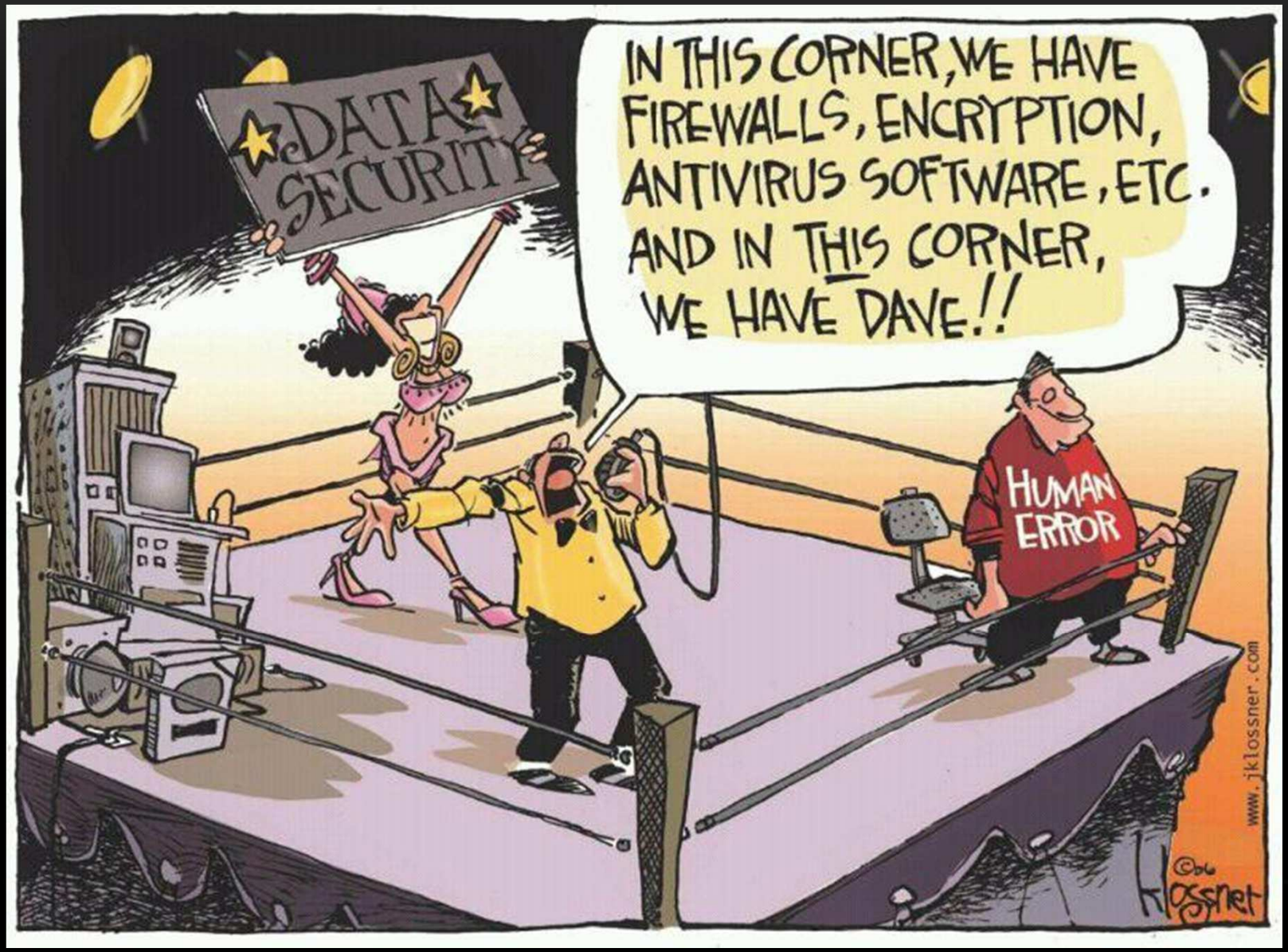
SITUATION 2021

1.2. Key findings

- More security vulnerabilities were disclosed in 2020 (18,103) than in any other year to date – at an average rate of 50 CVEs per day
- 57% of vulnerabilities in 2020 were classified as being 'critical' or 'high severity' (10,342)
- There were more high and critical severity vulnerabilities in 2020 than the total number of all vulnerabilities recorded in 2010 (4,639 including low, medium, high, and critical)
- Nearly 4,000 vulnerabilities disclosed in 2020 can be described as 'worst of the worst' – meeting the worst criteria in all NVD filter categories
- Low complexity CVEs are on the rise, representing 63% of vulnerabilities disclosed in 2020
- Vulnerabilities which require no user interaction to exploit are also growing in number, representing 68% of all CVEs recorded in 2020
- Vulnerabilities which require no user privileges to exploit are on the decline (from 71% in 2016 to 58% in 2020)
- 2020 saw a large spike in physical vulnerabilities

PRÉAMBULE ESSENTIEL

- Concernant toutes les attaques et techniques présentées, ramener le risque à l'enjeu :
  - **Le sécurité est avant tout une affaire de gouvernance**
  - Importance de relativiser en fonction de SON métier
  - Prééminence du PCA/PRA
  - Résilience vs sécurité.
- La quasi-totalité des attaques exploitent une ou plusieurs faiblesses, vulnérabilités ou erreurs
  - C'est l'extrême faiblesse des victimes qui est déterminante et non la « prétendue » force des attaquants (même s'il existe des attaquants très doués)
- Il y donc **toujours** une solution et les attaques ne sont pas une fatalité !


DATA SECURITY
IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC.
AND IN THIS CORNER, WE HAVE DAVE!!
HUMAN ERROR
www.jklossner.com
©bc Klossner

RISQUES MAJEURS ACTUELS

Le risque MAJEUR est le blocage de l'activité !!

- **Fuite de données (directe, indirecte)**
- **Arnaques et attaques financières**
- **Déstabilisation d'entreprise - Attaque contre les personnes – Désinformation**
- Toutes les attaques modernes reposent sur la collecte préalable et généralisée de renseignement! La partie informatique n'est qu'un outil, quelquefois au rôle réduit

SURFACES D'ATTAQUES

- Il n'y a pas que la partie technique et informatique qui entre en jeu mais bien d'autres aspects hérités des techniques de renseignement: attaques informationnelles, attaques humaines, ingénierie sociale...
- La plupart des attaques sont simples à préparer et peuvent être menées pas un grand nombre de personnes, pour un coût relativement réduit.
- Sphère informationnelle et humaine :
  - Passif (OSINT) : renseignement et préparation de l'attaque
  - Actif : déstabilisation, influence
- Sphère Informatique (SI) : attaque sur les ressources et services exposés
- Sphère physique : pénétration des locaux, piégeage… Cette menace augmente significativement

Comment se protéger

RÈGLEMENTATION, MESURES ET PROTECTION

PRINCIPE GÉNÉRAL

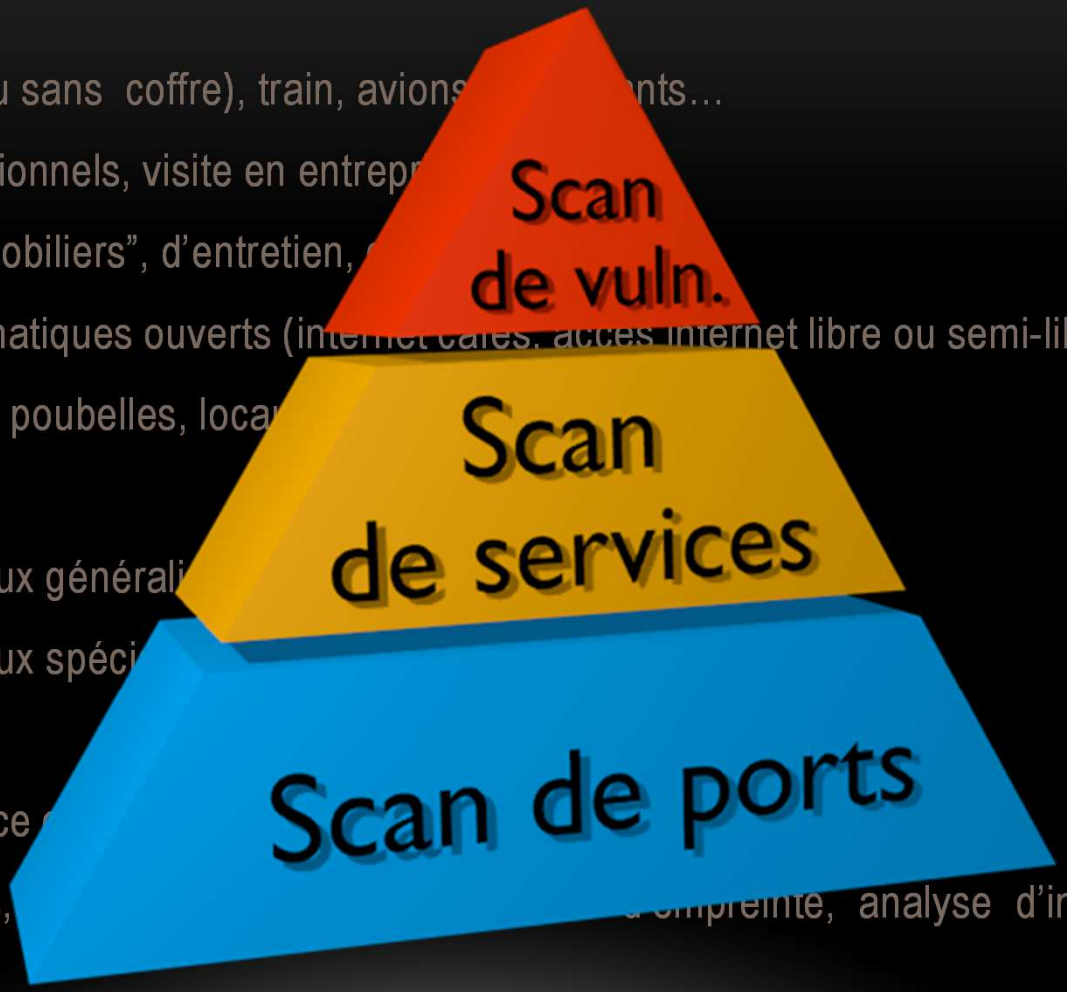
- La sécurité n'est pas un but en soi ! C'est un outil au service d'un cœur de métier !
- Une sécurité mal maitrisée tue le cœur de métier
- Trop de sécurité ou une sécurité trop envahissante tue la sécurité
- Le personnel de sécurité ne doit pas être un "Etat dans l'Etat"
  - Séquestre des mots de passe des comptes avec privilèges.
- C'est la connaissance des risques qui vous indiquera naturellement les pratiques adaptées à votre cœur de métier
  - Exemple : fuites de données et matrices des données/matrices des flux réseau
- La sécurité est avant une affaire de gouvernance et un état d'esprit !

CIBLES DE SÉCURITÉ

- Lieux physiques :
  - Hôtels (avec ou sans coffre), train, avions, restaurants…
  - Salons professionnels, visite en entreprises…
  - Personnels “mobiliers”, d’entretien, de maintenance
  - Espaces informatiques ouverts (internet cafés, accès internet libre ou semi-libres…)
  - Photocopieurs, poubelles, locaux entreprises…
- Lieux immatériels :
  - Réseaux sociaux généralistes (Twitter, Facebook…)
  - Réseaux sociaux spécialisés (Copains d’avant, Viadeo, LinkedIn…)
- SIC
  - La connaissance et la surveillance des ressources exposées est prioritaire.
  - Scan de ports, scan de vulnérabilités et prise d’empreinte, analyse d’infrastructure web…

CIBLES DE SÉCURITÉ

- Lieux physiques :
  - Hôtels (avec ou sans coffre), train, avions… nts…
  - Salons professionnels, visite en entrep…
  - Personnels "mobiliers", d'entretien, …
  - Espaces informatiques ouverts (internet cafés, accès internet libre ou semi-libres…)
  - Photocopieurs, poubelles, loca…
- Lieux immatériels :
  - Réseaux sociaux généra…
  - Réseaux sociaux spéci…
- SIC
  - La connaissance …
  - Scan de ports, … empreinte, analyse d'infrastructure web…



SÉCURITÉ DES CONNEXIONS DISTANTES AU SI ENTREPRISE

- Vérifier que les employés utilisent des mots de passe forts.
  - Tests de craquage de mots de passe
  - Imposer l'usage des gestionnaires de mots de passe (Keepass, BitWarden, Dashlane)
- Rendre le RDP disponible uniquement par le biais d'un VPN d'entreprise
  - Changer la valeur par défaut du port
  - Si vous n'utilisez pas RDP, désactivez-le et fermez le port 3389
- Utiliser l'authentification au niveau du réseau (*Network Level Authentication* - NLA)
- Si possible, les employés doivent utiliser une authentification à deux facteurs
- Gestion des correctifs de sécurité rigoureuse et réactive.

LUTTE CONTRE L'EXTORSION

- Usurpation d'identité (dirigeants, fournisseurs, tiers techniques…)
  - Définir des procédures et les tester/actualiser régulièrement
  - Maîtriser les informations de la société et des personnes
- Vol de ressources (fret, téléphonie, serveurs…)
  - Gérer les accès (cartographie des services), changer les mots de passe par défaut (software ET hardware), appliquer les correctifs de sécurité…
  - Mettre des mots de passe (ex. Caméra IP ou objets connectés)
- **Ransomware**
  - Sans politique de sauvegarde RIGOUREUSE et périodiquement testée, il n'y a aucune solution

MESURES DE BASE INCONTOURNABLES

- **En mobilité**
  - Chiffrez vos terminaux (portables, smartphones, tablettes)
  - Utilisez un filtre de confidentialité
  - La connexion au SI entreprise doit se faire obligatoirement par un VPN entreprise !
  - Utilisez systématiquement des VPN commerciaux (Windscribe, NordVPN, Black VPN, BolehVPN, Protonmail) pour les autres usages
  - Evitez les wifi tiers (et plus généralement toute ressource qui n'est pas la votre.
- Formez et sensibilisez constamment vos personnels et collaborateurs
- Utilisez des gestionnaires de mots de passe

PRINCIPALES MESURES

- Sur le plan technique
  - Cartographiez, cartographiez, cartographiez !
  - Importance du dossier de site
    - Schéma d'architecture physique, logique et applicatif
    - Interconnexions réseau
    - Interactions humaines (gestion des intervenants)
    - Scan de ports, analyse de vulnérabilités, analyse infrastructure web
    - Matrice des flux et surveillance des flux réseau
  - Mettez à jour. Application réactive des correctifs de sécurité.
  - Privilégiez le maintien du cloisonnement physique. Sinon filtrez strictement le sens de communication (diode) et/ou le contenu des protocoles (pare-feu)

PRINCIPALES MESURES (2)

- Sur le plan organisationnel
  - Cartographie des ressources (humaines, services, prestataires, composantes externes…)
  - Cartographie des données
- Importance primordiale des sauvegardes et de leur vérification régulière.
- Plan de gestion de crise notamment pour tout ce qui touche la communication.
- Rappel : toutes ces mesures relèvent directement du RGPD !
  - Le point le plus critique est la cartographie des sous-traitants, leur évaluation (compétences réelles, sécurité, contrat de service…) et leur gestion

ESURES (2)

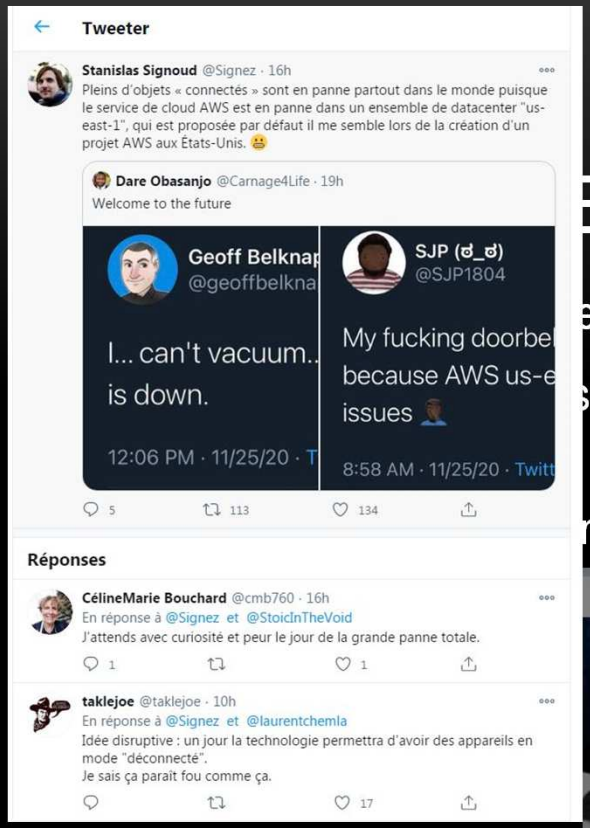
el

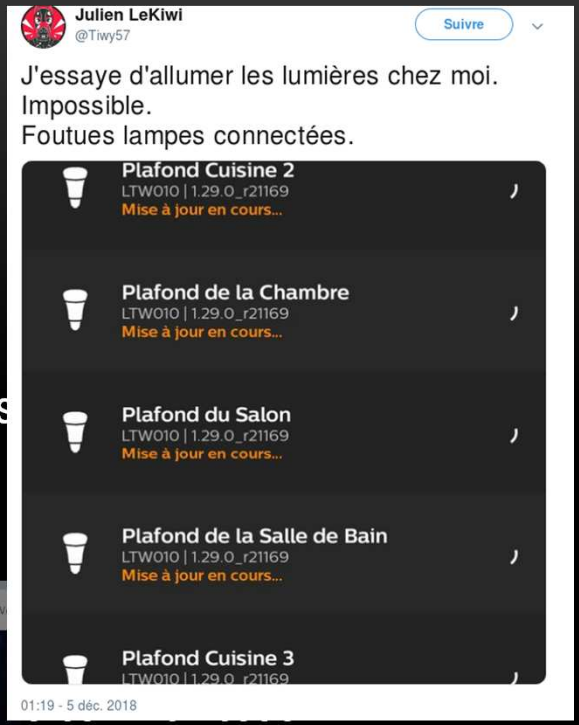
ssources (humaines, services, pres

nnées

!

- Le point le plus critiq itants, leur évaluation (compétences réelles leur gestion

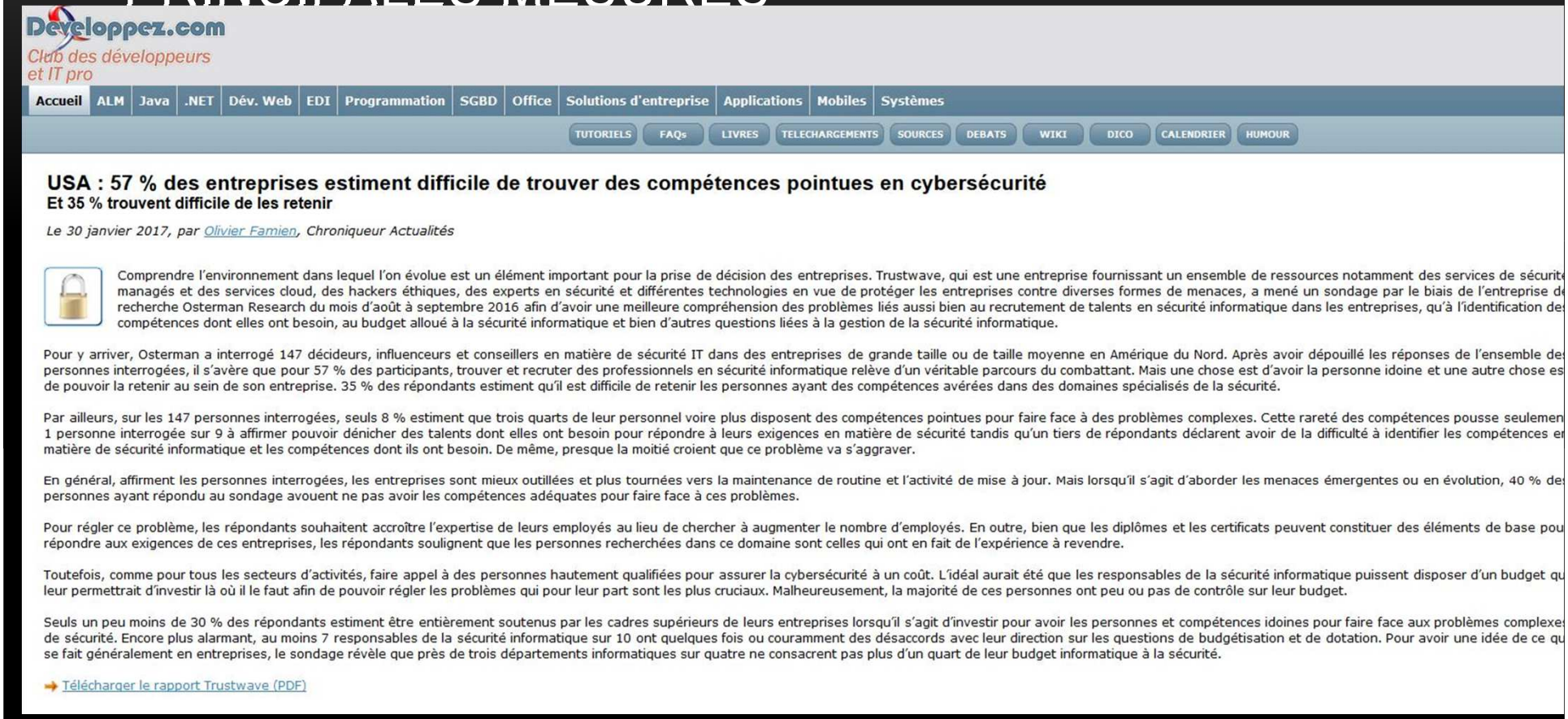




PRINCIPALES MESURES

- Sur le plan humain et DRH
  - La fragilité des entreprises va augmenter face aux mutations des mentalités
  - Réformer et adapter le management
    - Management technique et opérationnel : problème d'acceptation et de légitimité
  - Revoir les processus de recrutement
    - Pénurie de juniors
    - Volatilité et loyauté des personnels
    - Pénurie extrême de seniors « techniques » (cas CERT Banque)
    - L'Ethique avant la technicité.
    - Management RH classique : les règles et recettes classiques ne fonctionnent plus. Problème de maturité des personnels RH
  - Revoir les processus de gestion RH sur le long terme. *Investir plutôt que recruter !*

PRINCIPALES MESURES



Developpez.com
Club des développeurs et IT pro

Accueil | ALM | Java | .NET | Dév. Web | EDI | Programmation | SGBD | Office | Solutions d'entreprise | Applications | Mobiles | Systèmes

TUTORIELS | FAQs | LIVRES | TELECHARGEMENTS | SOURCES | DEBATS | WIKI | DICO | CALENDRIER | HUMOUR

USA : 57 % des entreprises estiment difficile de trouver des compétences pointues en cybersécurité
Et 35 % trouvent difficile de les retenir

Le 30 janvier 2017, par Olivier Famien, Chroniqueur Actualités

Comprendre l'environnement dans lequel l'on évolue est un élément important pour la prise de décision des entreprises. Trustwave, qui est une entreprise fournissant un ensemble de ressources notamment des services de sécurité managés et des services cloud, des hackers éthiques, des experts en sécurité et différentes technologies en vue de protéger les entreprises contre diverses formes de menaces, a mené un sondage par le biais de l'entreprise de recherche Osterman Research du mois d'août à septembre 2016 afin d'avoir une meilleure compréhension des problèmes liés aussi bien au recrutement de talents en sécurité informatique dans les entreprises, qu'à l'identification des compétences dont elles ont besoin, au budget alloué à la sécurité informatique et bien d'autres questions liées à la gestion de la sécurité informatique.

Pour y arriver, Osterman a interrogé 147 décideurs, influenceurs et conseillers en matière de sécurité IT dans des entreprises de grande taille ou de taille moyenne en Amérique du Nord. Après avoir dépouillé les réponses de l'ensemble des personnes interrogées, il s'avère que pour 57 % des participants, trouver et recruter des professionnels en sécurité informatique relève d'un véritable parcours du combattant. Mais une chose est d'avoir la personne idoine et une autre chose est de pouvoir la retenir au sein de son entreprise. 35 % des répondants estiment qu'il est difficile de retenir les personnes ayant des compétences avérées dans des domaines spécialisés de la sécurité.

Par ailleurs, sur les 147 personnes interrogées, seuls 8 % estiment que trois quarts de leur personnel voire plus disposent des compétences pointues pour faire face à des problèmes complexes. Cette rareté des compétences pousse seulement 1 personne interrogée sur 9 à affirmer pouvoir dénicher des talents dont elles ont besoin pour répondre à leurs exigences en matière de sécurité tandis qu'un tiers de répondants déclarent avoir de la difficulté à identifier les compétences en matière de sécurité informatique et les compétences dont ils ont besoin. De même, presque la moitié croient que ce problème va s'aggraver.

En général, affirment les personnes interrogées, les entreprises sont mieux outillées et plus tournées vers la maintenance de routine et l'activité de mise à jour. Mais lorsqu'il s'agit d'aborder les menaces émergentes ou en évolution, 40 % des personnes ayant répondu au sondage avouent ne pas avoir les compétences adéquates pour faire face à ces problèmes.

Pour régler ce problème, les répondants souhaitent accroître l'expertise de leurs employés au lieu de chercher à augmenter le nombre d'employés. En outre, bien que les diplômes et les certificats peuvent constituer des éléments de base pour répondre aux exigences de ces entreprises, les répondants soulignent que les personnes recherchées dans ce domaine sont celles qui ont en fait de l'expérience à revendre.

Toutefois, comme pour tous les secteurs d'activités, faire appel à des personnes hautement qualifiées pour assurer la cybersécurité à un coût. L'idéal aurait été que les responsables de la sécurité informatique puissent disposer d'un budget qui leur permettrait d'investir là où il le faut afin de pouvoir régler les problèmes qui pour leur part sont les plus cruciaux. Malheureusement, la majorité de ces personnes ont peu ou pas de contrôle sur leur budget.

Seuls un peu moins de 30 % des répondants estiment être entièrement soutenus par les cadres supérieurs de leurs entreprises lorsqu'il s'agit d'investir pour avoir les personnes et compétences idoines pour faire face aux problèmes complexes de sécurité. Encore plus alarmant, au moins 7 responsables de la sécurité informatique sur 10 ont quelques fois ou couramment des désaccords avec leur direction sur les questions de budgétisation et de dotation. Pour avoir une idée de ce qui se fait généralement en entreprises, le sondage révèle que près de trois départements informatiques sur quatre ne consacrent pas plus d'un quart de leur budget informatique à la sécurité.

Télécharger le rapport Trustwave (PDF)

- Revoir les processus de gestion RH sur le long terme. *Investir plutôt que recruter !*

PRINCIPALES MESURES

- Sur le plan informationnel
  - Défensif
    - Evaluer l'image de l'entreprise et de ses principaux salariés/dirigeants
    - Problème de discrétion professionnelle
    - Problème des réseaux sociaux
    - Audit informationnel à mener
  - Offensif
    - Comprendre l'environnement et ses adversaires, comment ils pensent et ils agissent (culture, sociologie, psychologie…).
    - Audit informationnel à mener

DROIT VERSUS TECHNOLOGIE

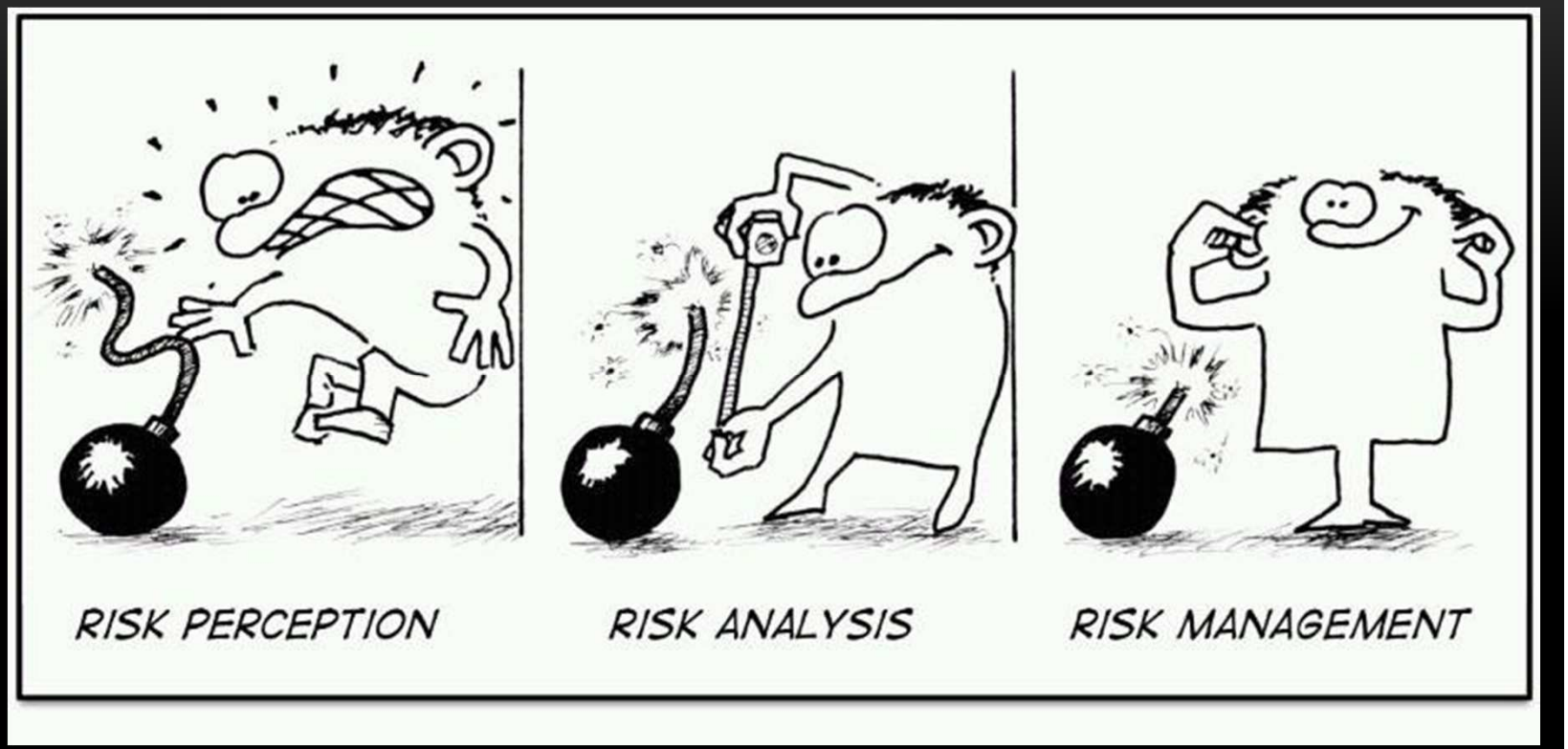
- La technologie (Cloud, VoIP/ToIP, hébergement externalisé…) n'est pas en cause
- La dimension essentielle est celle du droit
  - Droit français/européen (rapport commission LIBE du 12 mars 2014, RGPD)
  - Droit anglo-saxon
- Importance cruciale du contrat (source de droit prioritaire)
  - Doit être négociable (opérateurs privés préférables aux opérateurs publics)
  - Prestataire : devoir de conseil, de renseignement et de mise en garde (L.111)
  - Doit couvrir *a minima* trois types de mesures :
    - Ordre organisationnel (système de redondance, sauvegardes…). Lié au PCA/PRA
    - Ordre préventif : possibilité pour le client de diligenter des audits (clause d'audit)
    - Clause de réversibilité : obligation faite au prestataire pour redonner la main au client sur le système externalisé.
- Importance du contrat d'assurance

Points clef et idées maitresses

CONCLUSION

RAPPELS DE QUELQUES PRINCIPES (2)

- On doit apprendre à vivre avec le risque et savoir le gérer.
- Se préparer à un éventuel problème
- En entreprise
  - Identification des ressources, biens, personnels critiques
  - Politique de sauvegarde.
  - Politique de maintien d'activité en cas de problème (PCA)
  - Politique de reprise d'activité et de restauration (PRA)
  - Plan de gestion de crise
- Adéquation des moyens aux besoins réels (ramener le risque à l'enjeu)
- Prééminence du droit sur la technique. Le contrat de service est la clef.
- Investir et faire fond sur l'humain.



Merci de votre attention

QUESTIONS & RÉPONSES