Culture de la sécurité
et expérience des FHO dans les industries à risques

Par Marc-Xavier Joubert, Robert Breedstraet et Stéphane Deharvengt

L'organisation et le déploiement de la cybersécurité sont confrontés aux mêmes problématiques rencontrées au cours des dernières décennies dans les domaines de la sécurité des vols, de la sûreté nucléaire ou encore de la sécurité industrielle. Tous les Responsables de la Sécurité des Systèmes d'Information pourraient témoigner de la difficile évaluation coût-bénéfice de la sécurité, du défi que représente le compromis entre sécurité et disponibilité informatique, mais également de l'importance du fameux « facteur humain » ou de la nécessaire implication du « top management » …

MARC-XAVIER JOUBERT

Président de Suez Advanced Fire Engineering.

ROBERT BREEDSTRAET

Division information security officer. Adjoint au Corporate CISO d'Amadeus IT Group.

STÉPHANE DEHARVENGT

Adjoint chef de mission sécurité, sûreté, qualité du contrôle aérien français. Direction des Services de la Navigation Aérienne. DGAC.

Les professionnels de la sécurité industrielle voient ici un écho aux mêmes défis qu'ils affrontent depuis des dizaines d'année.

Pour dépasser la vision technique et procédurale de la sécurité, l'industrie (aéronautique, ferroviaire, nucléaire, chimique…) a étudié en profondeur les Facteurs Humains et Organisationnels (FHO) et le concept de culture de sécurité nécessaires à l'émergence et au maintien d'un niveau acceptable de sécurité. Quels enseignements pourrait-on donc tirer du management de la sécurité dans ces

industries à risques pour construire des cultures de cybersécurité adaptées aux défis de la métamorphose numérique de nos sociétés ?

Les professionnels de la cybersécurité et leurs managers devraient aller puiser dans cette ressource académique, scientifique et expérimentale pour en dégager les lignes directrices utiles au déploiement efficace de leurs politiques de sécurité et les adapter au contexte particulier de la menace cyber et de sa dimension intentionnelle. Nous ne traiterons pas ici de la manière dont ces industries intègrent les risques cyber. Nous irons plutôt explorer les concepts clefs qui ont permis d'atteindre un haut degré de sécurité de fonctionnement dans ces secteurs, puis nous qualifierons plus précisément la menace cyber et évoquerons les spécificités d'une culture de cybersécurité.

Un regard « Facteurs Humains et Organisationnels » sur la sécurité

« *Les FHO […] doivent aujourd'hui permettre d'élaborer une logique de sécurité, avec des normes bien sûr, mais aussi la prise en compte de la variation des conditions réelles et donc l'existence d'une sécurité gérée, ajustée par l'intelligence des hommes.* » (Amalberti and Boissières 2014).
Les Facteurs Humains et Organisationnels expriment une tension entre deux acteurs de la gestion de la sécurité, les humains et les organisations humaines, qui doivent s'articuler autour d'une stratégie permettant de faire face à la variabilité des processus maitrisés.

Le rôle de l'humain dans la gestion de la sécurité

L'humain intervient partout, qu'il soit acteur de première ligne (pilote ou manipulateur) ou acteur de l'entreprise (compagnie aérienne, site industriel, concepteur…). L'entreprise est une organisation humaine faite de processus managériaux et industriels, d'outils technologiques plus ou moins complexes et d'acteurs avec leurs compétences respectives. On retrouve bien sûr en cybersécurité les mêmes composantes procédurales (méthode AGILE, règles de codage…), technologiques (software et hardware) et humaines (développeur, concepteur, pentesteur…).

La question de l'erreur humaine est indissociable de l'histoire de la sécurité dans les industries à risques. Pour de multiples raisons - biais d'attribution rétrospectif, recherche d'un coupable - l'humain garde souvent le mauvais rôle dans les récits d'accidents alors que la plupart du temps, il est le facteur de sécurisation et de rattrapage qui rend ces systèmes techniques aussi sûrs. L'erreur peut être vue soit comme la cause d'un problème, soit comme le symptôme d'un souci plus profond (Dekker 2000). On retrouve également cette vision dans le domaine de la cybersécurité.

Afin de dépasser ce vieux débat, il faut prendre de la hauteur et s'interroger sur les mécanismes qui créent la sécurité ou la cybersécurité.

Les compromis des stratégies de sécurité

La tension entre humain et organisation se traduit concrètement par deux manières de gérer la sécurité, complémentaires et interdépendantes (Groupe de travail de l'Icsi « Culture de sécurité » 2017).

La « Sécurité Gérée » repose sur la compétence des acteurs, cette compétence étant un facteur de résilience du fait de leur forte adaptabilité. On a pu en voir un exemple très récent dans la crise sanitaire de 2020 lorsque les soignants ont réorganisé des services entiers des hôpitaux. Cependant le niveau de sécurité obtenu est peu élevé, puisqu'il s'agit de réagir dans l'urgence, sans plan bien préparé.

La « Sécurité Réglée » repose sur la prévision et le management des situations à risques, voire à les éviter si les conditions de sécurité ne sont pas remplies : un pilote peut décider de ne pas décoller ou d'aller atterrir ailleurs si les conditions techniques ou météorologiques ne rentrent pas dans des limites acceptables. Le système est très robuste mais il est peu adaptatif en cas de choc imprévisible : il s'arrête dans ce cas. Il en résulte un très haut niveau de sécurité – on les appelle de systèmes ultra-sûrs (nucléaire, aviation civile).

Chaque domaine possède ainsi ses stratégies, ses palettes d'actions, qui résultent de compromis stratégiques, de nature économique, de niveau de sécurité, et d'acceptabilité sociale. (Amalberti 2013). En fonction des domaines dans lesquelles elle va s'appliquer, la cybersécurité repose sur des choix plus ou moins explicites en fonction des stratégies de l'entreprise : c'est la logique portée en particulier par la Loi de Programmation Militaire sur la protection des Opérateurs d'Importance Vitale de certaines industries (avec en deuxième rideau des opérateurs de services essentiels), en leur demandant l'identification de leurs systèmes d'importance vitale (tous les systèmes ne concourent pas aux fonctions essentielles) puis en leur appliquant des règles de sécurisation au niveau adéquat.

Mais alors, comment qualifier la sécurité

ou la cybersécurité d'un système ?

Qu'est-ce qu'être sûr ou en (cyber) sécurité ?

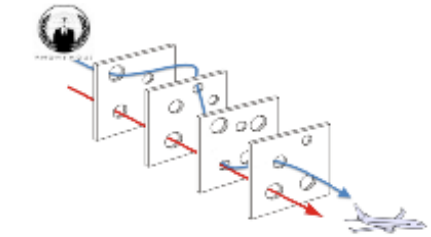
En écho à cette dualité sécurité gérée et sécurité réglée, l'état de sécurité peut être envisagé sous deux angles : statique et dynamique. Sous l'angle statique, la sécurité est comme un stock qui se caractérise par l'absence d'accident. Elle est un fait objectif constaté par des experts qui analysent la situation de façon rétrospective (« jusqu'à présent tout va bien »). L'effet pervers de cette approche est qu'elle peut conduire à rechercher l'élimination des imprévus (réduction de la probabilité des événements redoutés), à considérer l'homme comme le maillon faible faisant des erreurs et, *in fine*, à renforcer la bureaucratie. Sous l'angle dynamique, la sécurité est un processus et se caractérise par la somme des accidents évités. Il s'agit d'une construction permanente qui se traduit davantage par un ressenti de sécurité. Dans ce cadre, la sécurité est orientée pour que l'organisation soit capable de faire face à l'imprévu, en s'appuyant sur les hommes comme ressource pour rattraper les variabilités du système et du contexte. Il serait toutefois vain d'opposer ces deux visions qui, au contraire, doivent dialoguer au sein de l'organisation. En médecine, la santé est une propriété émergente, qualifiée par différents signes physiologiques et indicateurs relatifs à la qualité de vie. Dans les processus industriels, la sécurité est également mesurée par divers indicateurs et constats (Reason 1995). La cybersécurité en tant qu'état du système d'information que l'on peut caractériser et mesurer est donc également une propriété émergente de l'interaction entre les acteurs, les processus et les techniques.

Ainsi, la cybersécurité serait un état du système sociotechnique : on « est en cybersécurité », c'est-à-dire que l'on a mis toutes les barrières humaines et techniques nécessaires pour s'assurer que les dangers sont maîtrisés à un niveau acceptable, dépendant de compromis stratégiques sociotechniques.

Cette notion de maîtrise demande à être explicitée. Dans le cadre des systèmes de management, il est demandé de se donner des objectifs de sécurité, d'identifier les dangers et les manières de les maîtriser ou de les atténuer, puis d'effectuer le suivi de la performance en analysant les accidents ou incidents et d'améliorer le système si besoin (Paries, Macchi et al. 2018). La partie la plus difficile concerne souvent l'identification des dangers ou des menaces sur le système : on ne peut évidemment pas tout prévoir, en particulier dans le domaine cyber où la menace revêt des caractéristiques singulières.

La nature particulière de la menace cyber

Cependant, la cybersécurité introduit la gestion d'un processus particulier qui est celui de la protection contre une attaque, avec en arrière-plan une intentionnalité malveillante, celle de l'attaquant. Cette dimension demande une réflexion dépassant



les cas classiques de gestion de probabilité de pannes ou de dégradation des conditions opérationnelles.

Les trous du cyber-gruyère

Les industries à risques tentent de maitriser les vulnérabilités (les trous) dans les différentes barrières de protection mises en place (règlements, formations, conception, procédures…). En évitant qu'une succession de problèmes survienne, on casse la chaine accidentelle. C'est le principe du modèle de Reason (Swiss Cheese). (Reason 1997).

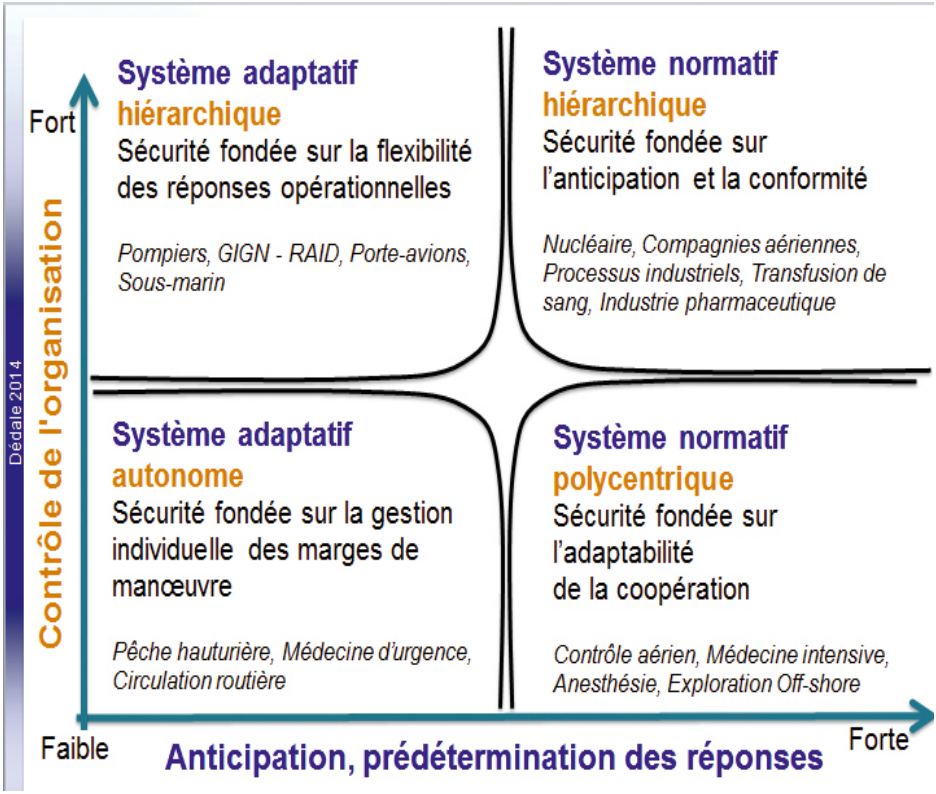
Lors d'une attaque de type cyber, l'attaquant, doué d'une intelligence, va tenter de créer des trous dans les défenses ou d'exploiter ceux qui existent déjà pour tracer son chemin d'attaque. La différence réside ici dans l'intentionnalité de la menace.

Dans les analyses de risques (sécurité industrielle ou sécurité des biens et des personnes), l'intention des intervenants est d'éviter l'accident pour mener à bien la mission, c'est-à-dire produire avec un niveau de qualité déterminé ou amener des passagers d'un point A à un point B en toute sécurité. Sur ce chemin, des erreurs, des omissions peuvent se produire, parfois même des violations de procédure mais l'intention est de bien faire son travail. Sauf si on est un terroriste, on ne se lève pas le matin en se disant qu'on va provoquer un accident industriel.

Dans un contexte de cybersécurité, on assiste à l'affrontement entre deux intentions, l'une en charge du fonctionnement du Système d'Information, parfois génératrice d'erreur ou d'incidents, l'autre animée d'une intention malveillante, cherchant parfois à provoquer l'accident redouté ou, tout au moins, à profondément perturber le fonctionnement normal.

Des menaces et des organisations

En fonction de la précision de la connaissance de la menace, les industries à risques ont développé des modes de gestion de la sécurité adaptés. Le schéma suivant présente sur l'axe horizontal la connaissance formelle des situations à risques, l'axe vertical les capacités de contrôle des organisations



opérant dans ces situations. Plusieurs exemples illustrent ces concepts.

Quel positionnement de la Cybersécurité ?

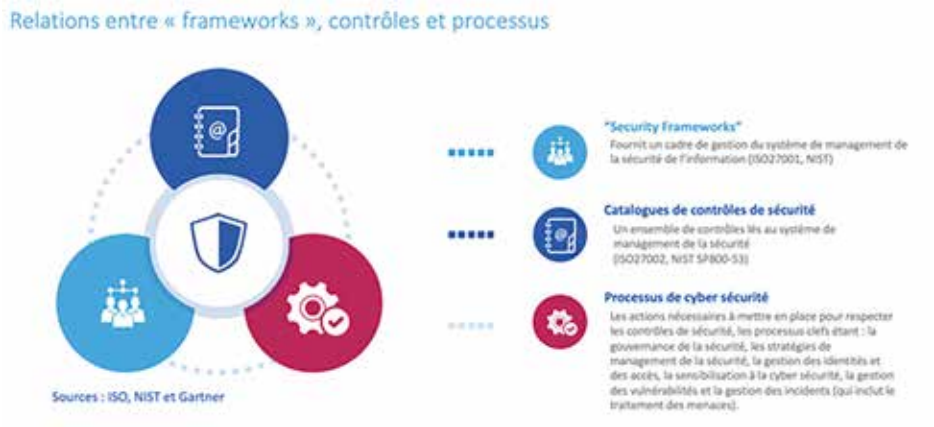
Il existe de nombreuses motivations à construire un système intégré de management de la cybersécurité.

D'abord, cela permet de sauver du temps et de l'énergie. On bénéficie ainsi de l'expérience et des leçons apprises par les autres entreprises, en construisant un langage et une terminologie communs.

Pour des raisons de responsabilité, de visibilité et de conformité, on peut ainsi prouver que la cybersécurité est rigoureusement gérée et on peut fournir

les indicateurs qui le prouvent. On utilise des composants renouvelables : des stratégies, des standards de sécurité et des objectifs de cybersécurité communs à toutes les strates de l'entreprise. Cela garantit des processus de cybersécurité stables basés sur des méthodologies établies. Tout cela permet de bâtir une défense en profondeur et de faire travailler tout l'écosystème de l'entreprise à l'amélioration constante de la cybersécurité.

Un système intégré de management de la sécurité permet de relier le cadre stratégique de la cybersécurité, les catalogues des contrôles et le bon fonctionnement des processus critiques de cybersécurité, c'est-à-dire :



la gouvernance, la gestion des règles (« policies management »), l'information et la formation à la cybersécurité, le management des vulnérabilités, le management des identités et de leurs accès ainsi que la gestion des incidents.

Il est évident qu'une gestion rigoureuse de ces processus est une manière fiable de réduire les risques liés à la digitalisation des entreprises tout en s'assurant que l'humain œuvrera à plus de sécurité et cela grâce aux contrôles mis en place.

Ces aspects sont familiers aux RSSI qui déploient ces structures au sein de leurs entreprises afin de remplir leur rôle de détection, de réaction, et in fine de protection des systèmes d'information. On retrouve ainsi les mêmes composantes organisationnelles et techniques qui fondent la stratégie de sécurité des systèmes à risques. Sur ces points, les organisations devraient s'inspirer des acteurs plus avancés tel que le secteur bancaire, déjà très expérimenté en matière de sécurisation des transactions financières.

Cependant, la composante essentielle sera toujours la partie humaine du système sociotechnique que l'on abordera sous l'angle de la culture de cybersécurité.

Construire la culture de cybersécurité

"*Few things are so sought after and yet so little understood.*"(Reason 1997). La culture de sécurité est un concept scientifique difficile à appréhender. Mais elle peut se construire en cybersécurité de la même manière que dans la sécurité industrielle.

Il faut pour la cybersécurité un complet changement de paradigme. Tant qu'elle sera vue comme un simple problème que des techniciens peuvent solutionner avec des outils techniques, on n'arrivera pas à construire une culture de la cybersécurité digne de ce nom. Construire cette culture est très probablement le plus grand changement des entreprises pour la prochaine décennie. Il est nécessaire d'introduire la cyber au centre même du business.

Sans une intégration poussée par le sommet de la hiérarchie et avec tout le soutien des comités exécutifs, un tel changement ne sera pas possible. Nos dirigeants doivent prendre la responsabilité de comprendre et d'adapter la culture de leur entreprise afin d'y inclure de bon niveau de reflexes de cybersécurité. La mise en place d'une stratégie et d'un cadre sécuritaire (ISO27K ou NIST) en sera la conséquence logique.

L'Institut pour une Culture de Sécurité Industrielle (ICSI) a défini les 7 attributs d'une culture de sécurité intégrée. Comme nous pouvons le voir ci-dessous, ceux-ci sont facilement transposables dans un contexte cybersécurité :

1. Conscience partagée des risques les plus importants,
2. Culture interrogative,
3. Culture intégrée, mobilisation de tous,
4. Équilibre pertinent entre le réglé et le géré,
5. Attention permanente aux trois piliers (technique, système de management, FHO),
6. Leadership du management et implication des salariés,
7. Culture de la transparence afin de générer la confiance.

Bien qu'il nous paraisse évident de cultiver la transparence et de partager les renseignements que nous possédons, il est encore difficile pour une entreprise d'admettre qu'elle a subi une attaque cyber ou bien d'évoquer ses vulnérabilités.

Il est donc délicat d'instituer cette culture

de la transparence mais nous pouvons et devons faciliter le partage des informations et des renseignements. De nombreux forums ont déjà été ou sont en train d'être mis en place pour ce faire : les États européens à travers leurs agences de sécurité informatique mettent en place des réseaux de CERT (« Computer Emergency Response Team ») qui œuvrent en ce sens, des regroupements sectoriels se sont créés, notamment aux États-Unis. Ils permettent de partager les indices de compromission et aident ainsi collectivement à améliorer le niveau de protection de ceux qui acceptent ce partage et donc ce niveau de transparence.

On apprend de nos erreurs : pour anticiper, pour améliorer les connaissances sur la menace, pour développer des procédures robustes. Au niveau d'une entreprise, il faut donc connaître la vie de tous les jours et les différences entre ce qui est prescrit et ce qui réellement réalisé. Les acteurs de terrain doivent avoir suffisamment confiance pour reporter les événements sans craindre de sanction en retour.

Toutefois, l'idée de sanction, déjà délicate dans le domaine de la sécurité industrielle, paraît encore plus difficile en contexte cyber : comment distinguer l'erreur de la faute, face à une menace qu'on ne comprend pas ou que l'on n'a pas détectée ?

Lors de la conception de la formation à la culture sécurité délivrée en 2020 à l'ensemble des agents du contrôle aérien français, la mention du signalement d'évènement à caractère cyber a été mentionnée. Même si la notion de signalement d'événement sécurité est très ancienne et ancrée dans les mœurs, tout particulièrement chez les contrôleurs aériens, la modernisation croissante des systèmes de navigation aérienne nécessite d'étendre cette culture du report. Celle-ci permet également de toucher les acteurs « non-opérationnels ».

Se préparer à la crise : résilience et construction du sens

La menace cyber fait peser un risque bien plus grand (tant en probabilité qu'en étendue) de crises majeures touchant l'ensemble d'une organisation. Les attributs clefs de cette culture de sécurité doivent donc être complétés par une meilleure préparation à la crise afin de rendre les organisations plus résilientes.

D'après Erik Hollnagel (Hollnagel, Pariès et al. 2010), une organisation résiliente arrive à maintenir en permanence la situation sous contrôle, qu'elle soit prévue ou imprévue. Cela revient à s'interroger en permanence autour de deux questions fondamentales : Qu'est ce qui fait perdre le contrôle ? Comment maintenir ou regagner le contrôle ? Il définit ainsi quatre attitudes clés qui doivent être entretenues dans les organisations et qui font échos aux concepts abordés précédemment :

1. Apprentissage : connaitre le passé (faits

objectifs et structurés) diffusé au travers d'un REX (Retour d'expérience) analysé et partagé ;

2. Réponse : savoir quoi faire et savoir le faire, notamment par des procédures réellement opérationnelles et connues ;

3. Monitoring : savoir quoi chercher (ce qui est critique) et le mesurer par des indicateurs prospectifs ;

4. Anticipation : savoir à quoi s'attendre (potentiels et scénarios) y compris l'impensable.

En complément, Karl Weick (Vidaillet 2003), au travers de l'analyse de la catastrophe de Mann Gulch nous éclaire sur quatre dimensions de la souplesse organisationnelle qui augmentent la résilience :

1. La capacité à improviser et à bricoler de nouvelles solutions, même sous la pression. Ceci sous-entend l'entretien d'une forme de créativité et de capacité d'initiative en dehors des phases de crise,

2. Un système de rôles à tenir, partagé entre les acteurs de l'organisation, qui permet à chacun de savoir quels rôles doivent être tenus en toutes circonstances (exemple : le chef, le secrétaire, le communicant…), même lorsqu'on est seul,

3. Une attitude de sagesse, comprise comme la capacité à prendre en permanence de la distance vis-à-vis de ses croyances, de ses certitudes et de sa propre confiance,

4. L'entretien de relations respectueuses entre les acteurs qui permettent d'être à l'écoute de solutions nouvelles, d'accepter en confiance la répartition des rôles.

Conclusion

Sans vouloir imposer un point de vue extérieur, la communauté cyber pourrait bénéficier d'un échange approfondi avec la communauté de la sécurité industrielle. D'un côté, ce que les sciences sociales dans les industries à risque nous disent : reconsidérer l'humain comme un élément de sécurisation du système et d'adaptation aux imprévus, des choix stratégiques et tactiques portant sur les caractéristiques des défenses mises en œuvre. De l'autre, ce que la déclinaison des théories actuelles en sécurité apporte au vu des spécificités des systèmes d'information : une intentionnalité malveillante, les caractéristiques de la résilience organisationnelle en réponse à une cyberattaque. Cet échange pourrait se concrétiser par le déploiement d'une culture de cybersécurité maîtrisée permettant d'atteindre un état de cybersécurité acceptable. En particulier, la transparence dans le report d'événement et le partage d'information suite à une analyse, valeur primordiale pour la culture sécurité,

devraient pouvoir trouver son expression dans une culture de cybersécurité.

Ce cheminement demande des efforts de la part des décideurs pour prendre en compte une réalité qui est loin d'être simple mais que ces connaissances et pratiques permettent d'éclairer. Cette dimension des enjeux de la transformation numérique ne doit pas être sous-estimée, en particulier si l'on veut responsabiliser les acteurs de terrains, adapter les espaces de travail, et construire la confiance qui sous-tend toute transformation. Quant au chemin de croix des RSSI, qu'il s'agisse de ressources, de budget, de compétences, d'arbitrages, de responsabilités, d'accès aux décideurs, il n'est pas sans rappeler celui du Directeur Sécurité. La prévention a souvent le mauvais rôle par rapport aux enjeux opérationnels immédiats, mais elle sera toujours plus payante qu'un accident ou une crise cyber majeure qui paralysera l'entreprise et affectera durablement son image.

Bibliographie

Amalberti, R., Ed. (2013). Navigating Safety, Necessary compromises and tradeoffs, Theory and Practice. Berlin, Springer.

Amalberti, R. (2017). « Les FHO dans l'entreprise : trois rails éclatés ? » Tribunes de la Sécurité Industrielle 1: 5.

Amalberti, R. and I. Boissières (2014). Interviews croisées. 6ème assises nationales des risques technologiques - Le Journal.

Dekker, S. W. A. (2000). The Field Guide to Human Error, Ashgate.

Groupe de travail de l'Icsi « Culture de sécurité » (2017). La culture de sécurité. Comprendre pour agir. Cahiers de la Sécurité Industrielle. D. Besnard, I. Boissières, F. Daniellou and J. Villena. Toulouse, France, Institut pour une Culture de Sécurité Industrielle. Numéro 2017-01.

Hollnagel, E., J. Pariès, et al. (2010). Resilience Engineering in Practice: A Guidebook, Ashgate Publishing, Ltd.

Paries, J., L. Macchi, et al. (2018). « Comparing HROs and RE in the light of safety management systems.» Safety Science.

Reason, J. (1995). « Safety in the operating theatre. Part 2: Human error and organisational failure. » Current Anaesthesia and Critical Care 6(2): 121-126.

Reason, J. (1997). Managing the risks of organizational accidents. Aldershot, UK.

Vidaillet, B. (2003). Le sens de l'action : Karl E. Weick, sociopsychologie de l'organisation / [F. Allard-Poesi, G. Koenig, H. Laroche, C. Roux-Dufort], Vuibert.

AUTEUR

Marc-Xavier Joubert – Président de Suez Advanced Fire Engineering
Au sein de SUEZ, Marc-Xavier Joubert dirige une start-up innovante pour développer des solutions environnementales pour lutter contre les incendies.
Après avoir servi au sein de l'Aviation Légère de l'Armée de Terre, il a rejoint SUEZ où il a acquis une expertise dans la gestion des risques environnementaux et industriels dans leurs dimensions techniques, humaines et organisationnelles.
Il était précédemment directeur de la performance et des risques industriels du Groupe SUEZ.
Il est également membre de la commission scientifique risques accidentels de l'INERIS. Diplômé de l'Ecole Spéciale Militaire de Saint-Cyr et d'un Master Spécialisé en Facteurs Humains et Organisation de l'ESCP Europe, il est auditeur IHEDN – INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

AUTEUR

Robert Breedstraet - Division information security officer, adjoint au Corporate CISO d'Amadeus IT Group.
Robert Breedstraet dirige le département gouvernance et contrôle, le management de projets de cyber sécurité comme la gestion des identités et des accès, la protection de la marque Amadeus.
Il a aussi sous son autorité les responsables régionaux de sécurité informatique (Amériques, Inde, Asie-Pacifique, Europe et Moyen Orient).
Robert a une expérience de plusieurs dizaines d'années en informatique et en particulier dans le domaine de la réservation aérienne.
Il est également représentant d'Amadeus dans différents groupes internationaux, informaticien et titulaire d'une maîtrise en politique économique, il est auditeur IHEDN – INHESJ de la première session nationale Souveraineté Numérique et Cyber-sécurité.

AUTEUR

Stéphane Deharvengt – adjoint chef de mission sécurité, sûreté, qualité du contrôle aérien français à la Direction des Services de la Navigation Aérienne - DGAC

Stéphane Deharvengt dirige l'équipe en charge du Système de Management de la DSNA (Contrôle aérien français) dans ses composantes Sécurité, Sûreté (physique et cybersécurité) et Qualité. Son expertise est issue des travaux qu'il a mené dans la conception et l'application de stratégies complexes de maitrise de la sécurité des vols et du contrôle aérien : Règlements opérationnels (retour d'expérience, systèmes de management, gestion de la fatigue) et de certification avion (conception cockpit et cabine, A380), Gestion des risques sécurité et cyber, Formations facteurs humains, nombreux programmes de recherche appliquée à la sécurité aérienne.
Il est également représentant français dans différents groupes internationaux. Ingénieur aviation civile de formation, il est titulaire d'un doctorat en ergonomie et auditeur IHEDN – INHESJ de la première session Souveraineté Numérique et Cybersécurité.