Sécurisation empirique de la sécurité

iro@cryptosec.org | @secucrypt

Mémoire soutenu à l'ESCP Paris le 27 janvier 2017

Introduction

La présente étude vise à établir une méthode permettant de fiabiliser les décisions dans le domaine de la sécurité. Nous commencerons par définir les concepts et pratiques que nous étudions, puis nous soulignerons l'importance du hasard et de l'imprévu lorsqu'il est question de risques, dont il découle une grande difficulté, ou impossibilité, à établir des méthodes déterministes. De plus, nos limitations humaines, individuelles et collectives, entraînent une grande incertitude en matière de prise de décision dans le domaine de la sécurité. En particulier du fait de biais psychologiques, affectifs, organisationnels. Dès lors, pour fiabiliser ces processus, nous verrons qu'une analogie s'avérera particulièrement intéressante : comment les développeurs d'applications peuvent éviter les vulnérabilités les pires et les plus courantes ? Nous choisirons ensuite trois domaines d'application, l'évaluation des risques, la mise en place de mesures de sécurité et la prise de décision en situation de crise. Dans ces trois domaines, nous citerons des problèmes concrets observés dans une grande organisation. Puis nous listerons des facteurs de risques humains typiques qui peuvent défavorablement orienter les décisions sécurité. Pour chacun de ces facteurs, nous en déduirons des questions opérationnelles permettant de les révéler. Enfin, nous confronterons ces questionnaires avec la liste des problèmes observés afin d'en vérifier la pertinence, et nous verrons en quoi la méthode que nous proposons est un bon outil d'aide à la non prise de mauvaises décisions sécurité.

La sécurité

Risques, menaces, sécurité sont des concepts polysémiques, très chargés symboliquement et désignant une multitude de notions particulières et différentes. Ajoutons que l'époque influe significativement sur ce que signifient les mots, et que notre début de XXIe siècle raffole de la

sécurité. Exemple de la cacophonie conceptuelle qui la caractérise, et des errements absurdes d'une certaine pensée sécuritaire, elle va parfois jusqu'à être qualifiée de « première des libertés ». Il importe donc de commencer par bien nommer les choses dont nous allons parler. Cela ne retirera pas du malheur au monde ; mais au moins cela nous aidera à mieux penser.

La sécurité est une situation objective caractérisée par la seule présence de risques maitrisés. En principe la *sécurité* est relative aux risques accidentels (résultant éventuellement d'actions humaines involontaires), tandis que la *sûreté* traite des actes malveillants. Néanmoins, dans la présente étude, nous utiliserons le terme « sécurité » pour désigner les deux concepts.

Les risques, eux, sont des contingences indésirables qui peuvent être avérées, potentielles ou futures. Ils découlent d'une probabilité qu'une menace exploite, intentionnellement ou non, une vulnérabilité.

Si l'on admet avec Spinoza que toute chose, en particulier un individu ou une organisation, s'efforce de persévérer dans son être, on en déduit qu'elle va chercher à minimiser les contingences adverses. C'est-à-dire qu'elle va essayer d'évoluer, dans l'espace et le temps, entre des états où elle maitrise les risques qui la menacent.

Ce que l'on voit ici, c'est que la sécurité, élément essentiel de l'existence, résulte d'une dynamique de maitrise. Pour *être*, toute chose tente de gérer les risques qui pèsent sur elle, qu'ils soient endogènes ou exogènes.

Il y a quatre façons de traiter un risque unitaire : tenter de le réduire, l'accepter, le refuser ou le transférer. Réduire un risque consiste soit à diminuer la probabilité que se matérialise une menace, soit à réduire son impact, ses conséquences, s'il se réalise. L'accepter consiste à considérer que l'effet indésirable du risque, qu'il soit faible ou létal, est acceptable en regard des enjeux, des objectifs, du désir ou des obligations de l'individu ou de l'organisation. Refuser un risque signifie modifier sa propre essence, ce que l'on est ou ce que l'on fait afin de se soustraire à des vulnérabilités. Cela revient à ne pas réaliser une action ou amputer une fonctionnalité. Enfin, transférer un risque consiste à le faire peser sur un tiers, que ce déplacement soit consenti ou non.

Il convient également de préciser que la sécurité résulte toujours d'une dynamique, même lorsque le système à sécuriser est parfaitement statique et n'évolue pas. D'une part parce que les menaces exogènes, elles, peuvent évoluer, et d'autre part parce que la réaction, la diminution des impacts d'un incident, sera nécessairement toujours dynamique.

De cette caractéristique dynamique on peut enfin déduire que la sécurité relève toujours de *processus* impliquant l'individu ou l'organisation, jamais uniquement d'une méthodologie, d'un système, d'une expertise ou d'un produit.

L'imprévu, facteur essentiel de la sécurité

Ces considérations permettent de mettre en lumière un élément essentiel et constitutif des risques et de la sécurité, l'imprévu. Par définition, les contingences indésirables que sont les risques ne sont pas déterministes. S'ils le sont, alors il s'agit de contraintes. C'est-à-dire qu'au cœur de toute action et de

toute réflexion autour de la sécurité se niche l'incertain à venir, l'indéterminé, le hasard, la probabilité. Autant de termes qui qualifient notre impossibilité fondamentale à prévoir l'avenir.

De là découle une différence structurelle entre une démarche de sécurisation et toute autre démarche : on ne peut s'enraciner sur aucune méthode déterministe. Il y a bien sûr de nombreux domaines où les aléas peuvent perturber les modèles théoriques utilisés. Prenons par exemple l'envoi d'une sonde sur Mars. De nombreux aléas peuvent faire échouer une telle mission. Néanmoins, la construction et l'envoi d'une telle sonde se font selon des modèles déterministes. C'est-à-dire qu'aux erreurs et manques d'informations près, et sans considérer les dimensions sécuritaires, la réalisation peut être parfaitement maitrisée. En théorie, un modèle peut être établi et sa stricte application peut être parfaitement prévisible. La situation est intrinsèquement différente dans une démarche de sécurisation. La connaissance des menaces est nécessairement parcellaire ; l'évaluation de la probabilité des risques est toujours, au mieux statistique, au pire qualitative, mais jamais certaine ; l'estimation des impacts d'un incident comporte une part importante d'imprévisible, d'aléas.

En reprenant l'illustration de la sonde martienne : nous savons manufacturer une sonde, nous en maitrisons les techniques ; nous savons comment lancer une fusée en orbite, et envoyer sa charge vers une autre planète ; nous savons calculer son mouvement dans l'espace ; nous savons prévoir où elle devra atterrir, et comment ralentir sa descente dans la ténue atmosphère martienne. Bien sûr, il y a des aléas, des techniques plus ou moins maitrisées, il arrive donc que la sonde s'écrase au sol. Mais nous avions le modèle pour la faire arriver saine et sauve. À l'inverse, si on considère la sécurisation de cette sonde, la modélisation est très difficile : pour la protéger des malveillances sur son lieu de fabrication, nous ne connaissons pas bien quelles sont les menaces qui pèsent sur elle (malveillance d'un ingénieur dépressif ? Terrorisme ? Espionnage ?) ; pour sécuriser le lancement en orbite, nous ne pouvons qu'essayer d'éviter ce qui, par le passé, a causé des accidents ; pour sécuriser son *amarsissage*, nous n'avons que peu d'expérience, beaucoup d'hypothèses.

Comme nous l'avons évoqué, la frontière entre risques et contraintes est poreuse : un risque bien connu, soit parce qu'il a été modélisé de façon efficace, soit parce que nous disposons de statistiques suffisamment fiables, peut cesser d'être un risque et devenir une contrainte, un élément connu que l'on sait parfaitement appréhender.

Mais concernant les risques que tout être tente de maitriser, étant donné que les contingences indésirables contiennent une importante dimension d'aléas, les modèles déterministes n'existent pas.

Ainsi, nombre d'experts et d'équipes sécurité travaillent presque en aveugle, cherchant en particulier à empêcher le syndrome du « cygne noir » (cf. la « théorie » du *cygne noir*, métaphore décrivant un événement imprévisible de faible probabilité d'occurrence, mais qui, s'il se réalise, a des conséquences d'une portée exceptionnelle).

Permettre versus empêcher

La plupart des actions humaines consistent à rendre des choses possibles, à créer des objets qui existeront ou des processus qui auront des résultats prévisibles. Gérer la sécurité est essentiellement différent. Cela consiste à créer des choses et mettre en œuvre des processus dont l'objectif est que

certaines choses n'arrivent pas (la matérialisation des menaces) ou, si elles adviennent, qu'elles aient le minimum d'impact défavorable. Le champ des possibles dans une démarche de réalisation d'un objectif (pourvu qu'il soit atteignable) est plus faible que celui des facteurs pouvant empêcher ou entraver la réalisation de cet objectif. Or la sécurité traite de ce second spectre des possibles.

On voit donc que, du fait de l'imprévu qui rend la modélisation de la sécurité très difficile, et de l'ordre de grandeur incommensurablement plus grand des causes adverses comparées aux causes favorables, une conception mécaniste (c'est-à-dire un ensemble modélisé de causes et de conséquences connues) de la sécurité est nécessairement limitée.

Dans la plupart des cas, les choix en matière de sécurisation reposent sur trois substituts dont la fiabilité est médiocre et incertaine : l'avis d'experts, le lobbying des fournisseurs de solutions, le *benchmarking*, c'est-à-dire la comparaison avec d'autres organisations similaires.

Dès lors, comment fiabiliser les décisions ? Comment évaluer des risques ? Comment prendre des décisions concernant les risques ? Comment réduire les risques pesant sur un système complexe à un cout raisonnable ? Comment décider s'il convient de les réduire ou de les éviter ? Comment organiser la réaction suite à la matérialisation d'un risque ?

Un périmètre, la décision

L'impossibilité ou la difficulté à établir des modèles déterministes pour gérer les risques rend cette activité très dépendante des choix humains.

Or la rationalité de la pensée humaine et des comportements collectifs sont limités et il n'en existe pas de modèle non plus. Mais la psychologie, les études sur le management et les organisations, l'étude de cas d'incidents, d'attaques, de catastrophes et de la façon dont les humains y ont réagi ont produit une quantité importante de littérature sur le sujet. Des problèmes typiques, des biais connus et des comportements problématiques peuvent être décrits, qu'ils concernent les individus ou les organisations.

Nous sommes donc dans la situation où nous avons à traiter des phénomènes peu ou pas modélisés, à l'aide nos cerveaux et de nos collectifs dont le fonctionnement est souvent erratique. En un mot comme en cent : nous commettons souvent beaucoup d'erreurs à l'heure de choisir, de déterminer, de décider concernant la sécurité et les risques.

Dans le cadre de la présente étude, nous nous concentrerons donc sur une dimension : les prises de décisions relatives aux risques, qu'ils soient faits par des individus ou des organisations.

En l'absence de modèle satisfaisant, et face à l'immense difficulté – voire impossibilité – d'en établir, l'analogie est en général la méthode la plus fructueuse.

Une analogie fructueuse

Ces dernières années le domaine de l'informatique a vu se développer exponentiellement les « applications » accessibles par des utilisateurs et rendant d'innombrables services en matière de

traitement de l'information. L'interaction avec des systèmes physiques augmente la présence et démultiplie les usages de ces applications.

Il existe des dizaines de langages informatiques qui permettent de développer des applications, des milliers de configurations matérielles, des centaines de milliers de personnes dans le monde possèdent les compétences pour les développer. La sécurité de ces applications est devenue un enjeu clé. Les résultats de trois ans de tests de sécurité au sein d'une équipe de *pentesters* que nous avons animé montrent que plus de 60% des vulnérabilités découvertes sont des vulnérabilités applicatives (dans le contexte de l'organisation que nous prenons comme sujet d'étude). Il existe des méthodes et des outils d'analyse des codes sources qui permettent de détecter les erreurs de programmation, et donc de limiter les vulnérabilités potentielles. Néanmoins ces analyses sont très couteuses et sont peu efficaces pour déceler les erreurs fonctionnelles (c'est-à-dire les erreurs de spécification).

Au cours des premières années du siècle a vu le jour une communauté, Open Web Application Security Project (OWASP) dont les travaux sont librement accessibles, et dont la vocation est de construire et proposer des recommandations, méthodes et outils de sécurisation des applications web. Le projet qui a rapidement connu un grand succès et est aujourd'hui une référence en matière de sécurité des applications est le « Top Ten OWASP » (cette liste est référencée par nombre de standards de sécurité, comme MITRE, PCI DSS, DISA, FTC, etc.). Il a pour but d'identifier et de lister les dix risques de sécurité applicatifs web les plus critiques.

La particularité de cette liste est qu'elle n'est pas le fruit de « bonnes pratiques » ou d'avis d'experts (comme peuvent l'être les référentiels ISO), mais le résultat de l'analyse de centaines de milliers vulnérabilités effectivement découvertes chez des milliers de clients.

Dans la même logique, le Center for Internet Security publie le CIS Critical Security Controls for Effective Cyber Defense (CIS CSC), liste de vingt recommandations de sécurité minimales à appliquer pour sécuriser un système d'information. S'il s'agit dans ce cas de mesures de sécurité préventives couvrant tout le spectre de la cybersécurité, la conception de cette liste et la priorisation de ses items a suivi le même principe : elle est issue de l'observation d'un panel significatif d'attaques réelles.

Dans les deux cas, ces listes se matérialisent par des *checklists*. Le principe sous-jacent est, dans les deux cas, qu'en l'absence de modèle de sécurité déterministe, un élément clé – mais non suffisant – pour sécuriser une application ou un système d'information est de vérifier que les vulnérabilités les pires et les plus fréquentes sont évitées.

Par analogie, nous allons donc essayer d'établir une liste des erreurs communément commises en matière de prise de décision, puis de l'instancier à quelques domaines de la maitrise des risques.

Les domaines d'application

Nous allons choisir trois activités critiques en matière de gestion des risques au sein d'une organisation :

- L'évaluation des risques ;

- La définition et la mise en place de mesures de sécurité préventives ;

- La prise de décision en gestion de crise.

L'évaluation de risques

Prenons le cas d'une organisation que nous avons eu l'occasion d'observer de l'intérieur. Il s'agit d'une entreprise de taille relativement importante (plusieurs milliers d'employés), dans le secteur tertiaire. Consciente que des menaces significatives pèsent sur son activité, elle a atteint au fil des années une maturité assez importante en matière de maitrise des risques. Nous entendons par là que cette activité est reconnue et financée en interne, que des cadres et des outils existent et que du personnel y travaille quotidiennement. Concrètement, elle s'est dotée d'une méthode d'analyse des risques qui permet d'estimer la criticité de ses activités et biens informationnels (selon trois axes, confidentialité, intégrité, disponibilité) et d'en déduire des mesures de sécurité à déployer en conséquence. Cette méthode est accompagnée d'une méthodologie projet qui impose dans les diverses phases de réalisation d'un projet de dérouler différentes étapes d'analyses de risques. Néanmoins, malgré le cadre, l'expérience et la bonne volonté, des problèmes sont régulièrement constatés.

Citons quelques exemples :

- À l'heure d'estimer la criticité d'une application ou d'une infrastructure, des équipes projet sous-estiment ou surestiment par erreur la criticité de leur application finale. Ces erreurs, toujours humaines, peuvent avoir de multiples causes.

- Parfois, sachant que des mesures de sécurité contraignantes vont en découler, les chefs de projet sous-estiment volontairement la criticité de leur projet.

- La sélection des mesures de sécurité correspondant à la criticité identifiée est automatiquement proposée par l'outil d'analyse des risques, mais une personnalisation au contexte est rarement faite. Cette activité de sélection des mesures peut sembler très rassurante, donnant une illusion de rigueur parce que reposant sur une méthodologie compliquée. Si rassurante que l'on omet de la contextualiser.

- Erreur flagrantes d'appréciation des risques ; il s'agit toujours d'erreurs humaines qui peuvent avoir de multiples causes.

- Des projets échappent à ces analyses de risques, soit parce qu'ils prennent la forme de changements et échappent à la méthodologie projet, soit parce que tout ou partie du projet est réalisé en faisant appel à des services externalisés (ce type de pratiques étant parfois qualifié de *shadow IT*).

- Le suivi et le bilan des risques résiduels sont souvent parcellaires ou omis.

- Comme pour le *shadow IT,* certains changements, étant hors projet, échappent tout à fait aux analyses de risques.

- Le processus d'acceptation formelle des risques résiduels est souvent défaillant. Un « projet » ou un « métier » sont classiquement les porteurs identifiés des risques. Or on constate que les risques sont beaucoup plus facilement acceptés par des services, fonctions ou des collectifs que par des individus nommément identifiés (conjointement à leur fonction).

Dans tous ces exemples, si les problèmes peuvent résulter de lacunes de la méthodologie, ils relèvent surtout d'erreurs d'appréciation et de décisions humaines erronées.

La définition et la mise en place de mesures de sécurité préventives

Au sein de cette même organisation a lieu une constante mise à jour et un renouvellement des outils et processus de sécurité la protégeant. Cela peut se traduire par des aspects documentaires, comme la rédaction de politiques de sécurité pour les composants critiques, par des actions de configuration sur les systèmes afin de les durcir, par le perfectionnement ou la création de processus organisationnels ou encore par l'acquisition de logiciels et matériel apportant de nouvelles fonctionnalités sécurité.

Là encore, des problèmes sont régulièrement constatés, par exemple :

- Grand soin apporté à la rédaction de documents, mais piètre suivi de la mise en œuvre de ce qu'ils recommandent.

- Choix de configurations techniques soit disproportionnées par rapport aux risques, soit inhomogènes, c'est-à-dire laissant des vulnérabilités non couvertes entraînant des situations de risque importantes.

- Choix de produits ou solutions sans analyse contradictoire suffisamment poussée, dont la conséquence est l'acquisition de produits à l'efficacité limitée.

- Acquisition de produits très satisfaisants, mais lacunes majeures dans la mise en place des processus de gestion (organisationnels) de ces produits.

- Mauvaise évaluation de la menace, menant à des choix stratégiques ou tactiques peu pertinents.

- Décisions techniques prises trop rapidement, sur la base de critères contestables.

- Perte de la mémoire de l'entreprise qui peut avoir pour conséquence la répétition d'erreurs très similaires.

- Situations de soumission et de fragilité contractuelle vis-à-vis des fournisseurs, par exemple manque de moyens de pression pour leur faire adopter des mesures de sécurité importantes.

- Il arrive également que la hiérarchie, convaincue par des vendeurs ou des consultants veuille imposer des solutions dont les équipes techniques savent ou anticipent qu'elles ne seront pas efficaces.

La prise de décision en gestion de crise

Enfin, cette organisation doit parfois gérer la conséquence de risques s'étant matérialisés, c'est-à-dire d'incidents ou de crises sécurité. Ici encore, la maturité de cette entreprise l'a dotée de processus de gestion de crise bien établis. Selon la gravité de l'incident, différents types de cellules de crises peuvent être convoquées, dont les caractéristiques sont qu'elles sont prioritaires sur toutes les autres activités et qu'elles réunissent dans une même unité de lieu et de temps les décideurs et les

techniciens. Leur principale raison d'être est de décider d'actions et de mesures de sortie de crise, et de décider de la communication vis-à-vis de l'extérieur. Des décisions peuvent alors être rapidement prises, hors des processus standards, pour parer aux urgences. Au fil des années l'organisation a également appris combien il est essentiel de bien communiquer afin de diminuer l'effet anxiogène sur les employés, clients et utilisateurs. Néanmoins, des dysfonctionnements sont souvent observés dans les gestions de crise, l'effet étant accru du fait de la faible expérience acquise (il y a peu de crises ou incidents majeurs).

Les dysfonctionnements souvent observés sont :

- Organisation prévue pour gérer les crises non appliquée lorsqu'elle arrive, ce dont il résulte une improvisation qui ralentit le retour à la normale.

- Difficultés pour la hiérarchie à prendre du recul vis-à-vis des actions techniques, et difficultés des techniciens à se départir des réflexes du quotidien.

- Les leçons post-incident sont en général bien faites, des actions sont prises et suivies, mais les leçons sur les problèmes de la gestion d'incident elle-même sont rarement formalisées.

- Les rapports de retour d'expérience (REX) sont parfois édulcorés du fait de leur future transmission à la haute hiérarchie.

- Certaines actions devraient parfois être explicitées avec plus de discrétion (par exemple le fait de solliciter un service sécurité pour investiguer sur une malveillance) pour ne pas susciter des rumeurs qui ajoutent au stress collectif.

- Il est arrivé que des actions techniques n'ayant aucune chance de résoudre les problèmes soient tentées en cours de gestion de crise (comme des redémarrages de serveurs), uniquement pour que cela ne puisse pas être reproché ultérieurement (de ne pas l'avoir « tenté »).

- Parfois, il est arrivé que des mesures de sécurité aient empêché d'intervenir rapidement pour gérer un incident majeur ou une crise, et qu'il n'y eût pas de possibilité de les débrayer en cas de situation exceptionnelle.

- Il arrive fréquemment que les cellules de crise, où siègent les décisionnaires, sollicitent trop les techniciens en charge de la résolution de la crise. Il en résulte souvent un stress peu propice au travail efficace. Dans certains cas, on a même pu observer une sorte d'inversion des rôles, c'est-à-dire que les cellules de crises se sont mises à ordonner des actions, au lieu de décider celles que leur proposaient les *sachants* et techniciens.

- Parfois, dans l'urgence de la gestion d'une crise ou d'un incident majeur, des décisions sont prises sur la base de fausses informations ou d'hypothèses erronées qu'il aurait été souvent aisé de disqualifier (souvent, un technicien aurait pu rapidement alerter sur l'erreur). S'il est essentiel de savoir décider sans disposer de toutes les informations, il est tout aussi vital de pouvoir s'appuyer sur quelques certitudes. Dans la plupart des cas c'est l'urgence et l'enthousiasme à l'idée de tenir une piste qui rend aveugle sur la qualité de ces informations.

Facteurs de risques humains pour les décisions sécurité

En nous référant aux travaux dans le domaine du management, de la psychologie, de la théorie des organisations, à notre propre expérience et aux descriptions de crises et catastrophes documentées, nous pouvons établir une liste de facteurs pouvant causer des dysfonctionnements dans la prise de décisions dans le domaine de la sécurité et de la sureté.

Probablement cette liste s'applique-t-elle à bien d'autres domaines, mais nous nous focaliserons sur la sécurité et la sureté.

Rationalité limitée	Les individus et les groupes ont l'intention d'être rationnels, mais en raison de leurs capacités cognitives limitées, ils n'y parviennent que dans une faible mesure. Afin de pallier cette lacune, les organisations pensent souvent rationaliser leurs choix en faisant appel à des chiffres.
Biais de confirmation	Tendance à favoriser l'information connue ou l'idée admise et à ne pas rechercher, à ignorer ou à rejeter les informations et les données qui la contredisent. Nous cherchons à confirmer nos idées, plus qu'à les remettre en question.
Biais de l'*énaction*	Nous construisons nous-mêmes, par nos actions et nos croyances, notre environnement. Nous le « mettons en scène » et avons tendance à considérer comme « vrai » ce qui semble « marcher » dans *notre* représentation du monde (« Je ne vois que ce que je crois »). Mais ce qui « marche » peut être faux, ou seulement partiellement vrai.
Histoires versus statistiques	Nous préférons la cohérence d'une histoire, d'un récit, à la réalité des statistiques (à noter cependant que rien n'est pire que des statistiques mal interprétées).
Rôle du hasard	Nous évaluons mal le rôle du hasard dans les événements.
Fausseté des souvenirs	Nos souvenirs sont souvent faux ou reconstruits. Ils ne sont jamais objectifs et sont toujours le fruit de notre vision du monde, passée et présente.
Le non-partage de l'information	Les groupes tendent à ne prendre en compte et traiter que l'information reconnue et admise par tous les membres.
Le biais de conformité	Les individus tendent à adopter l'opinion perçue comme dominante dans le groupe.
Groupthink	Phénomène de groupe par lequel le désir d'harmonie ou de conformité

	perturbe ou rend irrationnel les processus de décision. Les membres du groupe essayent de minimiser les conflits et parviennent rapidement à prendre des décisions par consensus sans analyse critique des alternatives vite écartées et en s'isolant des influences extérieures. Conditions favorisant le *groupthink* : cohésion du groupe / isolement du groupe / préférence du leader pour une alternative particulière / absence de procédures méthodiques / homogénéité socioprofessionnelle et idéologique / stress important lié à des pressions extérieures / une fragilisation de l'estime de soi liée à des difficultés récentes Conséquences sur la décision : examen incomplet des alternatives / examen incomplet des objectifs / non prise en compte des risques associés à l'option préférée / non-réévaluation d'alternatives rejetées au départ / recherche d'information limitée / biais de sélection des informations / absence de plans alternatifs.
Faux consensus	Non-révélation des divergences au sein d'un groupe. Les processus de décision en deviennent très rapides, mais la qualité des choix médiocre.
Hubris	Narcissisme et confiance excessive en soi qui conduisent à une surestimation de ses capacités.
Biais d'engagement	Lien d'attachement entre un individu ou une organisation et son action, résultant de plusieurs types de facteurs psychologiques : calcul stratégique, « coûts perdus », obligation de se justifier à ses propres yeux, obligation de se justifier aux yeux d'autrui. L'engagement, s'il n'est pas rompu, débouche sur l'escalade : tendance à poursuivre une action inefficace et/ou coûteuse et/ou trop risquée.
Normalisation du danger	Situation où des individus ou organisations sont confrontés à des risques initialement jugés trop importants suffisamment longtemps pour qu'ils deviennent la norme (et ne soient plus considérés comme exceptionnels).
Injonctions paradoxales	Un individu ou un groupe est face à une injonction paradoxale lorsqu'il doit répondre à des attentes ou des directives contradictoires et/ou impossibles à réaliser. Parfois l'une des obligations est consciente, l'autre inconsciente (en jouant par exemple sur des motivations comme l'honneur, le respect, l'amitié, l'espoir, etc.), ce qui permet d'obtenir des choses que ces individus ne « veulent » pas faire. Quelques exemples : *reporting* croissant/autonomie, réactivité/anticipation, développement d'activités nouvelles/maîtrise des coûts, sécurité / liberté.
Solutions préférées	Certaines options sont préférées par les individus ou les organisations. Il s'agit de celles qui sont ou semblent : - Évidentes, qui tombent « sous le sens » - Irrésistibles, qu'elles relèvent de l'*hubris*, qu'il s'agisse des solutions

dominantes ou qu'elles promettent des gains ou succès exceptionnels
- Commodes, c'est-à-dire qui exonèrent d'en envisager d'autres
- Disponibles, validées ou expérimentées par d'autres
- Faciles à justifier

Cadrage des situations

Le cadrage d'une situation est la manière dont les individus comprennent une situation ou un problème auquel ils sont confrontés. Le cadrage dépend souvent de la façon dont un problème est posé. Il peut être influencé par le langage, les circonstances, les priorités, l'expérience, la plausibilité, les croyances… Un mauvais cadrage peut empêcher de voir ce qui est, ou faire voir ce qui n'est pas (ou plus). Il révèle aussi une tendance à fuir le risque face à la possibilité d'un gain (une opportunité) et à le rechercher le risque face à la possibilité d'une perte (une menace).

Dysfonctionnements d'équipe

Des critères peuvent alerter sur des problèmes d'une équipe à prendre de bonnes décisions :
- Défaillances générales dans la gestion des facteurs humains
- Pas de préparation à l'imprévu
- Forte distance hiérarchique au sein des équipes
- Relations d'allégeance néfastes à l'esprit d'équipe
- Communication défaillante
- Culture du blâme (sanction de la faute) neutralisant les initiatives et une saine gestion des erreurs
- Difficultés à travailler dans un environnement hétérogène
- Excès de confiance

Communication défaillante

Certains éléments sont essentiels pour assurer une bonne communication vis-à-vis de tiers non impliqués dans le processus de décision:
- Assurer la cohérence du discours
- Parler du changement, l'expliquer, lui donner du sens
- Expliquer les enjeux
- Valoriser les bénéfices
- Répondre aux interrogations et réduire les incertitudes
- Créer les conditions de l'implication et stimuler l'adhésion
- Guider la progression (étapes, plannings, avenir prévisible, etc.)
- Ne pas communiquer d'informations confidentielles ou inutilement anxiogènes

Renoncement éthique

Les individus peuvent renoncer à formuler des jugements éthiques et moraux sur leurs actions ou celles qui les entourent, se contentant d'obéir aux instructions ou aux procédures. Ils cessent de penser, démissionnent et ne se voient plus que comme un rouage qui n'a pas son mot à dire (cf. le concept de banalité du mal d'Hannah Arendt). Ces renoncements à penser par soi-même peuvent être des facteurs clés dans la commission d'actions immorales.

Oubli	L'absence de mémoire d'une organisation favorise la répétition de problèmes déjà survenus, pour lesquels des solutions – bonnes ou mauvaises – avaient déjà été trouvées. Il cause aussi souvent une perte de suivi dans le temps des actions et décisions adoptées.
Erreurs de raisonnement	De nombreuses erreurs d'appréciation ou de raisonnement peuvent négativement influencer raisonnements et décisions. Exemples d'erreurs très communes : - Si A, alors B. B. Alors c'est que A - Illusion de lien de causalité là où il n'y a que corrélation - Généralisations abusives (généraliser une observation particulière sans le justifier) - Focalisation inconsciente et arbitraire sur certains aspects au détriment d'autres
Dilution de la responsabilité	Les décisions de groupe, portées par le groupe, aboutissent à des prises de risque plus élevées que les décisions portées individuellement (Kogan & Wallach – 1964)

Adaptation aux domaines choisis

L'objectif de la présente étude est d'obtenir une méthode opérationnelle. Il convient donc maintenant d'instancier les facteurs vus précédemment aux trois domaines que nous avons choisis - l'évaluation de risques ; la définition et la mise en place de mesures de sécurité préventives ; la prise de décision en gestion de crise.

De plus, afin d'en faire un outil tout à fait opérationnel, chaque thématique sera traduite sous la forme d'une ou plusieurs questions. Le résultat en sera une liste de questions par domaine. Cette forme semble la plus adaptée pour réaliser rapidement une analyse sans interrompre ou perturber le processus observé.

Liste de questions

Nous allons maintenant essayer d'associer des questions à chaque facteur de risque identifié et dans les trois catégories d'activités que nous avons retenues.

L'objectif de ces questions, à chaque fois, est de mettre en lumière, de révéler, un problème potentiel.

Afin d'en faciliter la compréhension globale, il est conseillé de lire d'abord toutes les questions des premières colonnes pour tous les facteurs de risques, puis toutes les deuxièmes et enfin toutes les troisièmes.

Rationalité limitée

Les individus et les groupes ont l'intention d'être rationnels, mais en raison de leurs capacités cognitives limitées, ils n'y parviennent que dans une faible mesure.
Afin de pallier cette lacune, les organisations pensent souvent rationaliser leurs choix en faisant appel à des chiffres.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Les risques identifiés, leurs probabilités et leurs impacts reposent-ils sur des hypothèses réalistes (en particulier techniques, ou parce qu'ils se sont déjà matérialisés) ?	Les mesures de sécurité envisagées ont-elles une chance d'être réellement efficaces (empêcher des évènements ou se préparer à y réagir) ?	Est-on prêt à décider sans disposer de toutes les informations (ce qui revient à assumer que le choix ne sera pas tout à fait rationnel) ?
Présence d'illusion de rationalité (situation dans laquelle on croit que les choix ou comportements sont rationnels alors qu'ils ne le sont pas – par exemple du fait de l'usage d'une méthodologie qui semble infaillible) ?	Utilisation abusive de chiffres peu fiables ou dont l'interprétation est ambiguë pour « rationaliser » des choix ?	Choisit-on la première solution satisfaisante qui se présente, et non la solution optimale (ce qui est la démarche la plus rationnelle) ?
Utilisation abusive de chiffres peu fiables ou dont l'interprétation est ambiguë pour « rationaliser » des choix ?		Constate-t-on une utilisation abusive de chiffres peu fiables ou dont l'interprétation est ambiguë pour « rationaliser » des choix ?

Biais de confirmation

Tendance à favoriser l'information connue ou l'idée admise et à ne pas rechercher, à ignorer ou à rejeter les informations et les données qui la contredisent. Nous cherchons à confirmer nos idées, plus qu'à les remettre en question.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Des risques, des impacts ou des menaces ont-ils été considérés comme évidents ou relevant du « bon sens » ?	Des mesures de sécurité ont-elles été choisies parce que considérées comme évidentes ou relevant du « bon sens » ?	Des options ont-elles été prises parce que considérées comme évidentes ou relevant du « bon sens » ?
Des risques ont-ils été rejetés sans analyse, sur la base d'un argument unique et	Des mesures de sécurité ont-elles été rejetées sans analyse, sur la base d'un	Des options ont-elles été rejetées sans analyse, sur la base d'un argument unique et

rapidement traité?	argument unique et rapidement traité?	rapidement traité?

Biais de l'*énaction*

Nous construisons nous-mêmes, par nos actions et nos croyances, notre environnement. Nous le « mettons en scène » et avons tendance à considérer comme « vrai » ce qui semble « marcher » dans *notre* représentation du monde (« Je ne vois que ce que je crois »). Mais ce qui « marche » peut être faux, ou seulement partiellement vrai.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Le réalisme (caractère plausible) des probabilités et impacts des risques est-il validé par tous les intervenants ?	Le contexte des menaces dont il faut se protéger semble-t-il raisonnable à tous les intervenants ?	Les décisions prennent-elles en compte que « ce qui marche » en temps normal ne « marche » peut-être pas en situation de crise ?
Comment ce qui est considéré comme « vrai » est-il devenu une certitude ?	Comment ce qui est considéré comme « vrai » est-il devenu une certitude ?	Comment ce qui est considéré comme « vrai » est-il devenu une certitude ?

Histoires versus statistiques

Nous préférons la cohérence d'une histoire, d'un récit, à la réalité des statistiques (à noter cependant que rien n'est pire que des statistiques mal interprétées).

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Peut-on utiliser des statistiques fiables, pertinentes et dont l'interprétation est claire ?	Peut-on utiliser des statistiques fiables, pertinentes et dont la définition est claire ?	Peut-on utiliser des statistiques fiables, pertinentes et dont la définition est claire ?
Y a-t-il des transitions non assumées (ou mal) d'évaluations quantitatives à des évaluations qualitatives ?		

Rôle du hasard

Nous évaluons mal le rôle du hasard dans les événements.

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise
L'intervention du hasard ou de l'imprévu est-il pris en compte ?	L'intervention du hasard ou de l'imprévu est-il pris en compte (par exemple envisager des vulnérabilités futures qui semblent théoriques actuellement) ?	L'intervention du hasard ou de l'imprévu est-il pris en compte ?

Fausseté des souvenirs

Nos souvenirs sont souvent faux ou reconstruits. Ils sont toujours influencés par notre vision du monde, passée et présente.

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise
Les références au passé sont-elles factuelles et représentatives (souvenirs ou données) ?	Les références au passé sont-elles factuelles et représentatives (souvenirs ou données) ?	Les références au passé sont-elles factuelles et représentatives (souvenirs ou données) ?

Le non-partage de l'information

Les groupes tendent à ne prendre en compte et traiter que l'information reconnue et admise par tous les membres.

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise
Y a-t-il des informations considérées comme importantes par certains participants, mais non prises en compte collectivement ?	Y a-t-il des informations considérées comme importantes par certains participants, mais non prises en compte collectivement ?	Y a-t-il des informations considérées comme importantes par certains participants, mais non prises en compte collectivement ?

Le biais de conformité

Les individus tendent à adopter l'opinion perçue comme dominante dans le groupe.

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise

Chacun a-t-il eu l'occasion de se faire entendre et d'exprimer son opinion de façon indépendante (éventuellement anonyme) ?	Chacun a-t-il eu l'occasion de se faire entendre et d'exprimer son opinion de façon indépendante (éventuellement anonyme) ?	Chacun a-t-il eu l'occasion de se faire entendre et d'exprimer son opinion de façon indépendante (éventuellement anonyme) ?
Y a-t-il des informations qui pourraient être prises en compte mais sont rejetées par la majorité ?	Y a-t-il des informations qui pourraient être prises en compte mais sont rejetées par certains ?	Y a-t-il des informations qui pourraient être prises en compte mais sont rejetées par certains ?

Groupthink

Phénomène de groupe par lequel le désir d'harmonie ou de conformité perturbe ou rend irrationnel les processus de décision. Les membres du groupe essayent de minimiser les conflits et parviennent rapidement à prendre des décisions par consensus sans analyse critique des alternatives vite écartées et en s'isolant des influences extérieures.
Conditions favorisant le *groupthink* : cohésion du groupe / isolement du groupe / préférence du leader pour une alternative particulière / absence de procédures méthodiques / homogénéité socioprofessionnelle et idéologique / stress important lié à des pressions extérieures / une fragilisation de l'estime de soi liée à des difficultés récentes
Conséquences sur la décision : examen incomplet des alternatives / examen incomplet des objectifs / non prise en compte des risques associés à l'option préférée / non-réévaluation d'alternatives rejetées au départ / recherche d'information limitée / biais de sélection des informations / absence de plans alternatifs

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Un consensus a-t-il surgi rapidement ?	Un consensus a-t-il surgi rapidement ?	Un consensus a-t-il surgi rapidement ?
Des risques ont-ils été trop rapidement acceptés, ou écartés ?	Des alternatives viables ont-elles été trop rapidement écartées ?	Des alternatives viables ont-elles été trop rapidement écartées ?
Le groupe est-il très homogène (fonctions, expérience, personnalités) ?	Le groupe est-il très homogène (fonctions, expérience, personnalités) ?	Le groupe est-il très homogène (fonctions, expérience, personnalités) ?
La hiérarchie ou le leader expriment-ils des préférences fortes pour les choix à faire ou les options à prendre ?	La hiérarchie ou le leader expriment-ils des préférences fortes pour les choix à faire ou les options à prendre ?	La hiérarchie ou le leader expriment-ils des préférences fortes pour les choix à faire ou les options à prendre ?

Faux consensus

Non-révélation des divergences au sein d'un groupe. Les processus de décision en deviennent très rapides, mais la qualité des choix médiocre.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Est-ce que les participants demandent des précisions sur les points de vue des autres ?	Est-ce que les participants demandent des précisions sur les points de vue des autres ?	Est-ce que les participants demandent des précisions sur les points de vue des autres ?
Est-ce que les participants accueillent les informations nouvelles et discutent des données ambiguës ?	Est-ce que les participants accueillent les informations nouvelles et discutent des données ambiguës ?	Est-ce que les participants accueillent les informations nouvelles et discutent des données ambiguës ?
Est-ce que les participants reformulent leurs propositions en intégrant les critiques reçues plutôt que de répéter les mêmes arguments ?	Est-ce que les participants reformulent leurs propositions en intégrant les critiques reçues plutôt que de répéter les mêmes arguments ?	Est-ce que les participants reformulent leurs propositions en intégrant les critiques reçues plutôt que de répéter les mêmes arguments ?
Est-ce que les participants sont tous actifs dans la discussion ?	Est-ce que les participants sont tous actifs dans la discussion ?	Est-ce que les participants sont tous actifs dans la discussion ?
Est-ce que les participants ont pu exprimer librement leur avis (vote secret si besoin) ?	Est-ce que les participants ont pu exprimer librement leur avis (vote secret si besoin) ?	Est-ce que les participants ont pu exprimer librement leur avis (vote secret si besoin) ?

Hubris

Narcissisme et confiance excessive en soi qui conduisent à une surestimation de ses capacités.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Y a-t-il des risques identifiés et analysés avec un excès de confiance manifeste?	La capacité à faire a-t-elle été factuellement évaluée ?	Y a-t-il des décisions dont la nécessité est affirmée comme « évidente »?
	La possibilité de désactiver des mesures de sécurité en cas d'urgence (par exemple en cas de crise) et l'entrainement à ces situations est-elle prévue ?	Si un ou des intervenants sont très actifs, sont-ils challengés à l'égal des autres ?
		Y a-t-il des arguments du type « nous y arriverons parce que

		nous sommes meilleurs que les autres » ?

Biais d'engagement

Lien d'attachement entre un individu ou une organisation et son action, résultant de plusieurs types de facteurs psychologiques : calcul stratégique, « coûts perdus », obligation de se justifier à ses propres yeux, obligation de se justifier aux yeux d'autrui. L'engagement, s'il n'est pas rompu, débouche sur l'escalade : tendance à poursuivre une action inefficace et/ou coûteuse et/ou trop risquée.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Perçoit-on un attachement émotionnel à certains risques, certaines menaces ?	Y a-t-il des arguments relevant de « nous avons commencé, il faut continuer » ?	Y a-t-il des responsables hiérarchiques qui s'impliquent trop dans la technique du fait de leurs anciennes fonctions techniques ?
Des risques sont-ils minimisés ou maximisés pour ne pas afficher une modification d'un risque précédemment évalué différemment ?	Les raisons de poursuivre une logique ou une action se justifient-elles indépendamment de ce qui a déjà été fait ?	Y a-t-il des intervenants qui semblent trop impliqués émotionnellement dans la gestion de crise ?
	Réinvestit-on dans une technologie du seul fait de l'engagement avec un fournisseur / prestataire / éditeur ?	

Normalisation du danger

Situation où des individus ou organisations sont confrontés à des risques initialement jugés trop importants suffisamment longtemps pour qu'ils deviennent la norme (et ne soient plus considérés comme exceptionnels).

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Y a-t-il des risques ou des dangers qui sont acceptés « parce que nous nous y sommes habitués » ?	Y a-t-il des mesures de sécurité préventives qui sont écartées parce qu'un risque est devenu « commun », « habituel » ?	Suite à un incident de sécurité majeur, y a-t-il lieu de modifier certaines évaluations de risques faites précédemment ?
Y a-t-il des arguments du type		Après la crise, toutes les *root*

« puisque le risque ne s'est jamais matérialisé, on peut continuer » ? Y a-t-il eu des modifications de l'évaluation des risques sans nouvelles informations (sur les menaces, les mesures en place, etc.) ?		*cause* sont-elles identifiées et traitées ?

Injonctions paradoxales

Un individu ou un groupe est face à une injonction paradoxale lorsqu'il doit répondre à des attentes ou des directives contradictoires et/ou impossibles à réaliser. Parfois l'une des obligations est consciente, l'autre inconsciente (en jouant par exemple sur des motivations comme l'honneur, le respect, l'amitié, l'espoir, etc.), ce qui permet d'obtenir des choses que ces individus ne « veulent » pas faire. Quelques exemples : *reporting* croissant / autonomie, réactivité / anticipation, développement d'activités nouvelles / maîtrise des coûts, sécurité / liberté.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Y a-t-il des instructions contradictoires (par exemple, demande que les risques soient bien évalués, mais que l'affichage ne soit pas anxiogène) ?	Y a-t-il des demandes dont il est évident qu'elles sont contradictoires ou impossibles à satisfaire (comme, parfois : plus de sécurité et plus de liberté pour les utilisateurs) ?	En cours de gestion de crise, y a-t-il des demandes paradoxales (par exemple exiger que les techniciens travaillent et proposent des solutions tout en tenant compte d'instructions techniques de la hiérarchie) ?

Solutions préférées

Certaines options sont préférées par les individus ou les organisations. Il s'agit de celles qui sont ou semblent :
- Évidentes, qui tombent « sous le sens »
- Irrésistibles, qu'elles relèvent de l'*hubris*, qu'il s'agisse des solutions dominantes ou qu'elles promettent des gains ou succès exceptionnels
- Commodes, c'est-à-dire qui exonèrent d'en envisager d'autres
- Disponibles, validées ou expérimentées par d'autres
- Faciles à justifier

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Y a-t-il des risques qui sont	Y a-t-il des options qui ont été	Y a-t-il des tentatives de sorties

jugés importants parce que « c'est évident » ?	adoptées surtout parce qu'elles sont évidentes, irrésistibles, commodes, disponibles ou faciles à justifier ?	de crise qui sont envisagées surtout parce qu'elles semblent « évidentes », « irrésistibles », « commodes », « disponibles » ou « faciles à justifier » ?
	Y a-t-il des options techniques qui ne sont décidées que par crainte que ne pas l'avoir fait soit reproché ultérieurement ?	Y a-t-il des décisions techniques qui ne sont décidées que par crainte que ne pas l'avoir fait soit reproché ultérieurement ?
	Y a-t-il des choix sécurité dont la seule justification est l'exemple d'un unique tiers (*benchmarking* incomplet et abusif)?	

Cadrage des situations

Le cadrage d'une situation est la manière dont les individus comprennent une situation ou un problème auquel ils sont confrontés. Le cadrage dépend souvent de la façon dont un problème est posé. Il peut être influencé par le langage, les circonstances, les priorités, l'expérience, la plausibilité, les croyances… Un mauvais cadrage peut empêcher de voir ce qui est, ou faire voir ce qui n'est pas (ou plus). Il révèle aussi une tendance à fuir le risque face à la possibilité d'un gain (une opportunité) et à le rechercher le risque face à la possibilité d'une perte (une menace).

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Les menaces et enjeux sous-jacents aux risques ont-ils fait l'objet d'une analyse contradictoire ?	La formulation de la problématique initiale a-t-elle fait l'objet d'une analyse contradictoire ?	La description du contexte, de l'état des lieux de la crise a-t-elle fait l'objet d'une analyse contradictoire ?
Les risques sont-ils exprimés dans un contexte d'un gain potentiel ou d'une perte ? (sachant qu'il y a une tendance à fuir le risque face à la possibilité d'un gain (une opportunité) et à le rechercher le risque face à la possibilité d'une perte (une menace)).	Y a-t-il des différences d'analyse du contexte dont l'origine peut être la langue, la culture ?	Les décisions seraient-elles les mêmes si, au lieu d'espérer un « gain » on limitait une « perte » ? Et inversement ?
Y a-t-il des différences d'analyse du contexte dont l'origine peut être la langue, la culture ?		Y a-t-il des différences d'analyse du contexte dont l'origine peut être la langue, la culture ?

Dysfonctionnements d'équipe

Des critères peuvent alerter sur des problèmes d'une équipe à prendre de bonnes décisions :
- Défaillances générales dans la gestion des facteurs humains
- Pas de préparation à l'imprévu
- Forte distance hiérarchique au sein des équipes
- Relations d'allégeance néfastes à l'esprit d'équipe
- Communication défaillante
- Culture du blâme (sanction de la faute) neutralisant les initiatives et une saine gestion des erreurs
- Difficultés à travailler dans un environnement hétérogène
- Excès de confiance

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Y a-t-il des relations d'allégeance ou de trop fortes distances hiérarchiques néfastes au fonctionnement de l'équipe ?	Y a-t-il des relations d'allégeance ou de trop fortes distances hiérarchiques néfastes au fonctionnement de l'équipe ?	Y a-t-il des relations d'allégeance ou de trop fortes distances hiérarchiques néfastes au fonctionnement de la cellule de crise ?
La communication au sein de l'équipe est-elle défaillante ?	La communication au sein de l'équipe est-elle défaillante ?	La communication au sein de la cellule de crise est-elle défaillante ?
Y a-t-il une culture du blâme (sanction de la faute) neutralisant les initiatives et une saine gestion des erreurs ?	Y a-t-il une culture du blâme (sanction de la faute) neutralisant les initiatives et une saine gestion des erreurs ?	Y a-t-il une culture du blâme (sanction de la faute) neutralisant les initiatives et une saine gestion des erreurs ?
		Les équipes semblent-elles préparées à gérer l'imprévu ?

Communication défaillante

Certains éléments sont essentiels pour assurer une bonne communication vis-à-vis de tiers non impliqués dans le processus de décision:
- Assurer la cohérence du discours
- Parler du changement, l'expliquer, lui donner du sens
- Expliquer les enjeux
- Valoriser les bénéfices
- Répondre aux interrogations et réduire les incertitudes
- Créer les conditions de l'implication et stimuler l'adhésion
- Guider la progression (étapes, plannings, avenir prévisible, etc.)
- Ne pas communiquer d'informations confidentielles ou inutilement anxiogènes

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise
S'il y a communication vis-à-vis de tiers, les critères suivants sont-ils respectés : cohérence du discours / explication du changement, lui donner du sens / expliquer les enjeux / valoriser les bénéfices / répondre aux interrogations et réduire les incertitudes / créer les conditions de l'implication et stimuler l'adhésion / guider la progression / pas de communication d'informations confidentielles ou inutilement anxiogènes ?	S'il y a communication vis-à-vis de tiers, les critères suivants sont-ils respectés : cohérence du discours / explication du changement, lui donner du sens / expliquer les enjeux / valoriser les bénéfices / répondre aux interrogations et réduire les incertitudes / créer les conditions de l'implication et stimuler l'adhésion / guider la progression / pas de communication d'informations confidentielles ou inutilement anxiogènes ?	S'il y a communication de crise (vis-à-vis de l'extérieur), les critères suivants sont-ils respectés : cohérence du discours / explication du changement, lui donner du sens / expliquer les enjeux / valoriser les bénéfices / répondre aux interrogations et réduire les incertitudes / créer les conditions de l'implication et stimuler l'adhésion / guider la progression / pas de communication d'informations confidentielles ou inutilement anxiogènes ?

Renoncement éthique

Les individus peuvent renoncer à formuler des jugements éthiques et moraux sur leurs actions ou celles qui les entourent, se contentant d'obéir aux instructions ou aux procédures. Ils cessent de penser, démissionnent et ne se voient plus que comme un rouage qui n'a pas son mot à dire (cf. le concept de banalité du mal de H. Arendt). Ces renoncements à penser par soi-même peuvent être des facteurs clés dans la commission d'actions immorales.

Évaluation des risques	Définition et mise en place de mesures de sécurité	Prise de décision en situation de crise
La façon dont les risques, menaces et impacts sont évalués est-elle éthiquement légitime ?	Les décisions ou actions dans lesquelles je suis impliqué ou auxquelles j'assiste sont-elles éthiquement légitimes ?	Les décisions ou actions de résolution de crise dans lesquelles je suis impliqué ou auxquelles j'assiste sont-elles éthiquement légitimes ?
L'analyse de risque peut-elle, d'une façon ou d'une autre, entrainer des conséquences éthiquement inacceptables ?	Les mesures de sécurité mises en place peuvent-elles entrainer des conséquences éthiquement inacceptables ?	Les décisions ou actions de résolution de crise peuvent-elles entrainer des conséquences éthiquement inacceptables ?

Oubli

L'absence de mémoire d'une organisation favorise la répétition de problèmes déjà survenus, pour

lesquels des solutions – bonnes ou mauvaises – avaient déjà été trouvées.
Il cause aussi souvent une perte de suivi dans le temps des actions et décisions adoptées.

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
A-t-on regardé si une analyse similaire avait été effectuée dans le passé ?	A-t-on regardé si des mesures de sécurité traitant les mêmes risques ont été discutées / envisagées / décidées / mise en place dans le passé ?	A-t-on regardé si on a déjà connu des crises similaires, et si oui, a-t-on regardé les décisions qui avaient été prises ?
L'évaluation des risques est-elle correctement conservée pour éventuelle utilisation ultérieure ?	L'information est-elle conservée pour capitaliser la connaissance et l'expérience ?	Les causes, les circonstances et les actions de résolution de la crise ou de l'incident donnent-elles lieu à un retour d'expérience (REX) objectif?
Les mesures de sécurité envisagées pour réduire un risque sont-elles correctement suivies dans le temps ?	Les actions et démarches sécurité sont-elles correctement suivies dans le temps ?	S'il y a un retour d'expérience (REX) « édulcoré » à des fins de communication (interne ou externe), un REX « brut » est-il néanmoins conservé et exploité ?
	Est-il prévu de faire un bilan a posteriori?	Les actions de résolution des problèmes (*root cause*) sont-elles correctement suivies dans le temps ?
		Un bilan est-il fait et des leçons tirées (dans le REX par exemple) spécifiquement sur la façon dont l'organisation a géré la crise ou l'incident (en vue d'améliorer la gestion de crise / d'incident) ?

Erreurs de raisonnement

De nombreuses erreurs d'appréciation ou de raisonnement peuvent négativement influencer raisonnements et décisions. Exemples d'erreurs très communes :
- Si A, alors B. B. Alors c'est que A
- Illusion de lien de causalité là où il n'y a que corrélation
- Généralisations abusives (généraliser une observation particulière sans le justifier)
- Focalisation inconsciente et arbitraire sur certains aspects au détriment d'autres

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**

Y a-t-il des erreurs de logique élémentaires dans les raisonnements ?	Y a-t-il des erreurs de logique élémentaires dans les raisonnements ?	Y a-t-il des erreurs de logique élémentaires dans les raisonnements ?
L'appréciation des risques est-elle relativement homogène ou l'analyse de certains risques est-elle disproportionnée ?	Les efforts de sécurisation sont-ils relativement homogènes et ne laissent-ils pas des vulnérabilités béantes non couvertes ?	

Dilution de responsabilité

Les décisions de groupe, portées par le groupe, aboutissent à des prises de risque plus élevées que les décisions portées individuellement (Kogan & Wallach – 1964)

Évaluation des risques	**Définition et mise en place de mesures de sécurité**	**Prise de décision en situation de crise**
Les porteurs des risques résiduels sont-ils clairement et nommément identifiés (différents d'un comité ou d'un service)?	Les porteurs des risques résiduels sont-ils clairement et nommément identifiés (différents d'un comité ou d'un service)?	Les porteurs des risques résiduels sont-ils clairement et nommément identifiés (différents d'un comité ou d'un service)?

Simulations d'application

Afin de vérifier la pertinence de nos questions, nous allons les dérouler pour chaque problème cité plus haut dans les trois domaines d'activité (évaluation des risques, définition et mise en œuvre de mesures de sécurité et prise de décision en situation de crise).

L'objectif est de vérifier que nos questions permettent d'identifier l'apparition ou la présence de ces problèmes, en cours de processus.

Application à l'évaluation des risques

Si nous reprenons les exemples de problèmes concernant les évaluations de risques et que nous déroulons la liste de questions que nous avons bâtie, nous pouvons remplir le tableau suivant :

Problèmes identifiés	**Questions permettant d'en identifier l'apparition ou la présence**
À l'heure d'estimer la criticité d'une application ou d'une infrastructure, des équipes projet sous-estiment ou surestiment par erreur la criticité de leur application finale. Ces erreurs, toujours	Beaucoup des questions de la liste permettent de déceler des problèmes de démarche ou de fonctionnement d'une équipe menant à ces erreurs d'appréciations.

humaines, peuvent avoir de multiples causes.	
Parfois, sachant que des mesures de sécurité contraignantes vont en découler, les chefs de projet sous-estiment volontairement la criticité de leur projet.	Les questions sur la normalisation du danger peuvent permettre d'éviter ces situations, par exemple : Y a-t-il des risques ou des dangers qui sont acceptés « parce que nous nous y sommes habitués » ? En effet, si le risque est volontairement sous-estimé c'est que l'on pense sincèrement que les mesures proposées sont exagérées.
La sélection des mesures de sécurité correspondant à la criticité identifiée est automatiquement proposée par l'outil d'analyse des risques, mais une personnalisation au contexte est rarement faite. Cette activité de sélection des mesures peut sembler très rassurante, donnant une illusion de rigueur parce que reposant sur une méthodologie compliquée. Si rassurante que l'on omet de la contextualiser.	Le problème d'une telle « automaticité », des mesures de sécurité proposées selon la criticité peut être décelé par les questions sur la rationalité limitée, par exemple : « Présence d'illusion de rationalité (situation dans laquelle on croit que les choix ou comportements sont rationnels alors qu'ils ne le sont pas – par exemple du fait de l'usage d'une méthodologie qui semble infaillible) ? »
Erreurs flagrantes d'appréciation des risques ; il s'agit toujours d'erreurs humaines qui peuvent avoir de multiples causes.	Beaucoup des questions de la liste permettent de déceler des problèmes de démarche ou de fonctionnement d'une équipe menant à ces erreurs d'appréciations.
Des projets échappent à ces analyses de risques, soit parce qu'ils prennent la forme de changements et échappent à la méthodologie projet, soit parce que tout ou partie du projet est réalisé en faisant appel à des services externalisés (ce type de pratiques étant parfois qualifié de *shadow IT*).	Il s'agit d'un problème organisationnel (processus défaillant de validation et de « rattrapage » des projets), qui n'est pas identifié par notre liste de questions.
Le suivi et le bilan des risques résiduels sont souvent parcellaires ou omis.	La question « Les mesures de sécurité envisagées pour réduire un risque sont-elles correctement suivies dans le temps ? » permet de relever ce type de problèmes.
Comme pour le *shadow IT*, certains changements, étant hors projet, échappent tout à fait aux analyses de risques.	Il s'agit d'un problème organisationnel (processus défaillant de validation des changements), qui n'est pas identifié par notre liste de questions.
Le processus d'acceptation formelle des risques résiduels est souvent défaillant. Un « projet » ou un « métier » sont classiquement les porteurs identifiés des risques. Or on constate que les risques sont beaucoup plus facilement acceptés par des services, fonctions ou des collectifs que par des individus nommément identifiés	La question « Les porteurs des risques résiduels sont-ils clairement et nommément identifiés (différent d'un comité ou d'un service)? » permet d'identifier ce problème d'acceptation claire des risques.

(conjointement à leur fonction).

Application à la définition et mise en place de mesures de sécurité

Si nous reprenons les exemples de problèmes concernant la définition et la mise en place de mesures de sécurité et que nous déroulons la liste de questions que nous avons bâtie, nous pouvons remplir le tableau suivant :

Problèmes identifiés	**Questions permettant d'en identifier l'apparition ou la présence**
Grand soin apporté à la rédaction de documents, mais piètre suivi de la mise en œuvre de ce qu'ils recommandent.	La question « Les actions et démarches sécurité sont-elles correctement suivies dans le temps ? » peut préventivement alerter sur ce risque d'absence de suivi.
Choix de configurations techniques soit disproportionnées par rapport aux risques, soit inhomogènes, c'est-à-dire laissant des vulnérabilités non couvertes entraînant des situations de risque importantes.	La question concernant les erreurs de raisonnement et d'appréciation peut aider à détecter ce type de problèmes : « Les efforts de sécurisation sont-ils relativement homogènes et ne laissent-ils pas des vulnérabilités béantes non couvertes ? »
Choix de produits ou solutions sans analyse contradictoire suffisamment poussée, dont la conséquence est l'acquisition de produits à l'efficacité limitée.	Plusieurs questions peuvent aider à déceler ce type de problèmes : - Les mesures de sécurité envisagées ont-elles une chance d'être réellement efficaces (empêcher des évènements ou se préparer à y réagir) ? - Des mesures de sécurité ont-elles été choisies parce que considérées comme évidentes ou relevant du « bon sens » ? - Chacun a-t-il eu l'occasion de se faire entendre et d'exprimer son opinion de façon indépendante (éventuellement anonyme) ? - Un consensus a-t-il surgi rapidement ? - Réinvestit-on dans une technologie du seul fait de l'engagement avec un fournisseur / prestataire / éditeur ? - Y a-t-il des options qui ont été adoptées surtout parce qu'elles sont évidentes, irrésistibles, commodes, disponibles ou faciles à justifier ? - Y a-t-il des choix sécurité dont la seule justification est l'exemple d'un unique tiers (*benchmarking* incomplet et abusif)?
Acquisition de produits très satisfaisants, mais lacunes majeures dans la mise en place des processus de gestion (organisationnels) de ces produits.	Bien que cette liste de question ne permette pas d'identifier spécifiquement l'oubli des aspects organisationnels, une question comme « Les actions et démarches sécurité sont-elles

	correctement suivies dans le temps ? » peut permettre de se rendre compte de ce travers. La question « Est-il prévu de faire un bilan a posteriori? » devrait aussi attirer l'attention sur cet aspect essentiel, la mise en place de procédures organisationnelles.
Mauvaise évaluation de la menace, menant à des choix stratégiques ou tactiques peu pertinents.	Les deux questions suivantes peuvent alerter sur ce type de problème : - Le contexte des menaces dont il faut se protéger semble-t-il raisonnable à tous les intervenants ? - Y a-t-il des mesures de sécurité préventives qui sont écartées parce qu'un risque est devenu « commun », « habituel » ?
Décisions techniques prises trop rapidement, sur la base de critères contestables.	Beaucoup des questions permettent de déceler les nombreuses causes de ce type de problèmes.
Perte de la mémoire de l'entreprise qui peut avoir pour conséquence la répétition d'erreurs très similaires.	La question « L'information est-elle conservée pour capitaliser la connaissance et l'expérience ? » peut alerter sur les mesures à mettre en place pour assurer une persistance de la connaissance (comme des processus de *knowledge management*)
Situations de soumission et de fragilité contractuelle vis-à-vis des fournisseurs, par exemple manque de moyens de pression pour leur faire adopter des mesures de sécurité importantes.	Une question comme « L'intervention du hasard ou de l'imprévu est-il pris en compte (par exemple envisager des vulnérabilités futures qui semblent théoriques actuellement) ? » peut révéler des lacunes dans les engagements contractuels (« Quelles obligations pouvons-nous demander aux fournisseurs en cas de… » ; « Que ferez-vous si… »)
Il arrive également que la hiérarchie, convaincue par des vendeurs ou des consultants veuille imposer des solutions dont les équipes techniques savent ou anticipent qu'elles ne seront pas efficaces.	La question « La hiérarchie ou le leader exprime-t-ils des préférences fortes pour les choix à faire ou les options à prendre ? » peut mettre en évidence ce type de travers. Il est d'autant plus critique lorsque le responsable ou le leader n'est pas un expert reconnu dans le domaine.

Application à la prise de décision en situation de crise

Si nous reprenons les exemples de problèmes concernant la définition et la prise de décision en situation de crise et que nous déroulons la liste de questions que nous avons bâtie, nous pouvons remplir le tableau suivant :

Problèmes identifiés	**Questions permettant d'en identifier l'apparition ou la présence**

Organisation prévue pour gérer les crises non appliquée lorsqu'elle arrive, ce dont il résulte une improvisation qui ralentit le retour à la normale.	Bien que ce soit un problème organisationnel qui n'est pas directement traité par notre questionnaire, la suivante peut alerter sur des défaillances flagrantes : « Les équipes semblent-elles préparées à gérer l'imprévu ? »
Difficultés pour la hiérarchie à prendre du recul vis-à-vis des actions techniques, et difficultés des techniciens à se départir des réflexes du quotidien.	Deux questions peuvent relever ce type de travers : - La hiérarchie ou le leader expriment-ils des préférences fortes pour les choix à faire ou les options à prendre ? - Y a-t-il des responsables hiérarchiques qui s'impliquent trop dans la technique du fait de leurs anciennes fonctions techniques ?
Les leçons post-incident sont en général bien faites, des actions sont prises et suivies, mais les leçons sur les problèmes de la gestion d'incident elle-même sont rarement formalisées.	La question « Un bilan est-il fait et des leçons tirées (dans le REX par exemple) spécifiquement sur la façon dont l'organisation a géré la crise ou l'incident (en vue d'améliorer la gestion de crise / d'incident) ? » permet d'assurer une possible amélioration continue en matière de gestion de crise / incident.
Les rapports de retour d'expérience (REX) sont parfois édulcorés du fait de leur future transmission à la haute hiérarchie.	La question « Les causes, les circonstances et les actions de résolution de la crise ou de l'incident donnent-elles lieu à un retour d'expérience (REX) objectif? » permet de s'assurer qu'un retour d'expérience sera bien rédigé, et la question « S'il y a un retour d'expérience (REX) « édulcoré » à des fins de communication (interne ou externe), un REX « brut » est-il néanmoins conservé et exploité ? » permet de garantir qu'un REX utile sera bien rédigé et exploité.
Certaines actions devraient parfois être explicitées avec plus de discrétion (par exemple le fait de solliciter un service sécurité pour investiguer sur une malveillance) pour ne pas susciter des rumeurs qui ajoutent au stress collectif.	La question sur la communication, en particulier le dernier item peut prémunir de ce type d'erreurs : « S'il y a communication de crise (vis-à-vis de l'extérieur), les critères suivants sont-ils respectés : cohérence du discours / explication du changement, lui donner du sens / expliquer les enjeux / valoriser les bénéfices / répondre aux interrogations et réduire les incertitudes / créer les conditions de l'implication et stimuler l'adhésion / guider la progression / pas de communication d'informations confidentielles ou inutilement anxiogènes ? »
Il est arrivé que des actions techniques n'ayant aucune chance de résoudre les problèmes soient tentées en cours de gestion de crise (comme des	La question « Y a-t-il des décisions techniques qui ne sont décidées que par crainte que ne pas l'avoir fait soit reproché ultérieurement ? »

redémarrages de serveurs), uniquement pour que cela ne puisse pas être reproché ultérieurement (de ne pas l'avoir « tenté »).	pointe spécifiquement ce type d'actions inutiles.
Parfois, il est arrivé que des mesures de sécurité aient empêché d'intervenir rapidement pour gérer un incident majeur ou une crise, et qu'il n'y eût pas de possibilité de les débrayer en cas de situation exceptionnelle.	Ce problème qui se révèle souvent en cours de crise ou d'incident majeur devrait avoir été identifié grâce à la question de la catégorie « Définition et mise en place de mesures de sécurité » : « La possibilité de désactiver des mesures de sécurité en cas d'urgence (par exemple en cas de crise) et l'entrainement à ces situations est-elle prévue ? »
Il arrive fréquemment que les cellules de crise, où siègent les décisionnaires, sollicitent trop les techniciens en charge de la résolution de la crise. Il en résulte souvent un stress peu propice au travail efficace. Dans certains cas, on a même pu observer une sorte d'inversion des rôles, c'est-à-dire que les cellules de crises se sont mises à ordonner des actions, au lieu de décider celles que leur proposaient les *sachants* et techniciens.	De telles dérives peuvent être décelées à l'aide des trois questions suivantes : - En cours de gestion de crise, y a-t-il des demandes paradoxales (par exemple exiger que les techniciens travaillent et proposent des solutions tout en tenant compte d'instructions techniques de la hiérarchie) ? - La hiérarchie ou le leader expriment-ils des préférences fortes pour les choix à faire ou les options à prendre ? - Y a-t-il des responsables hiérarchiques qui s'impliquent trop dans la technique du fait de leurs anciennes fonctions techniques ?
Parfois, dans l'urgence de la gestion d'une crise ou d'un incident majeur, des décisions sont prises sur la base de fausses informations ou d'hypothèses erronées qu'il aurait été souvent aisé de disqualifier (souvent, un technicien aurait pu rapidement alerter sur l'erreur). S'il est essentiel de savoir décider sans disposer de toutes les informations, il est tout aussi vital de pouvoir s'appuyer sur quelques certitudes. Dans la plupart des cas c'est l'urgence et l'enthousiasme à l'idée de tenir une piste qui rend aveugle sur la qualité de ces informations.	La question « Est-on prêt à décider sans disposer de toutes les informations (ce qui revient à assumer que le choix ne sera pas tout à fait rationnel) ? » rappelle l'importance de cet état d'esprit en situation de crise, tandis que la question « Comment ce qui est considéré comme « vrai » est-il devenu une certitude ? » devrait pouvoir alerter sur la nécessaire vigilance quant à la fiabilité des informations qui justifient des actions structurantes.

Méthodologie d'utilisation

La présente méthodologie a vocation à détecter des problèmes, pas à les résoudre.

Une importante proportion des questions est dédiée à relever des problèmes de fonctionnements collectifs, c'est-à-dire que ses lieux d'exercice privilégiés sont les réunions, comités, groupes de travail, cellules de crise.

Les questionnaires « Évaluation des risques » et « Prise de décision en situation de crise », bien que prévus pour analyser l'action de groupes pourront néanmoins être utilisés par des individus, sur eux-mêmes, pendant ou après leurs activités. Ils peuvent alors servir de garde-fous concernant leur propre travail, ou comme outil de vérification du travail d'autres équipes ou personnes.

Le questionnaire « Prise de décision en situation de crise », devrait typiquement être déroulé de façon continue (c'est-à-dire que parvenu à la fin de la liste on reprend au début) tout au long de la gestion de crise / d'incident. La tâche nécessite un certain recul vis-à-vis des actions de résolutions elles-mêmes. En faisant l'hypothèse qu'une cellule de crise est présidée par un responsable qui assume *in fine* les décisions importantes, qu'un autre responsable anime la réunion, coordonne et prend des notes pour le compte-rendu, la tache de dérouler le questionnaire devrait être dévolu à une troisième personne n'intervenant que lorsqu'il détecte un problème dans le déroulement de la gestion de crise.

Conclusion

L'exercice de confrontation des problèmes concrets observés sur les trois cas de figure étudiés avec les questions définies semble indiquer une certaine pertinence.

Néanmoins, ces questionnaires ne peuvent prétendre à l'exhaustivité. Comme les méthodologies OWASP ou CIS CSC citées plus haut, il faut les considérer comme des tamis. Selon la précision des questions, l'expérience et l'expertise de celui qui les pose, elles peuvent permettre d'identifier des biais courants, mais qui s'expriment toujours de façon particulière.

Et tout comme ces méthodes, ils ne deviendront efficaces que polis par la confrontation avec la réalité. Leur pratique seule permettra d'affiner les questions, d'en réduire le nombre ou d'ajouter des catégories importantes de risques humains.

Afin de compléter l'efficacité de ces questions, il pourra s'avérer utile d'ajouter des questions « positives », c'est-à-dire ne visant pas à identifier des problèmes connus mais à souligner des divergences avec certaines pratiques validées par l'expérience.

Un approfondissement de la méthode devra affiner les aspects temporels : comment déterminer le bon moment de prise d'une décision sécurité ? Comment éviter que les précautions prises – pour éviter de mauvaises décisions – ne finissent pas elles-mêmes par détériorer le processus de décision ?

Dans le but de faciliter l'utilisation de cette méthode en conditions opérationnelles, il conviendra de faire quelques propositions concrètes d'usage. Un outil pourra également être conçu.

Enfin, soulignons qu'au début de l'élaboration de cette méthode nous avions à l'esprit de la compléter par des recommandations qui viendraient d'une certaine façon répondre aux questions soulevées. Il apparait après quelques essais que ce serait réduire l'utilité de la méthode. En effet, si des recommandations étaient formalisées, elles seraient soit trop génériques et donc peu utiles, soit précises mais peu adaptées aux situations particulières. De plus, des recommandations auraient probablement l'inconvénient de pousser les utilisateurs de la méthode à directement consulter « la solution », la recommandation. Or l'intérêt principal de la méthode est de soulever des questions. De

pousser à la réflexion. D'inciter au doute. Charge à ceux qui l'utilisent d'apporter les réponses adaptées à leur contexte. Ainsi ouverte, cette méthode n'est donc pas un outil d'aide à la décision sécurité, mais bien plutôt un outil d'aide à la « non prise » de mauvaises décisions.

Références

La plupart des biais et travers communément observés sont issus du cours « Sécurité / Sûreté et management » de l'ESCP Europe, dispensés courant 2016 par Yannick Meiller, Jean-Philippe Bouilloud, Nathalie Prime, Florence Garrigues, Carla Mendoza et Hervé Laroche.

Licence