DDD 8 : spécial
Sécurité numérique

Le vrai risque numérique se situe entre l'écran et le clavier : l'homme et ses propres usages !

Severine Watry - PhotoMindset

Dans le tourbillon numérique, lucidité et bon sens se noient : pourtant ils sont nos meilleurs détecteurs de pièges !

La semaine dernière Facebook annonçait le piratage de 50 millions de comptes : un petit piratage, le record serait détenu par Yahoo avec un milliard de comptes !

Bonne nouvelle nous apprenons dorénavant ces piratages plus rapidement : auparavant il pouvait se passer des années durant lesquels nous laissions notre porte ouverte sans le savoir à quiconque avait pu récupérer ou racheter nos codes.

Moins bonne nouvelle, les piratages de comptes et autres attaques numériques deviennent si nombreux, qu'ils en deviennent "naturels". Mais bonne nouvelle les entreprises peuvent ainsi plus facilement jouer la carte de la transparence, même si elles ne s'empressent pas de le faire, primes d'objectifs ou cours de bourse obligent.

En effet nous avons mal perçu l'évolution de la quantité de piratages possibles, liée à « trois quantités » qui augmentent de façon exponentielle :

- La quantité d'objets connectés est devenue phénoménale : plusieurs dizaines de milliards, le nombre de 50 milliards avant 2020 étant le plus souvent évoqué). Le problème ? Même les objets les plus simples (ex. une lampe) ou ceux les plus à sécuriser sont faillibles (ex. : « *des milliers de failles détecté dans les pacemakers !* »).
- La quantité de types de programmes différents intervenant pour la création, le traitement, la mise en forme ou le transfert d'une information - souvent elle-même couplée à d'autres données – devient infinie. Mais surtout ces assemblages numériques sont « mouvants » : les versions et mises-à-jours de produits sont écrites selon des langages multiples… eux-mêmes évolutifs . Il n'est pas possible de figer une cartographie des risques et d'offrir l'anti-virus définitivement sûr. Certes des modélisations d'attaques nés de l'intelligence artificielle existent, mais ils ne peuvent pas prendre en compte ce qu'hier n'était même pas imaginable.
- La quantité d'acteurs humains et organismes impliqués - le plus souvent pas même localisables physiquement – ne permet plus de savoir « qui est qui » et « qui fait quoi » . Si les équipes qui produisent les programmes restent à 99% fiables, leurs multiplications… multiplient les 1% de personnes à risques comme dans toute profession.. D'autres part parmi elles, de plus en plus sont tentées par le piratage à but lucratif : du rançonning (devoir payer une rançon pour par exemple débloquer votre ordinateur, neutralisé à distance), à la vente de tout ou partie de vos données numériques (de votre correspondance (ex. 50 €) à votre "vie numérique" entière (ex. 300 €)).

Bonne ou mauvaise nouvelle, en grande partie être piraté ou pas à titre personnel ou pour une entreprise… dépend de nous. Au quotidien les risques grâce aux cyberprotections restent faibles, si l'on n'ouvre pas de manière compulsive tout fichier, tout lien ou tout site. C'est encore plus vrai quand on ne connaît pas la source, et que zapping numérique ou impulsivité obligent, nous ne nous laissons plus le temps de voir ce « qui cloche » : la meilleure arme anti-criminalité reste le bons sens !

Attention à la « ligne Maginot numérique »

En ce mois Européen de la Cybersécurite, salons et conférences se multiplient pour proposer process et technologies de protection numérique : mais regardez bien les programmes vous n'y trouverez presque jamais le mot comportement à risques (ou sécurité comportementale). Nous construisons une « ligne Maginot numérique » en bétonnant techniquement sans regarder ce qui se passe ailleurs. L'ailleurs est « entre l'écran et le clavier » : l'homme ou la femme qui clique.

Ce numéro est une invitation à regarder notre sécurité autrement en encourageant à remettre les comportements humains au cœur des débats : pas tout le temps (n'en faisons pas une obsession) mais au moins une fois par mois tel un DDD8 !

L'histoire secrète de nos comportements numériques

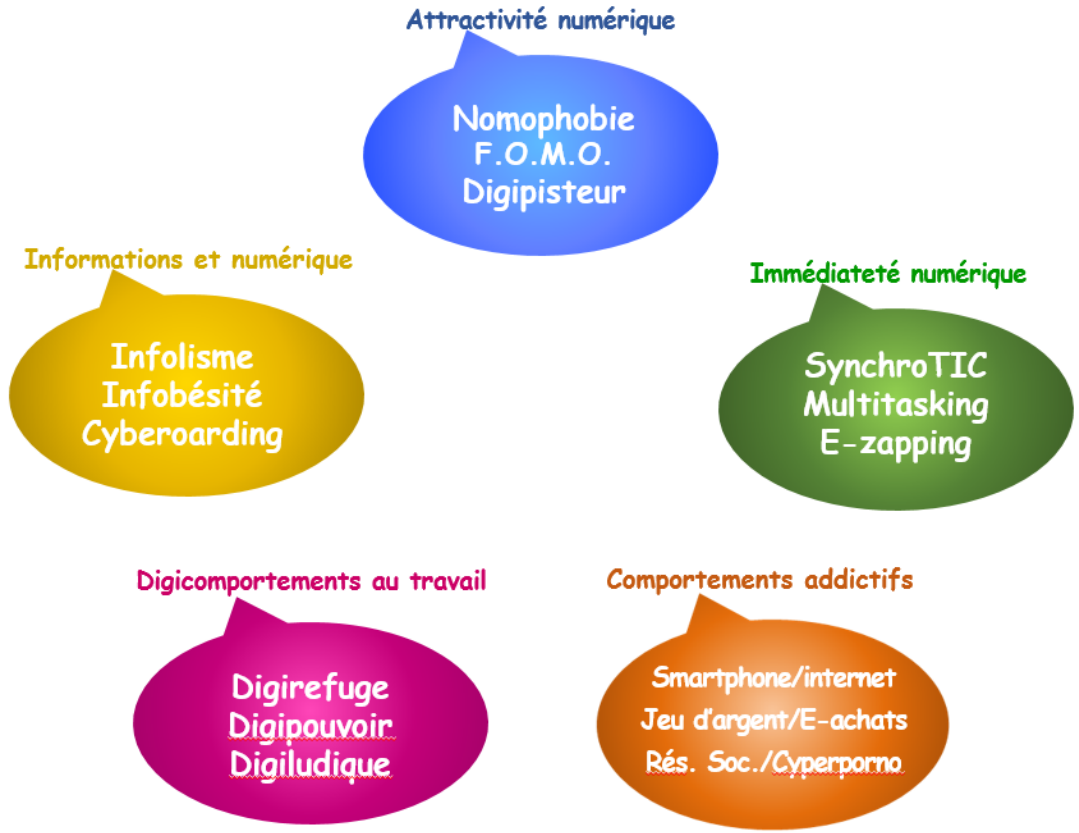
C'est une histoire secrète, celle de nos comportements numériques. Ils se sont silencieusement développés lors de la bascule 2012 vers l'hyperconnexion. Pour la 1ère fois sont réunis au grand jour les acteurs-clés de nos vies (ex. FOMO).

En 2018 les deux tiers d'entre nous connaissent la Nomophobie, ou peur d'être séparé de notre smartphone (ou s'il est hors zone, déchargé, égaré). Recevant ainsi messages et news 24/24H. la F.O.M.O. (Fear Of Missing Out) s'empare de nous : la peur de rater quelque chose. Digipisteurs, pour en savoir toujours plus nous pistons sans fin de liens en liens hypertext les "vérités".

Ainsi notre soif d'informations devient inextinguible, c'est l'Infolisme. L'"Infobésité nous guette, mangeurs jamais rassasiés d'informations. Nous les ramassons et stockons sans limite : c'est le Cyberoarding.

L'immédiateté règne : nous sommes SynchroTIC, centrés sur la relation en temps réel. Chaque message se traite dès son arrivée donc en même temps que la tâche en cours : c'est le Multitasking (multitâche). Habitués à passer de tâches en tâches et déconcentrés permanents, c'est l'ère du E-zapping.

Ces acteurs-clé de notre vie "naturelle" peuvent favoriser des Digicomportements au travail où des Comportements addictifs… et réciproquement.



Les acteurs-clé de nos vies numériques

La sécurité numérique *v.s* la synthèse de nos nouveaux comportements

Ces comportements nous font accéder trop vite à trop d'informations à risques, puis à les rediffuser immédiatement massivement.
Travailler en mode réflexe ne permet plus de repérer ce qui "cloche".

Retrouvez au DDD8 de novembre un exposé sourcés sur les acteurs-clé de nos vies numériques !

Risques comportementaux liés au numérique

Attractivité
Permanence

Surinformation
Infobésité

Immédiateté

Digicomportements
au travail

Comportements
addictifs

La majeure partie des risques numériques proviennent de notre précipitation à ouvrir liens, sites ou fichiers à risques. Déconcentrés par le travail en multitâche ou épuisés par les 24/24H digitaux, nous les ouvrons aussi par inadvertance ou rageusement lors des "RE-RE-RE" auxquels nous contribuons.

Infolisme et infobésité augmentent vertigineusement la masse d'informations éparses, du Cloud mal maîtrisé aux disques durs externes et clés USB éparpillées. L'attractivité/addictivité numérique nous pousse trop vers des sites, expériences et contacts à risques.

La majorité des risques numériques : les comportements humains !

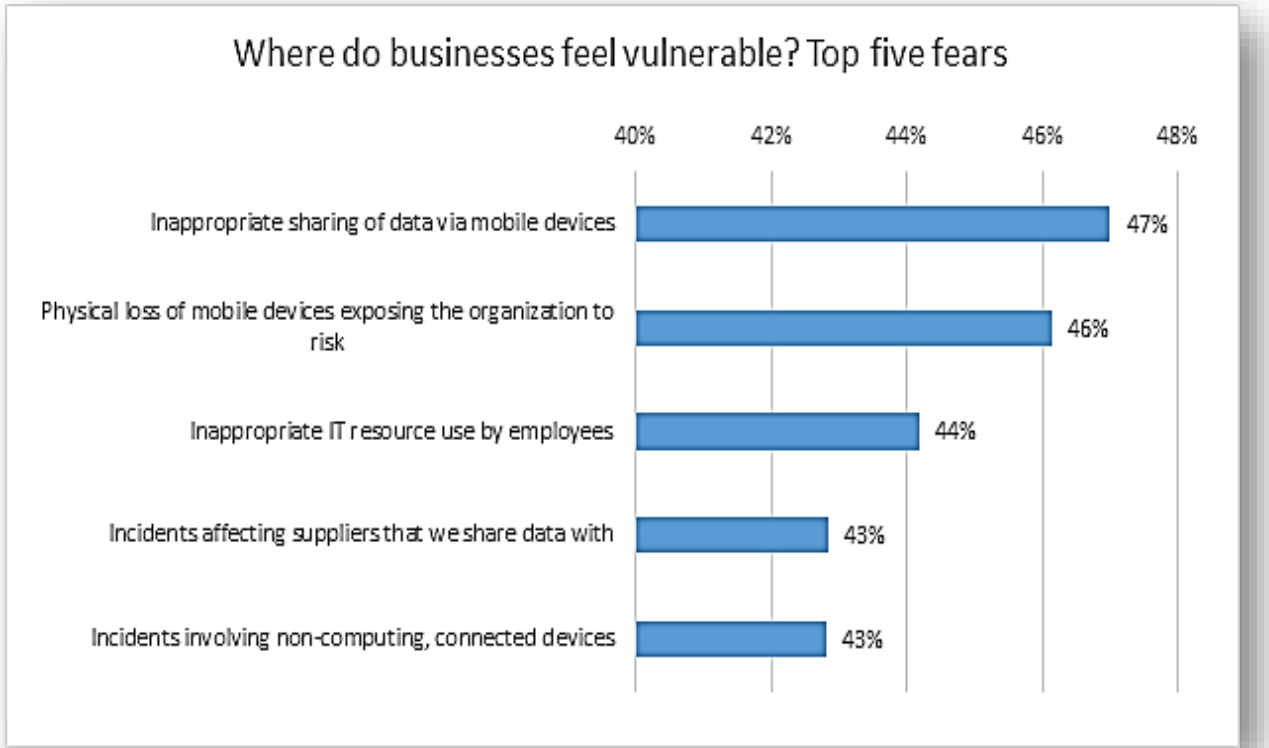
Le risque vient de « l'intérieur »

Dans un contexte de cyber-menace complexe et en pleine croissance, où 57% des entreprises pensent désormais que leur sécurité informatique sera compromise, elles se rendent compte également que leurs propres employés sont l'un des principaux obstacles à leur protection contre les cyberattaques.

En fait, **52%** des entreprises reconnaissent que les employés constituent leur plus grande faiblesse en matière de sécurité informatique, leurs actions négligentes mettant en péril leur stratégie de sécurité informatique.

La crainte d'être menacé de l'intérieur est clairement visible par le fait que, pour les entreprises, **les trois principales craintes de cybersécurité sont toutes liées aux facteurs humains et au comportement des employés**. Le tableau ci-dessous montre que les entreprises sont conscientes de la facilité avec laquelle une erreur humaine peut avoir une incidence sur la sécurité de leur entreprise.

https://www.kaspersky.com/blog/the-human-factor-in-it-security/



Source: IT Security Risks Survey 2017, global data

Réduire les risques personnels : reprendre la maîtrise de nos tempo numériques

Equilibre des Temps & Temporalités numériques :

Commençons par un fil conducteur des DDD8 : les Temps & Temporalités numériques.
Vous l'avez maintenant compris, notre premier piège est nous-même : pas par faiblesse d'esprit, mais par ce qui nous attire trop vers le risque (attractivité & addictivité numérique) et ce qui nous fait perdre vigilance et bon sens élémentaires.

Trois temporalités malmenées sont en cause :

- La permanence numérique - "Clics" partout tel dans un métro bondé où l'on voit à peine son écran, au milieu de la nuit ensuqué, en voiture concentré sur la route, etc. : "always connect" nous surmultiplions les situations à risques. Si le nombre d'heures d'écran est excessif, c'est la fatigue qui affecte notre vigilance générale, et dans tous les domaines. Nous pouvons aussi par hyperexcitation, trop prêts à des aventures numériques à risques.

- L'immédiateté – Fiers d'être "toujours joignables", nous nous précipitons pour répondre : comportement de conformité oblige, nous nous croyons aussi obligés de répondre en temps réel.

- Le multitâche – En traitant plusieurs tâches à la fois ou en suivant plusieurs conversations, entre prises de risques et "erreurs fatales" … et parfois mélanges des actions nous sommes hors de toute règle de sécurité.

La sécurité numérique impacte tous les aspects de notre vie

3 premiers conseils :

1) *Réapprendre à déconnecter à quelques justes moments : c'est l'enjeu des DDD8 (Cf. xxx)*
2) *Pour les messages à traiter : classer les "sûrs" et les traiter et pour les plus inconnus se fixer un moment plus zen.*
3) *Nos escapades numériques (ex. visites de sites en tous genres…) : ne pas les faire en même temps que d'autres actions.*

3 ennemis à éliminer de vos vies numériques

Chronophages, déprimants voire sources de problèmes, repérez les :

- « Troll » : polémistes et embrouilleurs. Sur les réseaux ils lancent des débats houleux qui vous font perdre temps et énergie.

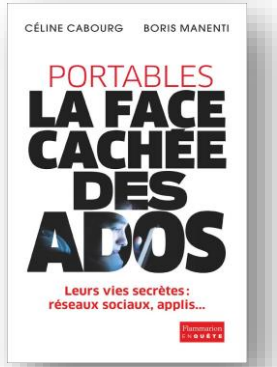
- « Mytho » : déprimants, ils font tout mieux que vous !

- « Hater » : on rit d'abord de leur moquerie : attention à ne pas en devenir victime car ils peuvent être destructeurs.

Parents et enfants : informez-vous en 3 actes !

Acte I - Il y a un monde entre eux et nous : découvrez leur monde !

Comprendre leur monde (ex. La face cachée des Ados) : c'est essentiel pour l'empathie (être un peu à leur place)… et dialoguer sans être décalé. Il s'agit aussi de disposer de bons repères : à quels âges peut-on autoriser quels usages par exemple, sans leur laisser prendre trop de risques mais sans en faire des exclus du monde numérique et qui plus que nous sera le leur.



Acte II – Hyperconnexion, au jeu du chat et de la souris : apprenez à gagner !

Ce sont dans les dessins animés que les chats ne parviennent jamais à attraper les souris : dans la vraie vie il en va différemment. Oui vous avez le droit de poser des limites salvatrices, tel pas de numérique après 22 heures par exemple (selon l'âge). Ils voudront "gruger" si vous voulez bloquer leur ordinateur : c'est normal. Au jeu du chat et de la souris vous pouvez être le chat : c'est votre territoire, restez le maître. A vous de vous informer plus auprès des "digital mum", ces nouvelles mères nées avec le digital et à qui "on l'a fait pas", ou dans votre entourage : on a tous des informaticiens et geek qui savent nous aider à exercer votre contrôle parental. Bien sûr la partie ne sera jamais définitivement gagnée : si vous revoyez les « petits yeux du matin » revenir c'est que votre petit génie aura trouver comment réactiver son smartphone la nuit. A vous de faire attention à ces signes… et de revoir vos amies "digital mum" ou "supergeek". Au fait, savez-vous que vos enfants – ils ne vous le diront pas - ne sont pas si hostiles à votre « protection numérique », ne serait-ce que parce que vous vous interessez à eux !

Acte III – Epuisement, isolement, sexualité, harcèlement, addiction : dialoguez avec eux ou ceux qui peuvent vous aider !

Par exemple seulement 10 % parlent à leurs parents de leur cyber-harcèlement ! Près d'un enfant sur deux a déjà été victime de cyberagresion ! Selon Catherine Blaya* : 41 % de cyberviolences et 7 % de cyberharcèlement. Se faire aider ? Ex. E-Enfance : https://www.e-enfance.org/

net écoute
0800 200 000
Appels & services gratuits

Hyperconnexion : 3 premiers conseils

1) *Donnez l'exemple quant aux bonnes temporalités : préservez à minima le dîner sans smartphone !*
2) *Tenez-vous informer des dérives possibles et de la manière de les gérer : vous savez faire ou avez tous dans vos entourages des geeks qui vous aideront*
3) *Dialoguez avec votre enfant sur 3 sujets à risques : harcèlement, sexualité, contacts à risques (groupes, sectes, copains borderline, défits dangereux…)*

Cyber-harcèlement : comment réagir ?

- ***Ne jamais tenter de résoudre le problème en contactant les harceleurs***
- *Parler avec votre enfant*
- *Rassembler les preuves (ex. captures d'écran)*
- *. Supprimer/signalez les contenus en ligne*
- *Faire un signalement ou porter plainte si nécessaire*

Télécharger le guide

Réduire les risques personnels, collectifs et sociétaux

En entreprise ou dans une organisation, vous l'avez bien compris le facteur humain est déterminant. Mais l'éducation à la sécurité numérique passe d'abord par une vision exhaustive des risques et une approche à 3 dimensions (personne – processus – technologie).

Quelques risques

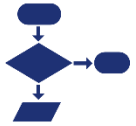
1) *Risques techniques : virus, piratage (Douzé et Héon, 2013), arnaques…*
2) *Risques socio-économiques : fractures liées aux inégalités d'accès ou de compétences (Plantard, 2011)*
3) *Risques cognitifs : perturbation des capacités d'attention (Hayles, 2016), appauvrissement des pratiques de lecture ou de la pensée (Amadieu et Tricot, 2014)*
4) *Risques psycho-sociaux : exposition à des contenus choquants, addiction (Stiegler et Tisseron, 2010, Jehel, 2015), harcèlement en ligne (Blaya, 2013)*
5) *Risques informationnels : enfermement dans des «bulles de filtres» (Pariser, 2011), capacité à évaluer l'information (Serres, 2012), et manipulations politiques notamment face aux « théories du complot » (Bronner, 2013)*
6) *Risques éthiques : protection des données personnelles, e-réputation et respect d'autrui dans sa vie privée (Cardon, 2015, Merzeau, 2013, Rouvroy, 2014)*
7) *Risques juridiques : violations des droits (d'auteur, de l'image, à l'image…), cybercriminalité*
8) *Risques liés à la santé : postures, troubles oculaires, exposition aux ondes.*

Source : cf. rapport Projet de recherche RISK – Risques numériques et école 2.0

Les personnes

- Prise de conscience, lucidité, s'informer, se former
- Comportements, évaluer l'information
- Confronter les interprétations, distinguer les faits
- …

Les processus



- Gestion du risque
- Gouvernance
- Exercices, amélioration continue
- …

Les technologies

- Efficaces, spécialisées
- Capacité de gestion
- Maintien de la sécurité et mises à jour
- Outils d'aide

Verbatim numérique et sécurité

« La digitalisation ou le numérique, c'est avant tout un changement de culture et une gestion de risques nouveaux. »

« En rentrant des vacances, il a fallu que je traite mes milliers de mails… Je suis déjà surchargé ! »

« Avant de reposer sur la technique ou encore les processus (le « château fort »), détecter l'aiguille dans la botte de foin »

« Big data », la cybersecurité commence par l'humain : culture, comportements,… »

« Ma navigation numérique ressemble à un chemin publicitaire défini par les algorithmes »

« Marcher avec son téléphone dans la main deviendrait-il une mode… »

« Je suis content que nous soyons au restaurant, cela nous permet à chacun de répondre à tous nos mes messages et notifications. Nous échangerons « un peu d'amour copier coller » plus tard. »

« Je n'arrive pas à suivre tout ce que mes amis postent sur les différents réseaux sociaux »

Retrouvez tous les DDD 8 précédents

https://www.federationaddiction.fr/?s=DDD8

. **8 Janvier - Lancement des DDD 8 : c'est la rentrée !**
Livret de lancement : pourquoi les DDD 8" ?

. **8 Février - Découvrir le numérique : journées "sans mobile" (6,7 et 8 février)**
Livret "Découvrir où j'en suis" de mes usages numériques par les autotests

. **8 Mars - Equilibre des temps de vie : Journée Internationale des femmes**
Livret "Comment organiser au travail, en famille ou en association les DDD8

. **8 Avril - Ajuster ses applications et réduire l'infobésité : ménage de printemps !**
Livret "Ménage de printemps numérique"

. **8 Mai – Ensemble déconnecter, se désaddicter : 8 mai jour… de la libération !**

. **8 juin - Qualité de Vie au Travail et personnelle : jour de la 'Méthode" (Descartes)**
La Table des 12 des Temps et des Temporalités liées au numérique

- **8 Juillet - Bonheur, vacances et détox digitale : ressourçons-nous !**

. **8 Août - Droit à la déconnexion : voté le 8/8/2016, en vacances à appliquer !**

. **8 Septembre - Nouvelles bonnes habitudes : c'est la rentrée !**

. **8 Octobre - Sécurité informatique : mois de la cybersécurité**

. **8 Novembre - Prévention Santé : hyperconnexion diabète, AVC, cancers**

. **8 Décembre - Responsabilité Sociétale : ex. Journée mondiale du climat**

Contribution au DDD8 « Sécurité » : Steven Lafosse Marin

Diplômé de l'ISEP, évolue au sein de grands groupes (Vivendi/SFR, Airbus Group), accompagne les dirigeants face aux risques cyber, intervient au sein de think-tanks (globalforum.items-int.com, Entrepreneuriat…)

CEO et co-fondateur d'une startup dans le secteur du **Développement afin de valoriser l'humain,** les écosystèmes et les nouvelles technologies face aux défis humanitaires et environnementaux.

Initiateur des DDD8 : Thierry Le Fur

Expert en comportements numériques & addictifs - Qualité de Vie au Travail lié au digital. Diplômé d'Etudes Supérieures Universitaires de Prise en charges des addictions (Paris VIII) ET Management/ Communication (MBA/IMP-ESG).

Contributeur : Sénat, Assemblée Nationale, France stratégie…

Auteur : Pouce ! Mieux vivre avec le numérique (Préface JP Couteron Pdt Fédération Addiction) **Média** : BFM TV, Allô Docteurs, CNEWS, RTL France Inter, L'OBS (tribunes), LE MONDE… **tlefur@addlib.fr – 06 38 82 87 08 - LinkedIn**