



MASTER 2 « MANAGEMENT ET INGENIERIE EN SECURITE GLOBALE APPLIQUEE »

«En quoi la culture de sécurité des chefs d'entreprises de TPE et PME contribue-t-elle à la gestion d'une situation d'exception ? »

Fabien Valente

08/01/2018

Sommaire

Sommaire	2
Remerciements	4
Résumé	5
Abstract	6
Introduction	7
1) Visiographie des Petites et Moyennes Entreprises en France : Qui sont nos TPE et PME ?	
a. Qu'est-ce qu'une Petite et Moyenne Entreprise ?	9
b. Quel panorama des TPE et PME en France ?	11
i. Les caractéristiques générales des entreprises en France	11
ii. L'identité des TPE et PME en France	12
iii. Les caractéristiques régionales des TPE et PME	20
iv. Les particularités des TPE et PME	20
2) Qu'elles problématiques de sécurité globale des TPE et PME et quelles solutions pour faire face aux situations de crise ?	
a. Qu'est-ce que la sécurité globale en entreprise ?	22
b. La cybersécurité	29
c. L'intelligence économique	33
d. La sureté des collaborateurs à l'étranger face au terrorisme	38
e. La santé et sécurité au travail	41
f. Quelle réponse des entreprises face aux situations de crise ?	46
3) Qu'est-ce que la culture de sécurité d'entreprise en France ?	
a. Définition du concept de culture	55
b. Définition du concept de culture nationale	58
c. Définition du concept de culture d'entreprise	60
d. Définition de la culture de sécurité d'entreprise	68

4) Hypothèse	
a. Méthodologie de travail	81
i. Le processus de recherche	81
ii. La démarche scientifique	81
iii. Méthodologie personnelle appliquée	84
b. La culture de sécurité des chefs d'entreprises n'est pas assez développée alors que celle-ci pourrait améliorer la gestion d'une situation d'exception	88
5) Axe 1 (Approche anthropologique) : L'acculturation des chefs d'entreprises de TPE et PME sur la sécurité globale	96
6) Axe 2 (Approche management) : L'intégration par les TPE et PME du management d'une situation d'exception et/ou de crise	104
Conclusion	113
Bibliographie	114
Annexes 1 à 6	120
Quelques citations...	138

Remerciements

Je tiens tout d'abord à remercier Madame Sophie CAZARD, Directrice de l'institut de Formation Sanitaire et Sociale de la Croix Rouge Occitanie qui m'a permis et facilité la reprise d'études supérieures en même temps de l'exercice de mon activité professionnelle.

J'adresse en suivant mes remerciements à l'Ecole Nationale Supérieure des Officiers de Sapeurs-Pompiers (ENSOSP) et l'Université Technologique de Troyes (UTT) qui ont retenu ma candidature et intégré au Master 2 en « Ingénierie et Management en Sécurité Globale Appliquée » (IMSGA) spécialité « management stratégique de situation de crise ». Je remercie tout particulièrement le Commandant Eric DUFES pour ses enseignements et son soutien lors de la constitution du dossier de financement et d'inscription au Master IMSGA ainsi qu'au Professeur Patrick LACLEMENCE et au Docteur Guillaume DELATOUR pour leurs enseignements et leur proximité bienveillante.

Mes remerciements s'adressent tout spécialement au Docteur Paul Henri RICHARD pour son accompagnement à la rédaction du présent mémoire avec tout le soutien technique et moral qu'il m'aura apporté.

Ces remerciements vont à mes collègues de travail qui m'ont encouragé dans mes études et pallié à mes absences, tout particulièrement Thierry FRECHAUD et Delphine BERTRAND, lors des périodes de cours à l'UTT et à l'ENSOSP.

Je n'oublie pas mes collègues et amis de promotion, Michael ADLER, Jean Philippe BORDELAIS, Guillaume BOUQUET, Max CHARREYRON, Eric CHATELON, Hicham CHOUKRI, Christophe DENISSAN, Alexandre DOUAY, Jean-Pierre LAMADE, Ramon NAVARRO, Soufian SAMGHOULI et Anthony VANDEN BERGHEIN pour leur bonne humeur, la qualité de nos échanges et relations fraternelles durant ces 18 mois.

Je remercie avec une affection toute spéciale, mon compagnon Benjamin pour sa patience et son soutien durant ma scolarité et plus particulièrement lors de la rédaction du présent mémoire. J'associe enfin à ces remerciements mes parents pour l'éducation qu'ils m'ont donné et l'esprit d'ouverture et de persévérance qu'ils m'ont inculqué.

Résumé

La France compte 140 000 TPE et PME générant 1300 milliards d'Euros de chiffre d'affaire et emplois 28% des salariés. Leur activité se trouve principalement dans le secondaire et le tertiaire. Elles se caractérisent un effectif de moins de 250 salariés et un chiffre d'affaire de moins de 50 M d'Euros.

Mondialisation des échanges, nouvelles technologies et géopolitique complexe, un réel paradigme de sécurité globale voit le jour depuis le début des années 1990. Il s'agit pour une Organisation, de placer tous les risques et menaces, quelle que soit leurs natures ou origines, au centre des préoccupations. Il convient ensuite de penser aux mesures de prévention et de protection, de continuité d'activité et de résilience, à mêmes de contrer toutes attaques.

Les entreprises sont soumises à des risques et menaces multiples et croissantes auxquels celles-ci doivent faire face sous peine de mettre en péril leur pérennité. Obligations de résultats en santé sécurité au travail, contexte terroriste, cyberattaques, concurrence agressive sont autant de dangers.

Evoluant dans un état d'équilibre précaire, les entreprises résolvent au quotidien des problèmes de sécurité globale. Les modifications profondes de cet équilibre peuvent provoquer une situation exceptionnelle. Rester dans une posture attentiste et refuser toute préparation, c'est prendre le risque de basculer dans une situation de crise. Il convient ainsi de développer une réelle stratégie de « management des situations de crise », incluse au projet d'entreprise.

Même si le chef d'entreprise est responsable de la sécurité, celle-ci est l'affaire de tous. Pour être appliquée, il convient de développer une culture de sécurité d'entreprise. Celle-ci représente l'ensemble des savoirs et des valeurs diffusés et partagés parmi les membres de l'organisation et traduits dans les pratiques de maîtrise des risques selon un niveau de priorité défini. Le premier concerné par cette acculturation est le dirigeant.

Cette culture n'est pas forcément innée et son acquisition peut être complexe. Ceci est d'autant plus vrai que les formations initiales des business school n'abordent pas ou très peu les problématiques de sécurité globales. Les actions de sensibilisation proposées par les organisations professionnelles ne sont suivies par les dirigeants qu'en cas de survenue d'un événement au sein de leurs structures ou en fonction de l'actualité. Leur préparation à la gestion de crise est quasi inexistante et selon les territoires, ces mêmes organisations apportent un soutien aux chefs d'entreprises.

Les dirigeants ont une vision de la sécurité globale et de la culture de sécurité en lien avec les définitions développées. Leur culture, acquise par l'expérience et la formation n'est pas innée. Des signes montrent l'intérêt porté par les dirigeants : thème abordé en CODIR, certifications, personne dédiée, actions de sensibilisation, évaluation. Toutefois ces actions restent ciblées sur la santé sécurité au travail (obligations de l'employeur) et la cybersécurité (occurrence des attaques). La majorité des situations rencontrées et jugées exceptionnelles par les chefs d'entreprises, n'ont eu que peu d'impact sur les organisations et gérées en grande partie en interne. Qu'en aurait-il été pour des situations plus complexes ? La majorité des dirigeants expriment un besoin en monté en compétences en interne pour une parfaite efficacité.

Abstract

France has 140,000 small businesses and SMEs generating 1300 billion euros in turnover and jobs 28% of employees. Their activity is mainly in the secondary and tertiary sectors. They are characterized by a workforce of less than 250 employees and a turnover of less than 50 million Euros.

Globalization of exchanges, new technologies and complex geopolitics, a real paradigm of global security has emerged since the early 1990s. It is an Organization, to place all risks and threats, whatever their natures or origins, at the center of concerns. Next, prevention, protection, business continuity and resilience measures should be considered to counter any attacks.

Companies are subject to multiple and growing risks and threats that they must face or risk jeopardizing their sustainability. Obligations of results in health and safety at work, terrorist context, cyberattacks, and aggressive competition are all dangers.

Evolving in a state of precarious balance, companies solve everyday problems of global security. The profound changes in this balance can cause an exceptional situation. Staying in a wait-and-see attitude and refusing any preparation means taking the risk of falling into a crisis situation. It is therefore necessary to develop a real strategy of "management of crisis situations", included in the business plan.

Even if the company manager is responsible for security, it is everyone's business. To be applied, it is necessary to develop a corporate safety culture. This represents all the knowledge and values disseminated and shared among the members of the organization and translated into risk management practices according to a defined priority level. The first concerned by this acculturation is the leader.

This culture is not necessarily innate and its acquisition can be complex. This is all the more true as initial business school training does not address or very little global security issues. The awareness-raising actions proposed by the professional organizations are only followed by the leaders in case of occurrence of an event within their structures or according to the news. Their preparation for crisis management is almost non-existent and depending on the territories, these same organizations provide support to business leaders.

Leaders have a vision of global security and safety culture in relation to the definitions developed. Their culture, acquired through experience and training is not innate. Signs show the interest of the leaders: theme addressed in CODIR, certifications, dedicated person, awareness actions, and evaluation. However, these actions remain focused on workplace health (employer obligations) and cybersecurity (occurrence of attacks). Most of the situations encountered and judged to be exceptional by business leaders have had little impact on organizations and are largely managed internally. What would it have been for more complex situations? The majority of executives express a need to build in-house skills for perfect efficiency.

La culture de sécurité des chefs d'entreprise au service de la gestion de crise...

Pour Jay Forrester l'entreprise est à considérer comme une organisation, une structure sociale et un centre de production et de profits. L'entreprise est un système complexe, s'adaptant en permanence, caractérisé par un ensemble d'hommes et d'un outil de production dont la finalité est de maximiser son profit. Elle a une dimension « intellectuelle » au travers de sa culture d'entreprise, en relation continue avec son écosystème. Des sous-systèmes quant à eux regroupent les flux réels (matières premières, personnes...), les flux financiers (entrées et sorties) et l'information, non isolés les uns des autres, et intégrant eux-mêmes des sous-systèmes... Cette organisation peut s'apparenter à un comportement d'organisme vivant ; La cellule, le tissu, l'organe, l'appareil, l'organisme. Ainsi chacune de ses fonctions vitales sont rattachées des sous fonctions contribuant à la bonne marche des premières. Un organisme vivant peut-être étudié de façon multiple dont son métabolisme, sa physiologie, son anatomie... et sur une échelle pouvant aller jusqu'à l'infiniment petit. Enfin, toute vie est soumise à attaques de divers éléments pathogènes de types virus, bactéries, parasites... L'entreprise peut subir des agressions, sources de vulnérabilité, pouvant affecter directement son fonctionnement et sa pérennité, au-delà des risques courants (défaut de paiement d'un client, retard sur les approvisionnements de matières premières, besoin en trésorerie à court terme...). Cette vulnérabilité se caractérise par deux paramètres : l'objet du risque (humain, technique, information, partenaire, financier) et l'impact potentiel (perte financière, perte de l'outil de production, perte humaine, perte d'image, perte de notoriété...). Peu importe le type de péril et ses origines, accident, malveillance, attaque... seul compte les effets, leurs impacts sur les centres de gravité (ressources, moyens, matériels, capacités, situation) dont l'entreprise tire son aptitude à atteindre ses objectifs. Les conséquences sont diverses et concernent les dommages subis directement par l'organisation, et ceux subits par des tiers et par l'environnement. Enfin, une atteinte à l'image et à la réputation peut nuire durablement voir définitivement à l'entreprise. Il s'agit alors de mettre en place une prophylaxie (préparation, gestion courante et événements graves, évitement de crise) et si nécessaire des traitements (gestion de crise) afin d'assurer une sécurité globale, dont la responsabilité incombe au chef d'entreprise. Toutefois, la sécurité est ce vivre sans accident grave, sans incidents ou suivre des procédures optimales ?

Adapter les valeurs ou changer les comportements sont deux approches sur la façon de progresser grâce à la culture de sécurité des entreprises. Les comportements désirés sont le suivi des procédures et l'observance de bonnes pratiques. Les valeurs sont l'engagement du management, la transparence et l'évitement d'une culture du blâme. Les approches historiques introduiraient la culture de sécurité comme l'optimisation finale après avoir utilisé les solutions techniques et organisationnelles, c'est-à-dire, les plus cartésiennes. L'International Nuclear Safety Group (INSAG), juste après la catastrophe de Tchernobyl, y voyait un système de valeurs tacites partagées à l'intérieur de l'entreprise pour lui donner une force ajoutée, une cohérence et une résistance collective aux accidents, sans nécessairement y voir une traduction visible à tous les instants, particulièrement en termes de comportements idéaux. Si l'on continue dans la métaphore sur les organismes vivants,

une bonne culture de sécurité confèrerait un corps sain plus robuste aux maladies, mais pas la suppression des maladies.

Nous pouvons dire qu'il n'existe pas d'entreprise sans culture. La question est quelle culture est désirable ? L'entreprise peut mourir de plusieurs causes dont une mauvaise sécurité (cyberattaque, vols de données commerciales ou de secret de production, décès d'un salarié dans un accident du travail...). La dimension culturelle ou valeurs partagées, serait un facteur favorable permettant à l'entreprise de traverser avec succès des crises là où d'autres auraient disparues et ce par une forte culture au changement et/ou à l'adaptation.

Dans le triangle que l'on retrouve communément, entre cultures de changement (flexibilité), de production (performance et qualité... du produit), et de sécurité (transparence, signalement, observance), l'entreprise ajuste en continue le curseur en fonction du contexte dans lequel elle se situe à un instant T. Cet ajustement ne positionne que rarement le curseur sur la sécurité (sauf évènement récent) au profit de la production, du cash-flow, du management... Mais cet état de fait n'est-il pas une vue réductrice venant rendre encore plus fragile l'entreprise dans son écosystème ? La culture de l'entreprise ne doit-elle pas parfois donner la priorité à la sécurité plutôt qu'à des dimensions et valeurs différentes de celles prônées par la culture de sécurité ?

L'objet du présent mémoire s'intéressera à répondre à la question « En quoi la culture de sécurité des chefs d'entreprises contribue-t-elle à la gestion d'une situation d'exception ? ». Pour cela, la première partie se consacrera à connaître ce que sont les très petites, petites et moyennes entreprises (TPE et PME) afin de cerner leurs caractéristiques (économique, commerciale, ressources humaines) avec leurs forces mais aussi leur(s) vulnérabilité(s). En second lieu, nous nous intéresserons au concept de sécurité global avec sa ou ses définition(s) adaptée au monde de l'entreprise. Dans la continuité un focus sera réalisé sur 4 domaines contemporains retenus par l'auteur en termes de problématiques de sécurité et les enjeux induits : cybersécurité, intelligence économique, sureté des collaborateurs à l'étranger face au terrorisme et santé sécurité au travail. Enfin, nous verrons des éléments de réponses sur l'organisation des entreprises pour faire face à une situation de crise, du concept théorique à des applications pratiques. Le troisième et dernier point abordé de cette première partie étudiera le concept de culture de sécurité d'entreprise en partant de la définition la plus générale, la culture, puis la culture nationale et la culture d'entreprise. Cette étude de l'art réalisée, la deuxième partie soumettra à recherche l'hypothèse comme quoi la culture de sécurité des chefs d'entreprises n'est pas assez développée alors que celle-ci pourrait améliorer la gestion d'une situation d'exception grâce à un travail de pré enquête. Enfin, l'enquête menée auprès de TPE et PME, permettra d'approfondir cette hypothèse au travers de deux axes d'approche ; l'un portera sur une approche anthropologique avec l'acculturation des chefs d'entreprises de TPE et de PME sur la sécurité globale et sur une approche managériale avec l'intégration par ces mêmes organisations, du management d'une situation d'exception et/ou de crise.

Cette étude a été choisie car faisant l'objet d'enjeux forts pour les entreprises quant à leur pérennité d'abord et en tant que levier de développement. Ce mémoire se voudrait incitatif dans sa lecture à une prise de conscience pour les chefs d'entreprises sur la nécessité de prendre en compte la sécurité dans une approche globale pour leurs entités et pour ceux engagés dans une démarche « sécurité », de conforter le bien fondé de celle-ci.

1) Visiographie des Petites et Moyennes Entreprises en France : Qui sont nos TPE ET PME

A l'instar du psychiatre qui étudie l'anatomie et la physiologie de l'être humain avant d'étudier son psychisme, nous nous intéresserons aux éléments « organiques » des entreprises françaises. Ce chapitre a pour prétention de donner au lecteur les connaissances générales sur les caractéristiques des TPE et PME avant de s'intéresser à leur « esprit ». Ici seule l'approche culturelle sera étudiée et plus spécifiquement la culture de sécurité.

a. Qu'est-ce qu'une Petite et Moyenne Entreprise ?

L'article 51 de la loi n°2008-776 du 4 août 2008 de modernisation de l'économie (LME) introduit un **classement des entreprises** en quatre catégories pour les besoins de l'analyse statistique et économique du tissu productif : les micros entreprises, les petites et moyennes entreprises (PME), les entreprises de taille intermédiaire (ETI) et les grandes entreprises (GE).

Sur cette base, l'Institut National de la Statistique et des Etudes Economiques (INSEE), définit le terme **PME** par la catégorie **d'entreprises qui occupent moins de 250 personnes, et qui ont un chiffre d'affaire annuel de moins de 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros.**

En France, la grande majorité des entreprises appartiennent à la catégorie des PME (Le144-coworking.fr).

Cette catégorie d'entreprises est définie par le décret d'application (**Décret n° 2008-1354 du 18 décembre 2008** relatif aux critères permettant de déterminer la catégorie d'appartenance d'une entreprise pour les besoins de l'analyse statistique et économique) de **l'article 51** de la loi de modernisation de l'économie, relatif aux **critères permettant de déterminer la catégorie d'appartenance d'une entreprise** pour les besoins de l'analyse statistique et économique.

Cette définition nécessite de connaître les valeurs de trois variables (effectif, chiffre d'affaires, total de bilan) pour les entreprises (définies par l'article 1er du décret, ce qui inclut les « entreprises profilées »), et sera mise en place progressivement dans les statistiques d'entreprises. Comme indiqué dans l'article 4 du décret, une définition permettant une bonne approximation de la catégorie peut être retenue, et doit être alors jointe aux données publiées.

Décret n°2008-1354 article 3 :

La catégorie des micros entreprises est constituée des entreprises qui :

- d'une part occupent moins de 10 personnes ;
- d'autre part ont un chiffre d'affaires annuel ou un total de bilan n'excédant pas 2 millions d'euros.

La catégorie des petites et moyennes entreprises (PME) est constituée des entreprises qui :

- d'une part occupent moins de 250 personnes ;
- d'autre part ont un chiffre d'affaires annuel n'excédant pas 50 millions d'euros ou un total de bilan n'excédant pas 43 millions d'euros.

Ces critères valent pour la France et diffèrent sensiblement selon les pays. Si le terme de micro-entreprise (moins de 10 salariés) est encore employé dans l'Hexagone, cette catégorie d'entreprises est de plus en plus rattachée à la catégorie des PME (Journal du net, juillet 2017).

Chiffre d'affaires	Total bilan	Effectif			5 000 salariés et plus
		Moins de 10 salariés	De 10 à 249 salariés	De 250 à 4 999 salariés	
2 M€ au plus	2 M€ au plus	Microentreprises (MIC)	Petites et moyennes entreprises (PME)	Entreprises de taille intermédiaire (ETI)	Grandes entreprises (GE)
Plus de 2 M€ à 50 M€ inclus	2 M€ au plus				
Plus de 50 M€ à 1,5 Md€ inclus	2 M€ au plus	MIC			
	Plus de 2 M€ à 43 M€ inclus				
Plus de 1,5 Md€	Plus de 43 M€				
	2 M€ au plus	MIC	PME		
	Plus de 2 M€ à 43 M€ inclus				
	Plus de 43 M€ à 2 Md€ inclus				
	Plus de 2 Md€				

Source : France stratégie.

Nous trouvons dans le Centre de Documentation Economie-Finances (CDEF), qu'en matière de législation européenne, la notion d'entreprise utilisée pour l'application de l'article 51 de la loi de modernisation de l'économie est celle du règlement (CEE) n° 696/93 du Conseil du 15 mars 1993.

Par ailleurs, le **décret 2008-1354 est rédigé au vu de la recommandation de la Commission européenne n° 2003/361/CE du 6 mai 2003 concernant la définition des micros, petites et moyennes entreprises**. La Commission européenne propose une rubrique complète sur la définition d'une PME du guide de l'utilisateur pour la définition des PME daté du 1er mars 2016.

Enfin, la notion de PME apparaît dans le cadre des marchés publics et la réglementation applicable à la commande publique. **Les PME sont définies au sens du code des marchés publics et notamment le II de son article 48** : « Dans l'avis d'appel public à la concurrence ou dans les documents de la consultation, le pouvoir adjudicateur peut demander aux candidats d'indiquer dans leur offre la part du marché qu'ils ont l'intention de sous-traiter à des tiers, notamment à des petites et moyennes entreprises telles que définies par l'article 8 de l'ordonnance n° 2004-559 du 17 juin 2004 sur les contrats de partenariat, ou à des artisans » (Annexe au décret n° 2006-975 du 1er août 2006 portant code des marchés publics).

D'autres références sont données dans le cadre de la commande publique :

- de l'article L. 1414-9 du code général des collectivités territoriales
- de l'article 8 de l'[ordonnance n° 2004-559 du 17 juin 2004](#)
- du [décret n° 2005-1308 du 20 octobre 2005](#)
- du [décret n° 2005-1742 du 30 décembre 2005](#)

b. Quel panorama des TPE et PME en France ?

i. Les caractéristiques générales des entreprises françaises

En 2013, on dénombre **3,75 millions d'entreprises dans les secteurs marchands non agricoles**, dont 3,66 millions correspondent à une seule unité légale indépendante (Unité organisationnelle de production de biens et de services et jouissant d'une certaine autonomie de décision).

En 2013, 274 grandes entreprises (GE) et 5 300 ETI sont présentes sur le territoire français, aux côtés de **140 000 PME**, et **3,6 millions de micro entreprises (MIC)**. Ainsi, les entreprises œuvrant en France relève du statut de **PME soit 3.7% des entreprises** (Rapport PME 2016).

Sur ces 3,75 millions d'entreprises, les grandes entreprises (GE) emploient 4,33 millions de salariés (2013), soit 29 % du total. À l'opposé les **3,61 millions de micros entreprises (96%) qui emploient environ 2,81 millions de salariés (19 % du total)**. Par-delà ce dualisme se dessine une partition assez équilibrée de la valeur ajoutée ou de l'emploi : les entreprises de taille intermédiaire (ETI) et **les petites et moyennes entreprises (PME) emploient respectivement 24 % et 28 % des salariés.**

Le secteur le plus concentré est celui des activités financières et assurances. 26 grandes entreprises y emploient 79 % des salariés. Dans l'industrie, 83 grandes entreprises et 1 630 ETI emploient toutes deux 33 % des salariés. Dans l'information-communication, une vingtaine de grandes entreprises et 260 ETI emploient respectivement 40 % et 27 % des salariés. Les différentes catégories d'entreprises ont un poids proche de la moyenne dans les activités du commerce, des transports, de l'hébergement et restauration. En effet, ces activités sont marquées par une grande diversité d'acteurs, des grandes entreprises internationalisées jusqu'aux micros entreprises qui desservent un marché de proximité. **La majorité des salariés des PME et micro entreprises sont dans les services destinés aux particuliers** (enseignement, santé, action sociale, autres services), **ainsi que les activités spécialisées scientifiques et techniques** (qui incluent notamment les professions libérales). **Dans la construction**, en dépit de la présence d'une dizaine de grandes entreprises, **70 % des salariés sont employés dans des PME et micro entreprises.**

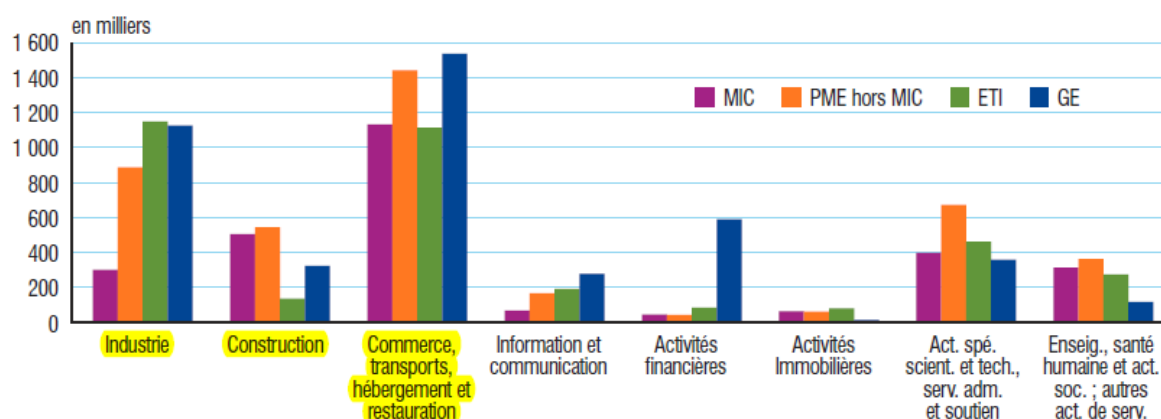
Après trois ans d'atonie de la croissance, **l'activité des entreprises en 2015 marque le retour d'une activité plus dynamique en France, avec une croissance du PIB de 1,2 %**, après + 0,7 % en 2014 et + 0,6 % en 2013.

Principales caractéristiques des entreprises par catégorie en 2013

	GE	ETI	PME hors MIC	MIC	Ensemble
Entreprises y compris activités financières et assurances					
Nombre d'entreprises	274	5 322	138 117	3 606 741	3 750 454
Nombre unités légales France	26 008	46 157	236 728	3 627 893	3 936 786
Effectif salarié au 31/12 (en milliers)	4 333	3 473	4 169	2 808	14 782
Effectif salarié ETP (en milliers)	4 022	3 185	3 715	2 487	13 408
Entreprises hors activités financières et assurances					
Nombre d'entreprises	248	5 121	136 468	3 553 923	3 695 760
Nbre d'unités légales situées en France	16 943	45 150	233 490	3 573 915	3 869 498
Effectif salarié au 31/12 (en milliers)	3 743	3 392	4 129	2 767	14 032
Effectif salarié ETP (en milliers)	3 467	3 110	3 678	2 450	12 706
Chiffre d'affaires (en milliards d'euros)	1 325	1 093	815	548	3 781
Chiffre d'affaires à l'export (en Md euros)	315	211	81	19	627
Valeur ajoutée hors taxes (en Md euros)	337	252	240	216	1 046

Sources : Insee, É sane, Clap, Lifi 2013.

Effectifs au 31/12 selon le secteur d'activité et la catégorie d'entreprise en 2013



Champ : France, secteurs marchands non agricoles.

Source : Insee, É sane, Clap, Lifi 2013.

Les entreprises en France sont concentrées pour plus de la moitié d'entre elles dans cinq régions : Île-de-France (26 %), Rhône-Alpes (10 %), Provence-Alpes Côte d'Azur (7 %), Pays de la Loire (6 %) et Nord-Pas-de-Calais (6 %) (Source INSEE, 2010).

ii. L'identité des TPE et PME en France

En 2013, on compte en France 136 500 PME soit 3,7% des entreprises toutes catégories confondues. Elles emploient **4,13 millions de salariés** et réalisent **23 % de la valeur ajoutée des entreprises**. Les PME comptent en **moyenne 27 salariés**. 60 % ont moins de 20 salariés et 12 % seulement atteignent ou dépassent 50 salariés. **Les activités qu'elles exercent sont plus diversifiées que pour les autres catégories d'entreprise.**

Les PME sont surreprésentées dans la construction, les industries de type traditionnel (textile, bois, papier et imprimerie, métallurgie, industries extractives). Dans les services, elles le sont dans l'hébergement et la restauration, l'enseignement marchand, l'hébergement médico-social et l'action sociale. Elles sont également surreprésentées dans plusieurs activités qualifiées. Ainsi, les PME emploient **38 % des salariés des activités scientifiques et techniques** soit plus que chacune des autres catégories. À un niveau plus fin, elles emploient **40 % des salariés des activités juridiques et comptables**. Les PME de l'industrie emploient en moyenne un peu plus de salariés que les autres catégories, avec **33 équivalent temps plein (ETP) en moyenne**.

Ratio sur les PME par secteur d'activité, 2013

NAF rév. 2, niveau A10	En entreprise Milliers	Effectif salarié au 31/12 Milliers	Effectif salarié ETP Nombre moyen	Valeur ajoutée HT par salarié k€	Immobilisations corporelles par salarié k€	Total des ressources par salarié k€	Salaire annuel moyen k€	Taux de marge EBE/VA HT %
Industries manufacturière, extractives et autres <i>dont Industrie manufacturière</i>	25 23	887 844	33 33	64 62	105 80	214 187	35 35	17,9 15,8
Construction	23	544	22	61	48	191	34	14,0
Commerce de gros et de détail, transports, hébergement et restauration	50	1 444	25	60	69	209	33	19,1
Information et communication	5	164	31	91	46	236	51	17,9
Activités spécialisées, scientifiques et techniques, services administratifs et de soutien	21	672	27	71	53	273	43	15,9
Enseignement, santé humaine et action sociale	6	257	33	57	35	92	35	14,6
Autres activités de services	3	102	27	49	68	138	34	11,4
Total PME non microentreprise	134	4 070	27	64	69	210	36	17,2

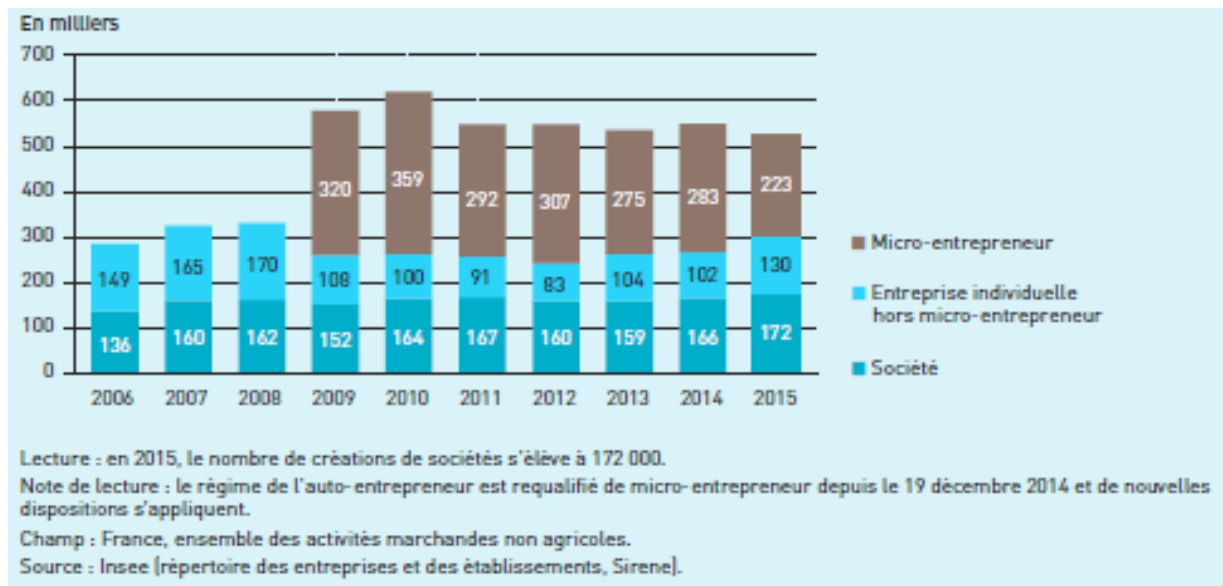
Note de lecture : l'effectif salarié est calculé, soit au 31 décembre de l'année observée, soit en équivalent temps plein (ETP).

Champ : France, PME non microentreprises du secteur marchand, hors activités agricoles, immobilières, financières et d'assurance et hors Administrations publiques.

Source : Insee (Ésane, Clap et Lifi, 2013).

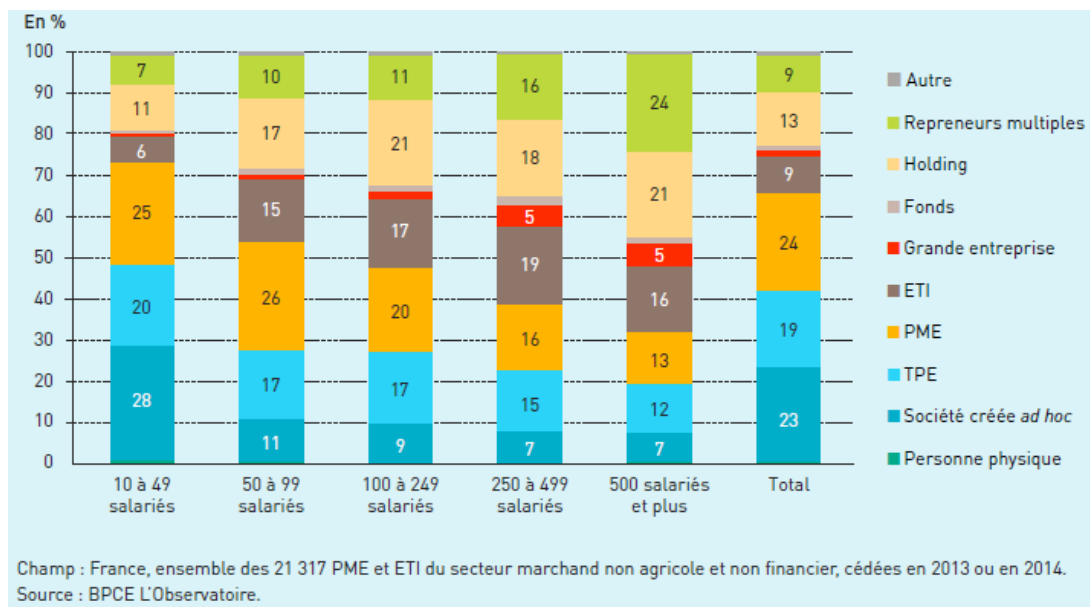
En 2015, **525 100 entreprises** ont été créées en France. On constate toutefois une **baisse de 5% par rapport à 2014** qui résulte du net **repli des immatriculations de micro-entrepreneurs** (- 21 % par rapport à 2014). En revanche, les **autres créations d'entreprises augmentent fortement (+ 13 %)**, particulièrement celles des autres **entreprises individuelles (+ 28 %)** et, dans une moindre mesure, celles des **sociétés (+ 4 %)**. Tous secteurs et tous types d'entreprises confondus, les créations diminuent dans presque toutes les régions. Hors micro-entrepreneurs, seules **8 % des entreprises sont employeuses à la création**. Elles **démarrent** alors en **moyenne avec 2,5 salariés**. Pour les créateurs individuels, **l'âge moyen se maintient à 38 ans** et la part des femmes atteint 40 %. Les entreprises créées, hors régime de l'auto-entrepreneur, l'ont été le plus souvent **par des salariés du secteur privé et des chômeurs**.

Evolution du nombre de création d'entreprises, 2006-2015



En moyenne, **7,4% des PME et ETI sont cédées chaque année en France** ce qui représente pour l'année 2014, 15 364 structures avec un recul d'un millier d'entreprises cédées par rapport à l'année précédente. Plus d'un tiers des opérations sont réalisées après le **60^{ème} anniversaire du cédant**. Les successions familiales représentent **17%** des actes de cession, **40%** par vente directe et **37%** par échanges de titres.

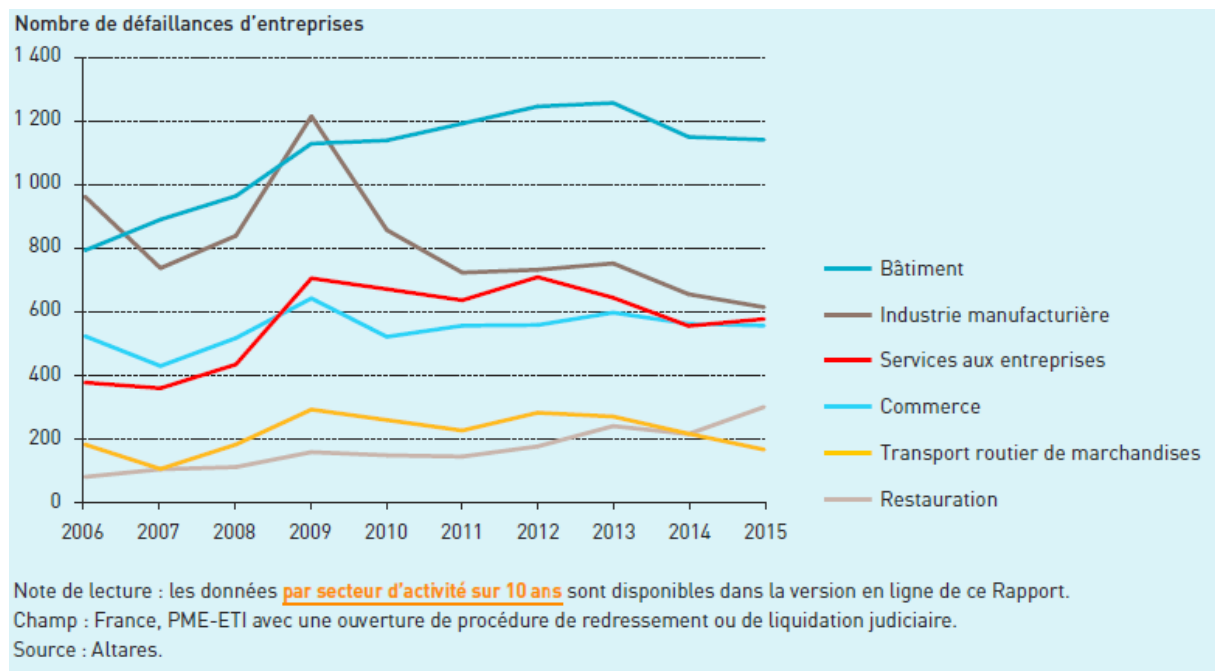
Répartition des cessions-transmissions de PME-ETI selon la taille d'entreprise cédée et le type de repreneur, moyenne 2013-2014



Depuis 2009, le nombre d'entreprises défaillantes reste bloqué au-dessus des 60 000. Les procédures collectives de 2015, menacent 235 000 emplois directs. Celles-ci concernent **4 549 PME-ETI** ce qui représente le meilleur chiffre depuis les 7 dernières années. Les PME résistent mieux dans un contexte économique difficile avec **4 510** défaillances. Les PME-ETI

représentent désormais **7,2 % de l'ensemble des défaillances**. L'analyse des cessations de paiement par tranche de chiffre d'affaires (CA) confirme que **les plus jeunes entreprises (- de 5 ans) développant un CA inférieur à 1 M€ enregistrent sont les plus fragiles**. La plupart des jugements, soit 4 139, sont portés sur des procédures de redressement ou de liquidation judiciaire. Si le nombre de **redressements judiciaires recule de 6 %** à 2 253, celui des **liquidations judiciaires augmente dans les mêmes proportions** à 1 886. **Les PME-ETI se présentent toutefois devant le tribunal avec davantage d'anticipation** permettant de maintenir le taux de liquidations directes sous les 42 %. C'est donc majoritairement **une solution de rebond qui est privilégiée par les juges pour cette catégorie de sociétés**, soit au travers d'une sauvegarde (9 % des procédures), soit par redressement (49,5 %).

Evolution des cessations de paiement des PME-ETI par secteur d'activité, 2006-2015



En 2015, le chiffre d'affaires des PME progresse de 1,7 %, marquant la fin de la décélération initiée en 2012. **Cette croissance résulte en grande partie de la reprise dans le Commerce** qui réalise près de la moitié de l'activité et dont les **ventes augmentent de 1,4 %** en 2015, après avoir stagné en 2014 (+ 0,1 %). Le secteur du commerce est principalement responsable de cette évolution alors que le **bâtiment enregistre une baisse de -0,9%**.

En conséquence, **la valeur ajoutée des PME progresse de 2 % sur l'année**, après 1,9 % en 2014, retrouvant ainsi sa croissance de 2012. Là aussi, le secteur du commerce apporte la plus forte contribution.

Le dynamisme de la valeur ajoutée a permis aux PME dans leur ensemble de disposer d'un excédent brut d'exploitation (EBE) en progression de 2,4 % en 2015.

Chiffre d'affaire et valeur ajoutée des PME, 2012-2015

En%	Chiffre d'affaires total					Valeur ajoutée				
	Répartition	Variation annuelle				Répartition	Variation annuelle			
		2015	2012	2013	2014		2015	2015	2012	2013
Total PME	100,0	2,8	1,8	1,1	1,7	100,0	2,0	1,6	1,9	2,0
<i>dont principaux secteurs :</i>										
- Industrie manufacturière	18,3	2,3	1,1	1,8	1,8	21,1	1,5	0,7	2,2	1,9
- Construction	10,9	2,3	1,1	0,3	- 0,9	14,0	0,9	0,6	0,0	- 0,9
- Commerce	47,5	2,7	1,7	0,1	1,4	27,1	1,3	1,2	1,5	1,9
- Transports et entreposage	4,2	2,9	1,9	2,4	2,2	5,4	1,7	2,8	3,8	3,3
- Soutien aux entreprises	7,8	4,1	3,1	3,2	4,5	12,7	3,5	3,0	2,7	3,8

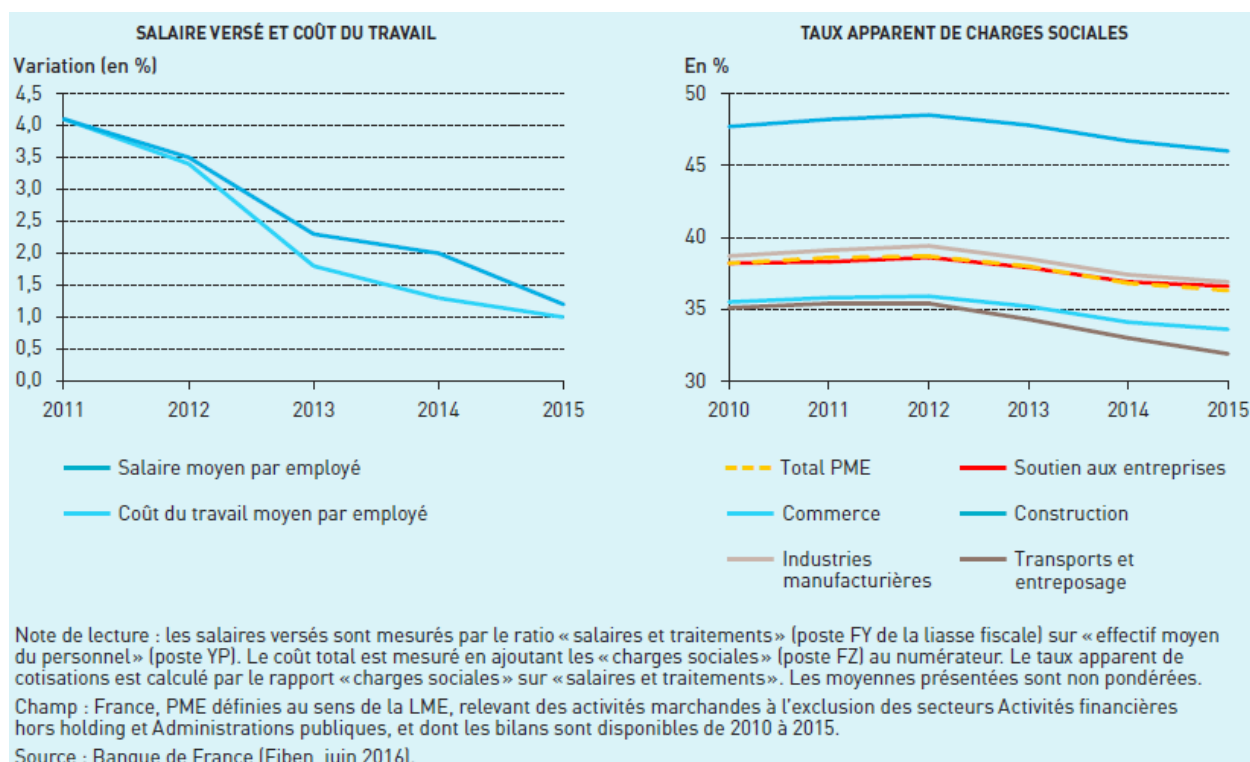
Note de lecture : les variations sont calculées sur un **échantillon de PME** dont les bilans sont présents dans Fiben pour deux exercices consécutifs (population cylindrée). Les entrées et sorties de l'échantillon dues à des absorptions, des défaillances ou des créations d'entreprises ne sont donc pas prises en compte. La taille et le secteur retenus sont ceux de l'année n-1, quelle que soit la situation de l'entreprise en année n.

Champ : France, PME définies au sens de la LME, relevant des activités marchandes à l'exclusion des secteurs Activités financières hors holding et Administrations publiques.

Source : Banque de France (Fiben, juin 2016).

En revanche, **les charges de personnel augmentent de 2,3 % sur 2015, mais cette hausse est contenue** notamment **par les effets du CICE**. Après un taux de croissance de 4,1 % en 2011, **le coût moyen du travail a fortement décéléré sur les cinq dernières années**.

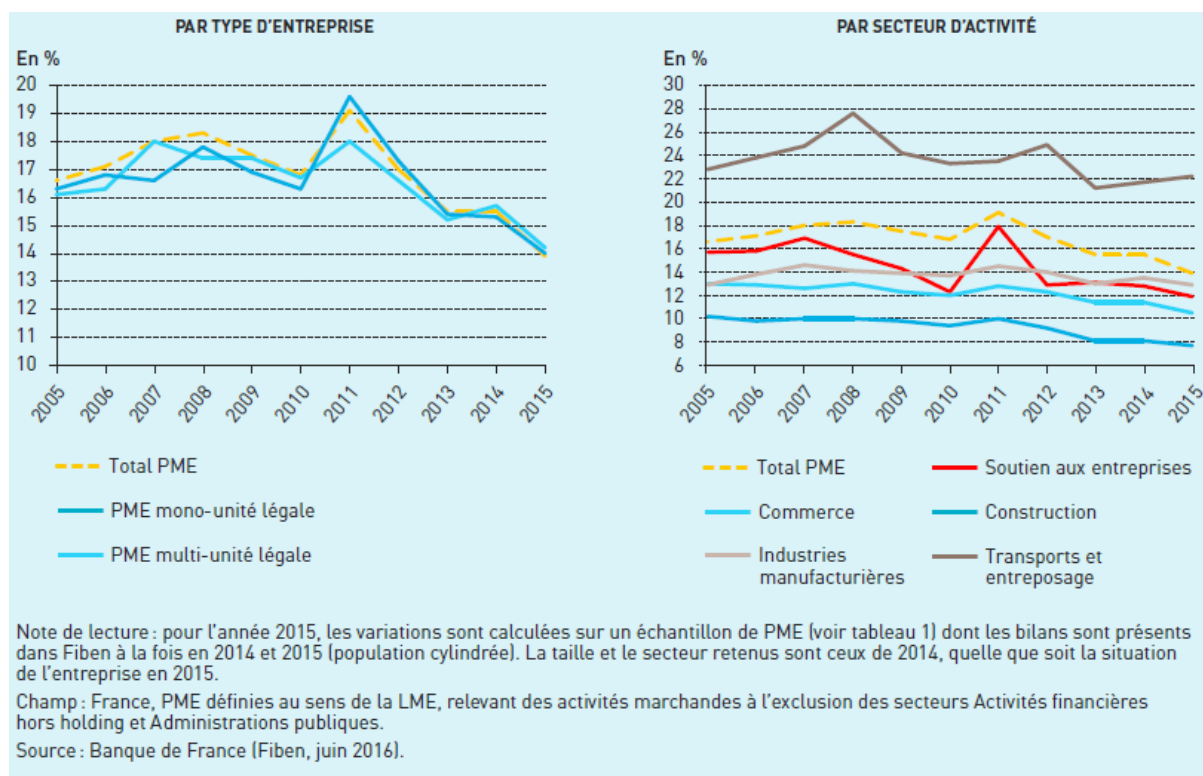
Coût Moyen du travail dans les PME



Après une diminution moins marquée en 2014, **l'investissement se contracte fortement de 6,8 % en 2015**, enregistrant une quatrième année consécutive de baisse. Alors que l'excédent brut d'exploitation et le taux de marge sont mieux orientés depuis deux ans, **cette nouvelle dégradation traduit une attitude encore attentiste de la part des entreprises**. La grande majorité des PME n'investit pas ou très peu. Parmi les PME avec une valeur ajoutée

positive, les trois quarts ont réalisé un investissement inférieur à 10 % de leur valeur ajoutée en 2015. Seules 13 % ont un taux d'investissement dynamique, supérieur à 20 %.

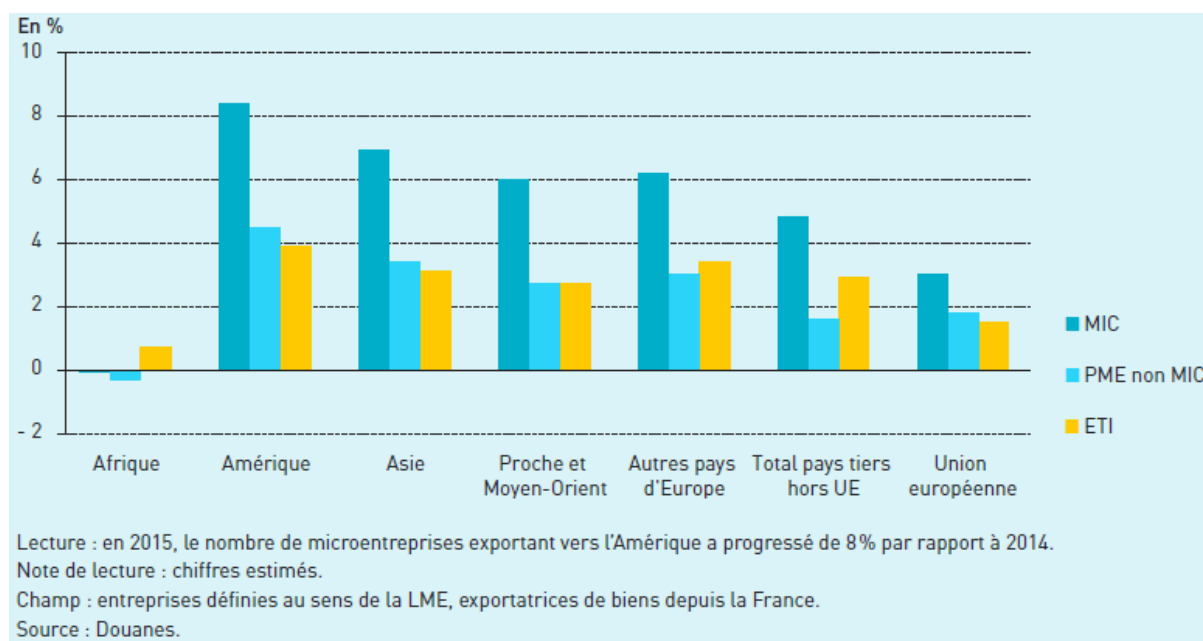
Taux d'investissement des PME, 2005-2015



En 2015, le nombre de **PME exportatrices** de biens depuis la France s'élève à 42 510. Leur **nombre et leur montant de vente à l'export augmentent sensiblement** de 3,2%. Le nombre de PME exportatrices croît de 1,8 % et leurs exportations de 3,1 %. Elles comptent alors pour 39 % des entreprises exportatrices et 12 % des exportations en valeur. **Les exportations des PME progressent fortement vers l'Amérique (+ 9 %), bénéficiant de la dépréciation de l'euro** par rapport au dollar. Pour les PME, la principale hausse vers les États-Unis concerne les ventes d'œuvre d'art. **Les ventes des PME s'améliorent en Asie (+ 5 %) et en UE (+ 3 %), mais diminuent légèrement vers l'Afrique (- 0,5 %) sous l'effet de du recul des ventes de céréales vers l'Algérie et le Maroc**, premiers débouchés pour les céréaliers français. **Ces hausses touchent aussi le Proche et Moyen Orient mais se rétractent vers l'Europe hors UE** particulièrement à cause du recul des échanges avec la Russie. La baisse pour les PME est de -38% mais compensée par une hausse des ventes vers la Suisse (+6%). **Le nombre de PME est croissant pour l'exportation vers toutes les zones du globe à l'exception de l'Afrique.** Dans l'industrie manufacturière, **les PME ne réalisent que 9 % du chiffre d'affaires exporté**, contre 37 % pour les ETI et 54 % pour les grandes entreprises. Les grandes entreprises et ETI de l'industrie exportent pratiquement toutes. **Les PME manufacturières sont encore 57 % à exporter, pour un quart en moyenne de leur chiffre d'affaires.**

Enfin, le **déploiement multinational des PME est très faible** : 4 % sont sous le contrôle de groupes étrangers, et 2 % seulement sont sous contrôle français et possèdent des filiales à l'étranger.

Evolution du nombre d'entreprises exportatrices par zone géographique d'export et catégorie d'entreprise, 2015



La part des PME dans la commande publique en 2014 fait l'objet un double mouvement. D'une part, le maintien de leur part relative en nombre de contrats à 57,5 % et d'autre part, la hausse relative en valeur de leur part dans le total de la commande publique, à 30,4 %, contre 27,2 % en 2013. 30 % des marchés publics initiaux ont été attribués à des PME en 2014, un montant en progression alors que la tendance générale est à la baisse pour 2015 avec -10,1%.

Répartition des marchés publics par catégories d'acheteur public et d'entreprise titulaire, 2014

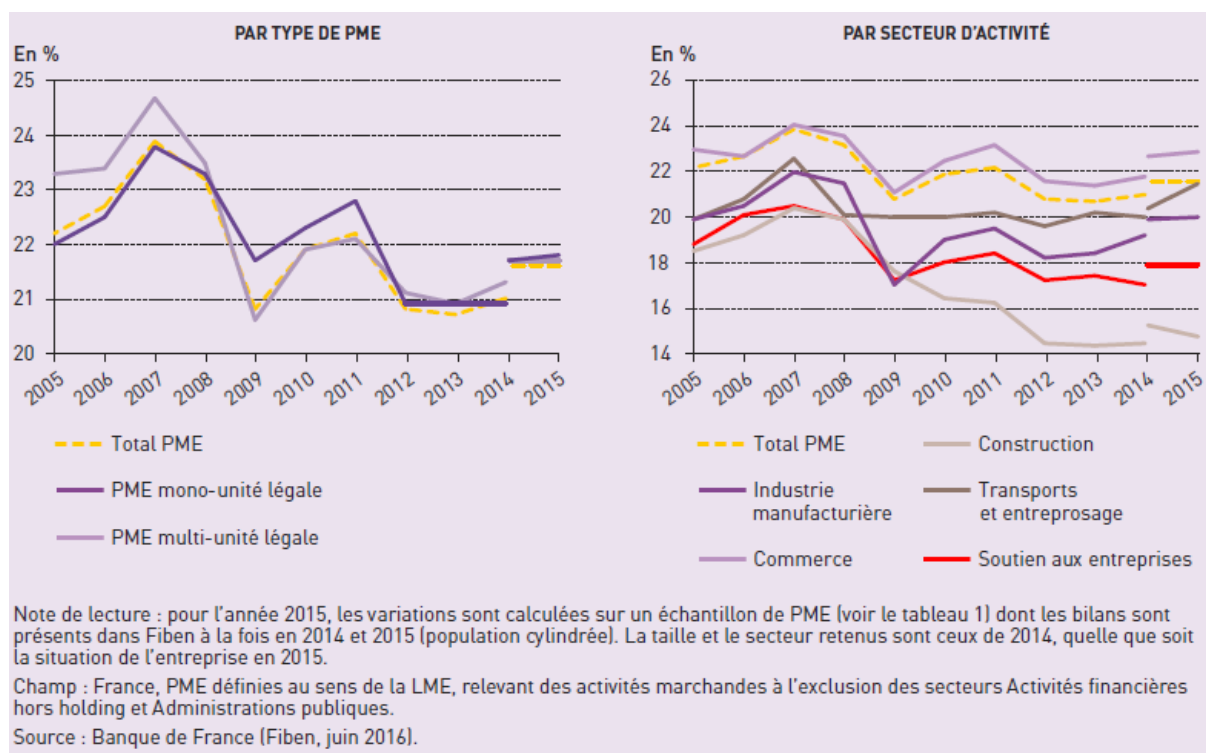
Acheteur public	PME		ETI		GE		Total entreprise	
	Contrat Nombre	Montant M€ HT	Contrat Nombre	Montant M€ HT	Contrat Nombre	Montant M€ HT	Contrat Nombre	Montant M€ HT
État	9 339	4 757	4 475	6 348	4 391	11 004	18 205	22 109
%	51,3	21,5	24,6	28,7	24,1	49,8	100,0	100,0
Collectivité territoriale	30 983	11 269	9 457	6 171	7 969	8 298	48 409	25 738
%	64,0	43,8	19,5	24,0	16,5	32,2	100,0	100,0
Opérateur de réseaux	5 444	3 580	2 888	4 305	4 658	8 743	12 990	16 628
%	41,9	21,5	22,2	25,9	35,9	52,6	100,0	100,0
Total	45 766	19 606	16 820	16 824	17 018	28 045	79 604	64 475
%	57,5	30,4	21,1	26,1	21,4	43,5	100,0	100,0

Lecture : en 2014, l'État a attribué 9 339 contrats à des PME, soit 51,3% des marchés publics qu'il a notifiés dans l'année.
 Champ : France, entreprises titulaires d'au moins une notification de marché public dans l'année, dont la catégorie d'entreprise au sens de la LME est connue.
 Source : OCEP (recensement).

Le Besoin en Fond de Roulement (BFR) agrégé des PME est structurellement positif, mais son poids décroît progressivement, traduisant des progrès dans la maîtrise des délais de paiement et dans la gestion des stocks. En 2015, le rythme de croissance du BFRE des PME ralentit. Il ne progresse que de + 2,0 %, contre + 3,4 % en 2014. Il masque cependant une

forte disparité sectorielle. Les délais de paiement des clients des PME est de 43 jours et leurs délais de règlement fournisseur de 49 jours. Cette amélioration des délais de paiement n'allège toutefois pas leur trésorerie. Le décalage en les décaissements et encaissements (solde commercial) est estimé à 11,5 jours de CA en 2015. **Le taux de marge demeure stable entre 2014 et 2015 et s'établit à 21,6 %** mais disparate selon les secteurs d'activité ; moindre pour le bâtiment et plus élevé pour le transport et l'entreposage. **Fin 2015, la structure financière des PME se renforce encore avec des capitaux propres représentant désormais 42 % des ressources mobilisées. L'augmentation des fonds propres, de + 6,7 % par rapport à 2014, est liée à une progression significative du résultat net (+ 7,6 % par rapport à l'année précédente), et à une baisse de la rémunération des actionnaires.** Les PME ont un **poids de l'endettement bancaire supérieur à un an en recul et stable pour les concours bancaire à court terme.** Depuis 2012, la tendance est au désendettement pour les PME. La réduction concerne principalement l'endettement bancaire et notamment l'endettement à moyen-long terme qui recule sur les trois derniers exercices. **Cette réduction est à rapprocher de la baisse du taux d'investissement sur la période (17 % en 2012 contre 14 % en 2015).** Les PME ont ainsi réduit leurs investissements sur les dernières années et amorti leur endettement à moyen-long terme.

Taux de marge des PME, 2005-2015



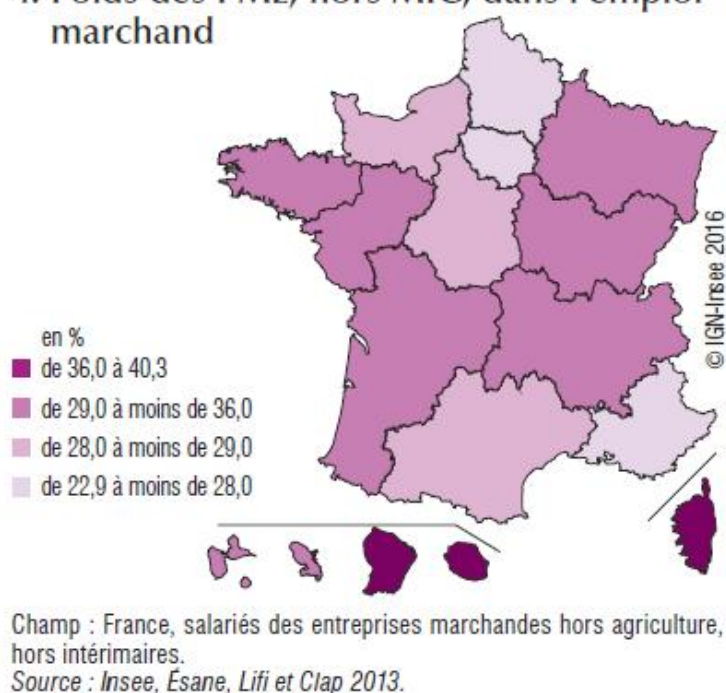
Le profil moyen des PME en 2015 est de 5 M€ de chiffre d'affaires pour un effectif de 21 salariés¹.

¹ « PME 2016 : Rapport annuel sur l'évolution des PME ». Observatoire des PME. Editeur Bpifrance – 2016. ISBN : 979-10-94762-02-8

iii. Les caractéristiques régionales des TPE et PME

Les petites et moyennes entreprises **emploient 28 % des salariés, assez équitablement répartis en province**. Cette catégorie d'entreprise correspond essentiellement à une **demande locale** comme la construction, le commerce de gros, les services juridiques et comptables, qui pèsent d'autant plus que les territoires sont peu tournés vers l'extérieur. Les PME sont également **fortement implantées dans certains secteurs industriels** comme par exemple la **fabrication de produits métalliques ou le textile**. Le poids de ces entreprises est très élevé en Corse et dans les DOM.

4. Poids des PME, hors MIC, dans l'emploi marchand



iv. Les particularités des TPE et PME

Les **TPE et PME** disposent de **caractéristiques** qui leurs sont **spécifiques**² :

- Passage plus facile vers la grande entreprise
- **Polyvalence des tâches** dans les fonctions
- **Opportunités d'évolutions internes limitées**
- **Opportunité d'évolution interne** plus **tournée vers des postes hiérarchiques** que fonctionnels
- Les **évolutions suivent** plus une **démarche opportuniste** que rationnelle
- **Moyens matériels et financiers** plus **restreints** que pour une ETI ou une GE

² « Différence entre grand groupe et PME ». In *Primastone Consultant* (En ligne), 2017. Consulté le 27 juillet 2017. Disponible sur <http://primastoneconsultant.net/conseils-projet-professionnel/81.html>

- Lieu de **privilégier** pour l'**adaptabilité**, l'**initiative**, le « système D », la **souplesse** de fonctionnement
- **Recrutement** de personnel **expérimenté** et **immédiatement opérationnel**
- **Faible mobilité** demandée aux collaborateurs
- **Fidélisation** des collaborateurs
- **Qualité de vie au travail**: employeur et collaborateurs plus faciles d'accès, communication directe, ambiance familiale, entreprise libérée
- **Réactivité** personnelle et de la structure **prédominante** (prises de décisions plus rapides)
- **Plus de liberté individuelle** dans la prise de risque et l'improvisation
- **Culture d'entreprise plus ou moins marquée**
- **Travaux moins routiniers**
- **Rémunération dépendante** des **savoirs faire** et **performances** plus que de l'âge ou des diplômes

Ainsi, **travailler et s'épanouir** dans une PME **passer par la qualité du management** et **l'approche globale des métiers** dans **une vision de réussite de l'entreprise**.

Que retenir ?

Avec 140 000 entreprises employant 28% des salariés pour un effectif moyen de 27 collaborateurs, les PME composent majoritairement le paysage français des secteurs des services, de la construction, de l'industrie, du social et médico-social. Réparties principalement dans le Nord, le Sud Est et l'Ouest, cette catégorie économique en croissance depuis 2015, avec 1300 milliards de chiffre d'affaire, réalise 23% de la valeur ajoutée française. Dynamisé par le taux de chômage et l'envie d'entrepreneuriat des jeunes quadragénaires, la création d'entreprises est en pleine croissance. Les chefs d'entreprises, sexagénaires pour 1/3 d'entre eux, cèdent 10% des PME dont près de 20% dans le giron familial. Les défaillances bien que ne baissant pas, sont en stagnation et les PME résistent au contexte économique difficile avec seulement 7% des procédures (jeunes entreprises au CA faible). L'augmentation des flux commerciaux bénéficie aux PME qui enregistrent une progression de CA de de valeur ajoutée de prêt de 2%, permettant ainsi d'accroître leur bénéfice brut. Les mesures gouvernementales et la croissance ont permis de contenir la progression du coût du travail. Prudentes, les PME ont tendance à limiter leurs investissements au profit de l'assainissement de leurs dettes. Bien que représentant un peu moins de 10% de leur CA, les PME sont de plus en plus nombreuses à se tourner vers l'exportation (Amérique, Asie, UE, Moyen Orient). Les PME bénéficient des marchés publics où 30% des commandes leur ont attribués avec une augmentation de la valeur d'achat et de la part consacrée. Avec un taux de marge maîtrisé à 21%, une augmentation du résultat net et une baisse de la rémunération des actionnaires et de l'investissement, les PME ont des fonds propres permettant de limiter leurs besoins en concours bancaires et de mobiliser plus de capitaux propres. Enfin, les PME puisent leurs forces dans un management se voulant favorable à l'autonomie, la diversité des tâches, l'épanouissement de l'individu et une empreinte culturelle forte.

Ces éléments économiques plutôt bons, fournissent un terreau favorable aux chefs d'entreprises pour l'innovation et l'entrepreneuriat mais aussi pour une démarche responsable et attentive à la sécurité globale de leurs organisations. Mais qu'en est-il vraiment ?

2) Qu'elles problématiques de sécurité globale des TPE et PME et quelles solutions pour faire face aux situations de crise ?

a. Qu'est-ce que la sécurité globale en entreprise ?

Initiée en 1982 des travaux de la commission Palme, la notion de « sécurité commune » liée à l'interdépendance croissante des états due au développement des échanges économiques, le concept de sécurité global apparait au début des années 1990 (Arcudi, Giovanni, 2006) ; Remise en cause des paradigmes classiques par les Etats Unis et l'Europe (Waltz, Buzan, Roucaute, 1991), travaux de la Commission de l'ONU³ qui définissent une « overall security governance » et de Susan Strange sur l'idée que la sécurité est multidimensionnelle et doit être abordée d'un point de vue économie, environnemental et culturelle⁴. La mondialisation et les nouvelles technologies de l'information de la communication (TIC) vont voir émerger le développement des nouveaux risque et nouvelles menaces (terrorisme, espionnage industriel et cybercriminalité). Un réel paradigme de sécurité globale voit le jour et ce place au centre des préoccupations sur les risques et menaces (Résolution de différents profonds par la force militaire d'Etats ou de coalition, guerre asymétrique, terrorisme international, cybercriminalité, crises sanitaires internationales, réseaux mafieux et crime organisé mondialisés, catastrophes naturelles, changement climatique) conduisant les Etats occidentaux à penser leur sécurité de façon plus globale et réorganiser celle-ci en tenant compte des problématiques intérieures mais aussi des enjeux stratégiques internationaux⁵⁶⁷

Ainsi, le paradigme de sécurité globale permet de penser la capacité d'un Etat à parvenir et à assurer à l'ensemble de ses membres un niveau maximum de sécurité face aux risques et menaces, de façon à permettre la protection de ses habitants, la pérennité des activités collectives et individuelles, avec un maximum de résilience⁸. Une autre définition, donne la sécurité globale comme la capacité d'assurer à une collectivité donnée et à ses membres, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités collectives et individuelles (INHES, 2003). Enfin, la notion de sécurité globale peut être pensée comme relevant d'un mouvement de partage des réflexions, des responsabilités et des actions (Laclemence, 2005 ; Roucaute et Roche, 2010).

³ (en) « Shridath Ramphaml » (<https://www.iisd.org/biography/shridath-ramphal>), sur *International Institute for Sustainable Development*, 3 mars 2015

⁴ (en) Strange, Susan, *The Retreat of the State, The diffusion of Power in the World Economy.*, Cambridge, Cambridge University Press, 1996

⁵ Roucaute, Yves, « Une revue scientifique pour penser la sécurité globale », *Cahier de la Sécurité*, n°14, octobre-novembre 2014, p. 7-15

⁶ (en) Roucaute, Yves, « The ongoing European shake-up », *Cahier de la Sécurité*, n° Spécial issue, mars 2010

⁷ Roucaute, Yves, « Le bouleversement inachevé européen », *Cahiers de la Sécurité*, n°14, octobre-novembre 2010

⁸ WIKIPEDIA, « Sécurité globale (concept) », modifié le 28 septembre 2016 à 03:38 Consulté le 19 juillet 2017. Disponible sur [https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_globale_\(concept\)](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_globale_(concept))

Les éléments étudiés ayant amené la naissance du concept de sécurité globale et des définitions qui en découle, permettent d'appliquer cette notion étatique décrite ci-dessus au monde de l'entreprise et notamment des PME. Plusieurs marqueurs le justifient :

- Développement des échanges économiques
- Notion de facteurs multidimensionnels
- Mondialisation
- TIC
- Risques et menaces
- Pensée globale
- Problématiques internes
- Enjeux internationaux
- Sécurité face aux risques et menaces
- Protection, pérennité, résilience
- Prévention et protection face aux risques et menaces
- Développement sans ruptures
- Partage des responsabilités et des actions

Les définitions et pensées précédemment citées peuvent être modélisées en version « entreprise ».

Le paradigme de sécurité globale permet de penser la capacité d'une **entreprise** à parvenir et à assurer à l'ensemble de **son organisation** un niveau maximum de sécurité face aux risques et menaces, de façon à permettre la protection de ses **salariés**, la pérennité des activités de **conception, commercialisation, production et distribution**, avec un maximum de résilience. Une autre définition, donne la sécurité globale comme la capacité d'assurer à une **entreprise** donnée et à ses **salariés et son outil de production**, un niveau suffisant de prévention et de protection contre les risques et les menaces de toutes natures et de tous impacts, d'où qu'ils viennent, dans des conditions qui favorisent le développement sans rupture de la vie et des activités **conception, commercialisation, production et distribution**. Enfin, la notion de sécurité globale peut être pensée comme relevant d'un mouvement de partage des réflexions, des responsabilités et des actions.

En 2013, 23 M€ de détournés en une vingtaine de jour par une subtile escroquerie à « l'arnaque au président » au détriment de l'entreprise Vallourec⁹, cryptage de tous les fichiers de la PME Insmatel en 2014, victime d'une cyber attaque de type « Ransomware »¹⁰ avec un préjudice financier de 1000 Dollars seulement mais des données partiellement

⁹ « La fraude était tellement sophistiquée... ». *Le Parisien.fr* Fait du jour, 17 novembre 2013. Consulté le 26 juillet 2017. Disponible sur <http://www.leparisien.fr/espace-premium/actu/la-fraude-etait-tellement-sophistiquee-17-11-2013-3322519.php>

¹⁰ Wikipédia <https://fr.wikipedia.org/wiki/Ransomware> : Un **ransomware** (ou logiciel rançonneur ou d'extorsion), est un logiciel malveillant qui prend en otage des données personnelles.

retrouvées¹¹, successions d'attentats en Indonésie et Burkina Faso revendiqués par l'Etat Islamique et Al-Qaïda en janvier 2016 dans des zones à forte concentration de voyageurs d'affaires et d'expatriés¹², décès d'un maçon suite à une chute de 12 mètres sur le chantier d'un immeuble à Toulouse en juillet 2017¹³... autant de cas que les chefs d'entreprises doivent subir et affronter aujourd'hui au sein de leurs structures quel que soit la taille de celles-ci et les PME n'échappent pas à cette funeste énumération.

Dans les années 70, les entreprises ont mis en place des Directions dédiées à la Qualité avec une approche mono centrée sur cette fonction stratégique. Changement de cap dans les années 80 où l'approche est réalisée par un « management globale par la qualité » dans lequel toutes les parties prenantes de l'entreprises sont concernées ; effet immédiat, une forte amélioration de l'appareil industriel français ! Cependant, autant la sureté des installations industrielles est une réalité maîtrisée, notamment grâce aux normes drastiques, autant l'approche de sécurité globale des entreprises reste le parent pauvre des cultures d'entreprise. La sécurité, dans notre confort hexagonal, est renvoyée à des concepts régaliens où l'Etat providence assure celle-ci alors que le quotidien des entreprises est marqué par des risques d'atteintes à la sûreté et à la sécurité des personnes, des biens et des organisations. Selon la sensibilité des chefs d'entreprises, tel ou tel secteur sera privilégié sans qu'il y ait une vision globale de la sécurité de la structure alors que cette approche est toute différente dans le fonctionnement opérationnel et stratégique de l'entreprise ; interactions du service R&D avec le marketing, commercial, financier et RH lors du développement d'un produit. Dans un monde globalisé, l'entreprise doit être capable de réaliser un diagnostic des risques potentiels – au-delà de ce qui est attendu dans le document unique d'évaluation des risques professionnels, ciblés santé et sécurité au travail – et de les anticiper afin de préserver et sauvegarder sa capacité de croissance et d'innovation. Aussi une acculturation du management, qui inculquée à l'ensemble des collaborateurs permet de contribuer à la sécurité globale de l'entreprise. Cette contribution passe par des comportements individuels et collectifs quotidiens. Cette démarche doit être diffusée dans l'ensemble des entreprises de par l'accroissement des risques et menaces et place celles-ci comme entités vulnérables. Ainsi, tous les risques doivent être couverts dans une vision 360°. *Il s'agit ici de passer d'une logique de préservation de l'activité à une logique d'anticipation sur tous les aspects de l'intégrité d'une entreprise (Exemple, l'utilisation frauduleuse d'un réseau).* Le manager dirigeant, responsable au pénal et au civil (tout comme l'entreprise en tant que personne morale) doit veiller à ce que chaque collaborateur soit associé à la diffusion et au respect d'une culture de Sécurité Globale. La diffusion de cette culture nécessite du temps et des actions en amont, dès le stade de la formation

¹¹ BESTRON, Christian, « Interview » in : *6 minutes pour trancher*. Radio : RTL, 17 mai 2017, 07:09

¹² HOLLANDER, Alexandre. « Ce qu'une entreprise devrait faire pour assurer la sureté de ses employés à l'étranger » (En ligne). *Huffingtonpost*. 23 février 2016, 14 :45. Consulté le 11 mai 2017. Disponible sur : http://www.huffingtonpost.fr/alexandre-hollander/surete-expatries-entreprise_b_9297454.html

¹³ COHADON, Jean. « Sur un chantier, un maçon se tue en tombant de 12 mètres ». *Ladepeche.fr* (en ligne) le 06 septembre 2017, 12 :43 (Consulté le 26 juillet 2017). Disponible sur <http://www.ladepeche.fr/article/2017/07/06/2607854-chute-mortelle-d-un-ouvrier-a-toulouse.html>

initiale des futurs professionnels et par la formation continue pour les salariés et non-salariés. Enfin, l'ensemble des organisations professionnelles, patronales et salariées, doivent se mobiliser pour accélérer cette prise de conscience sur la Sécurité Globale à l'image de ce qui existe déjà dans beaucoup de pays compétiteurs de nos entreprises. L'activité économique est atteinte plus ou moins durablement lors de problème de sécurité publique ou privée. La perception que l'entreprise doit avoir de la Sécurité Globale est une approche par l'investissement et non par le cout et comme un levier de croissance et non un frein¹⁴.

Les directeurs de sûreté, responsables sécurité, *risk manager*... doivent démontrer la rentabilité des investissements à réaliser dans le domaine de la sécurité à la direction de l'entreprise tout en se conformant aux impératifs de normes, réglementation, caractéristiques techniques... Voilà pourquoi les recrutements de ces profils dans les entreprises, s'axent sur des populations de techniciens ou d'ingénieurs de leur entreprise, des *risk managers* venus du monde de l'assurance, ou des managers et experts en risques. Ces responsables ont une approche d'une sécurité globale orientée business car pour eux, c'est le business qui précède et justifie le retour sur investissement dans la protection et la sécurité et non pas la sécurité qui protégerait le business. Leur défi est de savoir transformer une contrainte apparemment improductive en une ressource à plus long terme. Si la sûreté n'a pas de prix, elle a bel et bien un cout à optimiser, sans nuire au développement durable de l'entreprise. Ce sont des adeptes et des praticiens de toutes les techniques de rationalisation de l'optimisation des couts par le biais du calcul des retours sur investissements (ROI).

P. Gard, dans sa préface à l'enquête « En toute Sécurité et Agora (2010) » explique :

L'entreprise n'a ni la rigueur militaire ou policière, ni l'esprit de compassion. Son mode de fonctionnement est structuré sur une efficacité financière et une rentabilité (...). Celui de la Sûreté-Sécurité n'est ni pris en considération à sa juste valeur, ni évalué (...). Si le taux d'AT se mesure, si le taux de démarque se décèle, si les pertes subies par les événements accidentels se provisionnent, on n'incrémente que la colonne « passif ». (...) Quand il n'y a ni vol, ni accident, on ne remarque même plus le travail accompli par ces équipes qui veillent au quotidien sur les personnes et les biens. Il me semblerait juste de pouvoir mesurer la non-perte en un profit (p.7).

Toutefois en France, l'esprit des dirigeants prédisposerait plus ceux-ci à recruter dans un vivier d'experts, immédiatement opérationnels (militaires, gendarmes, policiers) et

¹⁴ Paragraphe écrit sur la base des informations contenues dans l'article de TRALET, Claude. « La sécurité globale contribue à la croissance ». In : Lesechos.fr (En ligne) le 12 mai 2017 17:42 (Consulté le 19 juillet 2017). Disponible sur <https://www.lesechos.fr/idees-debats/cercle/cercle-169927-la-securite-globale-contribue-a-la-croissance-2086457.php>

productifs, plutôt que de tenter des aventures de monter et de compétences internes et des démarches de sécurité innovantes : « *Comme on ne sait pas faire, prenons ceux qui sauraient faire* ». Ces profils nécessitent une acculturation au monde de l'entreprise pour une acceptation par celle-ci.

*« J'ai combattu le travers du risque de la culture militaire, en me reconvertissant très tôt pour obtenir un diplôme qui m'en éloigne et me fasse mieux accepter dans la clan de l'entreprise. Il me fallait surtout prouver, non pas mes faits d'arme dans l'armée, mais ma capacité à m'intégrer dans l'entreprise. Et cela passait par l'épreuve du généraliste, d'où l'acquisition de compétences en comptabilité, fiscalité, droit du travail, RH, marketing... Et c'est un plus, puisque ce vocabulaire est devenu commun avec d'autres entités de l'entreprise. Je m'y sens beaucoup plus adopté. »*¹⁵

Entreprises et sécurité globale : un cadre d'interprétation

Faute d'approches universitaires critiques (...) l'art de protéger les entreprises vulnérables contre risques et menaces internes ou externes (Nous trouvons des références chez Ocqueteau et Pottier, 1995, Ocqueteau, 2002, Bonnet, 2007 et 2008, Minot, 2009, Hassid, 2010, Dupont, 2011, Deharo, 2011) reste encore assez peu interrogé et rarement évalué empiriquement, en France tout au moins. (...) La mise en sûreté (*et sécurité*) de l'entreprise fait en réalité l'objet d'investissements normatifs encore assez peu contraignants. Car, hormis le domaine de la sécurité du travail et de l'incendie, très consolidé par le poids de l'histoire de l'État-providence (Ewald, 1986), la mise en sûreté reste une prérogative assez largement autonome. Les causes et conséquences de cette liberté relative donnent lieu à des pratiques protectrices réelles, mais encore assez peu standardisées. Et vu que la perception des risques et des dommages demeure un domaine d'appréciation souverain encore largement subjectif (...), les coûts d'investissements consentis pour limiter la survenue des risques liés à des actes hostiles ou leurs conséquences négatives fluctuent considérablement d'une entreprise à l'autre. Ils fluctuent surtout au gré des capacités de financements spécifiques des entreprises que leurs dirigeants sont prêts à investir.

À partir des années 2000, une littérature d'inspiration managériale finalisée sur la gestion des menaces a apporté d'utiles repères à une meilleure connaissance du terrain de leur mise en sûreté à l'ère de la globalisation (Pierre, 2009a). Si l'objectif de ce savoir n'est pas « critique » à proprement parler, son apport à la connaissance de la réalité des procédures de mise en protection concrètes (...). Le savoir cumulatif apporté par cette littérature grise se déploie au sein de deux grandes inspirations déterministes : c'est la diversité des menaces qui explique mécaniquement la mise au point du dispositif de sûreté dans l'entreprise capitaliste, l'État restant en retrait. Ou bien, c'est l'État qui, en certaines circonstances, dicte

¹⁵ Paragraphes rédigés sur la base des données d'OCQUETEAU, Frédéric. « Chefs d'orchestre de la sûreté des entreprises à l'ère de la sécurité globale » 2001.

encore aux entreprises les règles du jeu de leur mise en sûreté dans des domaines où se négocient les stratégies de lutte contre des menaces communes.

Une expertise spécialisée accompagne la *révolution culturelle* de la mise en sûreté globale des entreprises par les menaces et attaques dont elles seraient de plus en plus fréquemment l'objet (Roucaute, 2010). L'objectif de cette expertise vise *in fine* à transformer certaines mentalités entrepreneuriales aventurières et preneuses de risque (J.A. Schumpeter) en des mentalités plus inventives dans la mise en précaution sous *l'ère du risque*, auprès d'acteurs échappant aux figures anciennes de « l'héritier rentier » ou du simple « administrateur gestionnaire ». Cette littérature d'expertise se focalise essentiellement sur la description des *menaces*, leur ampleur et leur récurrence, leur nouveauté et plasticité, pour promouvoir les dispositifs humains et technologiques de prévention chez des entrepreneurs réputés à la traîne des réalités menaçantes. (...) La plus élaborée des dernières en date s'appuie sur le paradigme stratégique du *décèlement, de l'étude et de la formation à la résilience du risque et de la menace*. Yves Roucaute (2010) évoque par exemple une hiérarchie des menaces (« processus provoqués par la volonté humaine »), les englobant dans une rhétorique guerrière de la façon suivante : 1 - d'abord, le périmètre des conflits de haute intensité et les agressions commises par des *États malveillants, fragiles ou faillis* cherchant à s'en prendre aux réseaux numériques et vouloir détruire les infrastructures ; 2 - ensuite, les menaces dues aux *guerres asymétriques*, telles qu'incarénées par l'islamisme radical, le terrorisme ou le crime organisé ; 3 - puis, les menaces liées au *soft power* cherchant à miner l'autorité, la légalité et la légitimité d'un État, d'un gouvernement et de la culture d'une nation ; 4 - enfin, les menaces liées aux cyber-attaques opérant contre des individus, des cadres, des entreprises ou un pays entier. L'implicite de cette expertise est généralement behavioriste : la menace malveillante explique le comportement de protection sans être jamais pensée, sauf du bout des lèvres, comme engageant une responsabilité collective (...).

On observe d'autres traces de cette rhétorique des dangers dans un ouvrage (Hassid, Masraff, 2010) dédié aux seules préoccupations de mise en protection de grandes entreprises ou grands groupes. Sont inventoriées les stratégies de prévention possibles face à un spectre de menaces répertoriées (des « crimes ») dans l'entreprise, à leur tour regroupées dans la typologie suivante : *menaces contre les valeurs immatérielles et informationnelles* de l'entreprise ; *menaces à l'encontre des personnes* ; *menaces à l'encontre des biens*. Cet ouvrage s'appesantit plus particulièrement sur les *menaces contre l'image de marque ou la réputation de l'entreprise* (par les attaques informationnelles) et les *menaces contre les autres actifs immatériels* (liées à l'espionnage industriel, la contrefaçon, la cybercriminalité). Il s'attarde en outre sur les *menaces contre les collaborateurs* de l'entreprise (salariés et cadres expatriés), enfin, sur les *menaces contre les installations, actifs matériels et marchandises*, liées aux environnements politiquement instables où sont délocalisées les filiales, dans le droit fil de la globalisation de l'économie-monde (dérives contestataires, terrorisme, piraterie).

(...) Le souci premier de la plupart des entreprises consiste à vouloir conjurer des risques endémiques liés à la récurrence des pertes de biens, qu'elle soit due à la malveillance ou à la négligence des salariés et des collaborateurs, plutôt que de se préoccuper de la rareté d'événements médiatiques spectaculaires sur l'environnement desquels l'entreprise s'estime sans grande prise. Ce qui donne une première indication au fait que, si les menaces sont globalement perçues selon des hiérarchies de préoccupations identiques dans les grandes entreprises comme dans les moyennes ou petites, la taille ou la grandeur ne ferait peut-être pas grand-chose à l'affaire. Par conséquent, la « fonction de sûreté » serait uniquement pensée par le risque le plus récurrent générant le plus de pertes maîtrisables. Elle le serait beaucoup moins par le risque rare et réputé quasi immaîtrisable par l'intéressé. Mais si telle est encore la configuration dominante, c'est parce que l'on situe le raisonnement dans les pratiques des entreprises industrielles et commerciales moyennes (...).

Une autre enquête française (Thalès *et al.*, 2008) (...) a apporté quelques nuances substantielles à ce sujet. Prendre en compte dans les enquêtes la variable du « secteur d'activité » de l'entreprise interrogée provoque apparemment une nette démarcation entre elles, quant à leurs préoccupations prioritaires. Il semblerait par exemple que les industriels soient beaucoup plus soucieux de se protéger de l'espionnage (85%) et des risques sanitaires (62%) ; les opérateurs d'infrastructures, de prévenir les accidents (90%) et des risques extrêmes vulnérabilisant leurs réseaux (70%) ; (...) ; enfin, dans les entreprises de services et le commerce de proximité, la préoccupation majeure concernerait la violation des lois et des réglementations sur les entreprises recevant du public (ERP) (95,5%), étant donné la nature de l'exposition de risques à l'interface de la production et du client.¹⁶

Dans un contexte mondial où la menace c'est installée dans notre quotidien, les chefs d'entreprises doivent aujourd'hui faire face aux nouvelles menaces et ainsi, à des interrogations peu abordées jusqu'ici. La sûreté et sécurité de leur environnement ne sont plus acquises et les confrontent à une nouvelle problématique, tant en France qu'à l'international. Un nouveau paradigme s'installe avec une vision globale de la sécurité qui ne se réduit plus à la santé sécurité des collaborateurs ou les problèmes de démarque inconnue. Là où les consciences commençaient à évoluer en terme de cyber sécurité et d'intelligence économique, les événements survenus ces deux dernières années ont contribué à un changement de perception et à une approche globale de la sécurité, celle-ci étant multi tête. *De là à modifier les habitudes en profondeur, il y a toutefois un chemin à parcourir, et beaucoup, par manque de moyens, de personnel et d'accompagnement, n'en ont pas encore fait une priorité.* Toutefois, une étude menée en 2016 par OpinionWay avec le CDSE et Axa Assistance, auprès de 300 dirigeants montre que seul 18% des dirigeants interrogés pensent que l'insécurité est une menace faible. Toutefois, aucune stratégie de sûreté-sécurité n'est pour autant mise en place.

¹⁶ OCQUETEAU, Frédéric. « Chefs d'orchestre de la sûreté des entreprises à l'ère de la sécurité globale » 2001

Le Premier frein n'est pas spécialement dû au manque de moyens, mais par un manque de vision et de connaissances, d'experts et de stratégies. *Un tiers des entreprises françaises sont toujours ignorantes de leurs responsabilités juridiques lors de l'envoi de collaborateurs à l'étranger.* Loin d'être une entrave au développement des entreprises, la sécurité, de par sa transversalité et son impact stratégique, est une composante majeure de la performance et de la réputation¹⁷.

Après cette approche de la notion de sécurité globale en entreprise, j'ai fait le choix de développer quatre problématiques de sécurité en entreprises, pour illustrer plus en profondeur des composantes qui sont pour moi les plus significatives en termes d'enjeux et/ou d'actualité. Ces domaines présentent aussi le plus d'occurrence lors de recherche sur le web et de par mon expérience et contact au quotidien avec les entreprises.

Ces domaines sont :

- La cybersécurité
- L'intelligence économique
- La sureté des collaborateurs à l'étranger face au terrorisme
- La santé et sécurité au travail

b. La cybersécurité

En 2014, la société Domino's Pizza se fait pirater par un groupe de cybercriminels appelés « Rex Mundi ». Ceux-ci menacent de rendre public les données de 590 000 clients si 30 000 € ne leur sont pas versés. En 2016, c'est une petite entreprise béarnaise, employant 23 salariés qui est victime d'une cyberattaque, mettant ceux-ci au chômage technique pendant près d'une semaine. Nicolas GUYAMIER, chef d'entreprise d'une PME de transport en Gironde a lui aussi été victime d'une attaque avec demande de rançon de 5000 €, payables en bitcoins, pour laquelle il n'aura pas cédé, assumant la perte de d'un tiers de ses données informatiques. Les exemples sont nombreux et l'actualité récente nous le rappelle encore.

En 2016, plus de 40% des entreprises européennes auraient été attaquées et leurs systèmes informatiques infestés par un ransomware ; 57% de ces entreprises sont des PME. Selon le rapport de 2014 « IT Security Risk Survey » de Kaspersky Lab et du cabinet B2B international, 94 % des 3900 entreprises (toutes tailles confondues) ayant répondu à l'enquête et issues de 27 pays, ont connu un problème de sécurité informatique au cours des 12 derniers mois. Si toutes les entreprises sont concernées par la problématique de cybercriminalité, beaucoup de PME considèrent que leur taille les protège car ne présentant que peu d'intérêt pour des hackers et ne considèrent pas leur stratégie IT comme une priorité. Par exemple, seul 14%

¹⁷ BEZIERS la FOSSE, Arnaud, FAGE, Sébastien, DARDON, Hubert. « Sécurité des entreprises : Construire une véritable stratégie ». LinkedIn le 23 mars 2017.

des entreprises de distribution et de e-commerce, considèrent comme stratégique la cybersécurité de leur organisation et 4% comme priorité principal. Kaspersky Lab précise que les PME peuvent subir de lourdes pertes en cas d'infection par un malware ou par des pertes de données. Celles-ci sont estimées à 10 000 dollars pour les services d'un expert, 5 000 dollars pour la formation des équipes afin d'empêcher une nouvelle attaque et des dommages en terme de réputation et d'image auprès des clients, fournisseurs et prescripteurs.

Cet état est d'autant plus préoccupant que l'évolution des attaques et demandes de rançons sont facilités par l'accès via le Darknet, à des kits de piratage ne nécessitant pas de haut niveau de connaissances et compétences techniques. « Des personnes qui n'ont aucune compétence en hacking peuvent acheter des ransomwares prêts à l'emploi », explique David Emm, coauteur du rapport Kaspersky Lab^{18 19}

Selon une autre enquête menée en 2015 par OpinionWay pour le « Club des experts de la sécurité de l'information et du numérique », 81% des entreprises françaises ont été visées par une cyberattaque. Ces attaques se déclinent en ransomware pour 61%, déni de service à 38%, défiguration de site à hauteur de 23% et vol de données personnelles dans 13% des cas. L'enjeu des Directeurs des Services d'Information (DSI) est devenu clé, quel que soit la taille ou secteur d'activité de l'entreprise même si les pertes financières potentielles les plus lourdes touchent plus particulièrement aux secteurs des nouvelles technologies, des systèmes d'informations, des médias, transports, logistique et grande distribution. Guillaume Poupard, directeur de l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), estime que les entreprises devraient consacrer 5 à 10% de leur budget à la cybersécurité. Ce montant est sans commune mesure par rapport aux coûts d'une violation de sécurité informatique. Selon NTT Com Security, une cyberattaque coûterait en moyenne 300 000 € pour une PME de moins de 1000 salariés et nécessite 9 mois pour résoudre les problèmes techniques. Au-delà des données chiffrées quantifiables financièrement (intervention d'expert, dommages sur les matériels à remplacer, temps consacré à résoudre le problème, temps perdu par les équipes ne pouvant plus travailler...), se rajoutent l'impact sur l'image et la notoriété. « Il y a souvent trop de problèmes de comportement humain, où les gens n'ont pas la compréhension de la menace ni des risques » selon Philippe Trouchaud, expert en cybersécurité associé au sein du cabinet PwC. 35% des incidents sont générés par des erreurs de collaborateurs de l'entreprise. Le même expert précise : Il existe beaucoup de littérature sur la cybersécurité. Paradoxalement, il y a

¹⁸ IBACH, Chrystelle. « Attaque et demande de rançon en ligne : comment y faire face ». Cadre et Dirigeant magazine (En ligne). 20 mars 2017.

¹⁹ DE COATPONT, Tanguy. « Attaque et demande de rançon en ligne : comment y faire face ». EconomieMatin (En ligne). 02 novembre 2014. Consulté le 31 juillet 2017. Disponible sur <http://www.economiematin.fr/news-attaque-informatique-piratage-pme-tpme-differnece-protection-strategie>

pléthore de livres très technologiques, mais peu sur les sciences de management sur le sujet »²⁰.

Yves Gael BILLET, expert systèmes connectés, rappelle que l'ANSII estime qu'un système industriel est un système d'information qui a la particularité d'engendrer des actions physiques. Ainsi, il va irait de soi qu'un système industriel soit vulnérable aux mêmes attaques qu'un système des techniques de l'information et des communications. Ainsi une même attention en termes de sûreté et de sécurité informatique doit lui être apportée. Le terme de « sécurité » fait référence à une protection contre des risques provoqués par des actes involontaires et le terme de « sûreté » implique des actes malveillants. Ainsi, la cybersécurité d'un système industriel traite le risque de défaillance du processus suite à un incident dont l'origine provient des technologies de l'information. Je rajoute que cette défaillance peut être engendrée de façon accidentelle, plutôt en interne ou faite de façon volontaire, plutôt en externe. Aussi, la loi de programmation militaire du 18 décembre 2013 introduit des dispositions relatives à la sécurité des systèmes industriels des opérateurs d'importance vitale (OIV) et l'obligation pour ceux-ci de sécuriser leurs systèmes. Toutefois, à l'ère de l'usine connectée (solutions sur Ethernet, télémaintenance, Manufacturing Execution Systems (MES), Customer Relationship Management (CRM)...) une démarche de cybersécurité s'avère fondamentale pour l'ensemble des entreprises. Aussi, la sécurisation cyber du système industriel passe par la compréhension de celui-ci (infrastructure, organisation...). D'un point de vue technique, la mise en place de commutateurs administrables sur le réseau Ethernet est un très bon point de départ (diagnostic et suivi réseau et fonctions sécurité). Mais les résolutions techniques ne suffisent pas pour assurer une protection du système industriel. Ainsi une formation en informatique et réseau et une sensibilisation à la cybersécurité doivent être portées aux automaticiens pour que ceux-ci et les informaticiens parlent le même langage. Réciproquement, les informaticiens doivent connaître le « métier » des automaticiens car bien que partageant des objectifs communs, leurs priorités sont différentes : confidentialité du système d'information pour les uns et disponibilité de l'information pour les autres. Dès lors qu'une acculturation commune est en place, une démarche de sécurisation globale peut être envisagée²¹.

Si nous prenons en exemple le secteur de l'aéronautique qui fait partie des rares domaines où les indicateurs économiques sont au vert, la seule ombre au tableau est la cybersécurité (sécurité des vols et supply chain). Avec un trafic passager qui devrait être multiplié par 2.5 d'ici 20 ans amenant plus de 10 milliards de passagers à prendre l'avion chaque année²², le secteur est une manne pour les cybercriminels. Pascal Pincemin, responsable du secteur

²⁰ « Cybersécurité : 5 chiffres-clés à connaître ». Microsoft Ideas (En ligne). 30 août 2016. Consulté le 11 mai 2017. Disponible sur <http://www.economiamatin.fr/news-attaque-informatique-piratage-pme-tpme-differnece-protection-strategie>

²¹ MEDDAH, Hassan. « Les usines sont vulnérables aux cyberattaques ». L'Usine Nouvelle (En ligne). 22 octobre 2016. Consulté le 11 mai 2017. Disponible sur <http://www.usinenouvelle.com/article/tribune-les-usines-sont-vulnerables-aux-cyberattaques.N453387>

²² Etude Cabinet Deloitte, 2017 « Les grandes tendances 2017 de l'industrie et défense ».

Aerospace and Defense chez Deloitte précises que « *le secteur est vulnérable aux cyberattaques* ». Il est tout à fait concevable d'imaginer même la possibilité de mettre un logiciel dans la puce d'un équipement et rendre critique la sécurité en vol. En 2015, le directeur de l'Agence Européenne de la sécurité Aérienne (AESAs) avait fait la démonstration auprès de ses experts qu'il est possible de pirater le système de contrôle d'un avion. Toutefois, le scénario le plus possible et réaliste est une attaque auprès des sous-traitants, majoritairement composés de PME. « *En France, plus de 60% des entreprises ont moins de 50 salariés. Souvent, elles n'ont pas la taille critique pour se payer un responsable de la sécurité informatique. C'est une cible facile pour un pirate* » rappelle Pascal Pincemin. Ceci est d'autant plus inquiétant que les grands donneurs d'ordre de ces PME (AIRBUS, LATECOERE...) ont engagé ces entreprises sous-traitantes dans une dynamique de numérisation et de modernisation, les fragilisant encore plus sur le plan informatique d'où une nécessité absolue de plus de cybersécurité et d'acculturation des équipes à cette menace²³.

Les données essentielles des entreprises sont prises en otage puis libérées contre le paiement d'une rançon réglée en Bitcoins. Attaques hautement techniques, opportunisme de facilité de gains financiers par des petites frappes, simple négligence humaine, employé corrompu ou placardisé, concurrence, organisations criminelles, organisation idéologique ? Utilisation trop fréquente des mêmes mots de passe basés sur nos vies personnelles, méthode de social engineering, publication non sécurisée de données personnelles sur Facebook, cadeau de clé USB piégées... les exemples de stratagèmes pour pénétrer un système ne manquent pas. L'ANSII et les ministères concernés (défense, intérieur, industrie) accompagnent les OIV et publient des guides de bonnes pratiques dans les usages informatiques. La tâche ne s'arrête pas à ces seuls opérateurs. Nous avons vu que tous les secteurs sont concernés : viticulteurs, menuisiers, imprimeurs sont attaqués pouvant soit les fragiliser financièrement ou en terme d'image et de notoriété, soit les amener à fermer et faire disparaître des emplois. L'internet des objets démultiplie les brèches ouvertes aux hackers : caméras de surveillance, robots agricoles, industriels ou médicaux. En 2016, l'Usine Nouvelle et Orange Business mène une étude où 56% des entreprises industrielles interrogées reconnaissent avoir été victime d'une cyberattaque ce qui représente 5% de plus qu'en 2015. Malgré les sensibilisations menées dont celles conduites par la gendarmerie, une autre étude montre la disparité de perception entre des responsabilités et impact de la cybercriminalité entre les responsables IT et dirigeants d'entreprises. Face à l'ampleur du phénomène, il ne s'agit plus de sensibiliser mais de former les collaborateurs, de l'employé au cadre, aux problématiques techniques, aux menaces récurrentes internes et externes. Seule la formation initiale ou continue peut couvrir ces besoins. A ce jour, les écoles de commerce ou d'ingénieurs n'ont pas généralisés l'enseignement de modules en lien avec la sécurité, sûreté et encore moins la cybersécurité dont les filières informatiques (sic). Les

²³ MEDDAH, Hassan. « La cybersécurité, nouveau talon d'Achille du secteur aéronautique ? ». L'Usine Nouvelle (En ligne). 13 mars 2017. Consulté le 11 mai 2017. Disponible sur <http://www.usinenouvelle.com/article/la-cybersecurite-nouveau-talon-d-achille-du-secteur-aeronautique.N513924>

hackers fonctionnent sur des modèles d'entreprises pour conduire leurs actions illégales : objectifs de parts de marché, offres de services différenciés, diversification ou spécialisation des activités, sous traitance, externalisation... L'adversaire est à combattre avec les armes de l'entreprise et de s'acculturer de cette menace au plus tôt des cursus de formation ou par la contribution à cela des plans de formation²⁴.

c. L'intelligence économique

La protection des données et des innovations n'est pas l'apanage des grands groupes. Les PME prennent conscience des risques encourus et s'emparent de la question d'intelligence économique. « *La sûreté économique est aussi un problème local. Les PME sont toutes concernées* », explique Sophie Larivet de l'INHESJ²⁵. Les PME prennent conscience de la nécessité de protéger leur savoir-faire pour se prémunir contre des actions malveillantes. C'est de l'agent de sécurité au dirigeant qu'il convient d'agir. Dans ce domaine, la sûreté passe par le traitement du risque par le biais de la malveillance²⁶. Environ 15 à 20% des PME pratiquent l'intelligence économique mais 40% ne font que de la veille sans aller plus loin²⁷. La sûreté économique permet aux PME de préserver leurs innovations et de garder un avantage compétitif ; c'est un facteur fort de développement et de performance. Les 3 piliers de l'intelligence économique que sont la veille économique, la mise en place de mesure de protection des données et le travail d'influence, donnent aux entreprises des outils pour leur permettre de prendre les meilleures décisions stratégiques²⁸ Pour Rémy Pautrat, Préfet de région honoraire et précurseur dans la vision sur les enjeux de l'intelligence économique, « *il y a malheureusement dans notre pays une faiblesse dramatique de la pensée stratégique notamment dans le domaine de l'information. La pratique de l'intelligence économique n'est pas encore assez répandue notamment en raison d'un problème culturel face à ces questions contrairement aux pays anglo-saxons. On note un manque de familiarité culturelle à ces questions. Ces encore un peu jeune dans notre pays même si on est moins en retard qu'il y a 15 ou 20 ans* » dit Eric Delbecque, chef du département Sécurité à l'INHESJ. Cette notion culturelle d'intérêt porté pour l'EI est reprise par Sophie Larivet : « *Le terme d'intelligence économique n'est pas toujours bien appréhendé et prête à confusion. Il a été préféré à « renseignement économique » pour traduire le terme anglais de « compétitive intelligence ».* Un choix lié à la mauvaise image des renseignements

²⁴ MEMHELD, Pierre. « Faut-il plus de cybersécurité, de cyberdéfense ou de cyberrenseignement ? » The Conversation 5 (En ligne). 09 mars 2017. Consulté le 11 mai 2017. Disponible sur <http://theconversation.com/faut-il-plus-de-cybersecurite-de-cyberdefense-ou-de-cyber-renseignement-73215>

²⁵ Colloque « Intelligence économique » du 19 au 23 mai 2014 organisé par l'Institut National des Hautes Etudes de la Sécurité et de la Justice. Sophie Larivet, chercheuse en sciences de gestion (INHESJ).

²⁶ BOLLET, Laurent. « Maitriser la sécurité des entreprises ». Bienpublic.com (En ligne). 05 décembre 2016. Consulté le 19 juillet 2017. Disponible sur <https://portail-ie.fr/short/1350/la-d2ie-appelée-a-disparaitre>

²⁷ LARIVET, Sophie. *Intelligence économique : Enquête dans 100 PME*. Le Harmattan, 2009, 260p, (Intelligence Economique). ISBN 2296073778

²⁸ AFP. Les PME se mettent à l'intelligence économique. L'Entreprise.com (En ligne). Publié le 23 mai 2014 et mis à jour le 19 janvier 2015. Consulté le 11 mai 2017. Disponible sur http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/les-pme-se-mettent-a-l-intelligence-economique_1545939.html

en France. Les sociétés anglo-saxonnes, scandinaves ou belges sont davantage persuadées de son importance (...). C'est l'attitude du chef d'entreprise qui est déterminante dans la réussite d'une telle démarche ». En 2013, le gouvernement met en place une délégation interministérielle à l'intelligence économique (D2IE) pour sensibiliser les entreprises sur cette nécessité. Olivier Buquen, directeur de la D2IE : « avec cet outil de sensibilisation, nous souhaitons mettre à votre disposition un site internet qui soit à la fois simple, complet et opérationnel »²⁹. Cette délégation réformée en janvier 2016 renforce l'importance portée par les pouvoirs publics sur la problématique de l'intelligence économique³⁰. Ainsi, Jean Baptiste Carpentier, commissaire à l'information stratégique et à la sécurité économique à Bercy (2016) précise : « Aujourd'hui, l'action de l'Etat vise à prendre en compte un certain nombre de difficultés des entreprises à ce sujet. Nous devons assurer la maîtrise de la sécurité (...). Concrètement, c'est éviter des pertes de compétitivité pour au contraire en créer. Pour cela, il faut évoluer vers **un concept de sécurité globale d'entreprise** ». Christophe Reville, organisateur du sommet sur l'intelligence économique de Chamonix³¹ et expert en contre-espionnage économique, complète en disant « Ainsi les entreprises, en lien ou pas avec l'Etat doivent être sensibilisées et doivent impérieusement agir dans leur organisation ».

Toutefois, bien que 1000 attaques (*espionnage industriel*) aient été relevées en 2010 selon le rapport du député Bernard Carayon et que les PME représentent la moitié des affaires d'espionnage industriel selon Sophie Larivet, un vide juridique entoure l'espionnage économique et industriel en France. Toutes les tentatives pour instaurer un « secret des affaires » (Bernard Carayon en 2012, Jean Jacques Urvoas en 2014) sont restées lettre mortes. Le dernier essai date d'un amendement de la loi Macron qui lui aussi a été retiré sous la pression des journalistes qui craignaient d'une restriction de la liberté de la presse et des « lanceurs d'alerte ». Ces échecs montrent la difficulté à légiférer sur le sujet alors qu'en même temps une nécessité d'évolution culturelle est demandée aux chefs d'entreprises...³²

L'Institut National des Hautes Etudes de la Sécurité et de la Justice propose à ce sujet une formation sur la « Protection des entreprises et Intelligence économique ». Celle-ci est enregistrée au RNCP et a une équivalence bac+5 et s'adresse à un large public dont cadres supérieurs, dirigeants et associés d'entreprise. Cette formation vise à développer une vision

²⁹« La Délégation Interministérielle à l'intelligence économique a son site internet ». Club des Directeurs de Sécurité et de Sûreté des Entreprises (En ligne). 15 avril 2013. Consulté le 01 aout 2017. Disponible sur : <https://www.cdse.fr/la-delegation-interministeriel-a->

³⁰ « La D2IE appelée à disparaître ». Portail de l'IE (En ligne). 28 janvier 2016. Consulté le 01 aout 2017. Disponible sur <https://portail-ie.fr/short/1350/la-d2ie-appelée-a-disparaître>

³¹ Le sommet de l'intelligence économique et de la sécurité / sûreté (IE2S) de Chamonix est une rencontre de haut niveau entre experts de l'IE et de la sécurité/sûreté dans tous les domaines de l'activité économique, et dirigeants d'entreprises sensibles à ces problématiques. Site web <http://sommet-ies.org/>

³² RIMONDI, Laurent. « Intelligence économique, un outil de compétitivité pour les PME ». Le Nouvel Economiste.fr (En ligne). 15 avril 2015. Consulté le 01 juin 2017. Disponible sur <https://www.lenouveleconomiste.fr/lesdossiers/intelligence-economique-un-outil-de-competitivite-pour-les-pme-26792/>

globale de la sécurité-sûreté quel que soit le secteur d'activité ou la taille de l'entreprise, la culture et les savoir-faire nécessaires pour appréhender l'ensemble des enjeux. L'autre idée est de concevoir la sûreté comme un atout de compétitivité intégré dans la stratégie des entreprises et leur dynamique de développement. Enfin, avoir une vision partagée entre public et privé sur l'intelligence économique et la sécurité des économies alliant dynamique libérale et sécurité nationale³³.

Le développement de politiques efficaces d'intelligence économique est devenu un enjeu majeur pour les entreprises. La formation des managers futurs et actuels à un usage de l'information pour conquérir de nouveaux marchés dans des échanges mondialisés sera un avantage décisif pour la compétitivité des entreprises. C'est une action indispensable dans une économie ouverte où l'information et la connaissance sont devenues des enjeux stratégiques. Toute entreprise, quel que soit son secteur ou sa taille, doit se saisir de ce concept de management du 21^{ème} siècle pour faire face à la mondialisation, gagner en innovation, protéger ses savoir-faire, rester offensif et défensif face à la concurrence et gagner des parts de marché à l'instar de PME tel que Dacral, Markal, Raymond, Sisley ou Sphère qui se sont tournées vers des stratégies d'intelligence économiques performantes. Ainsi des dirigeants et cadres dirigeants de PME, membres du groupe de Technologie Avancée de l'Association HEC a conçu une méthode MADIE® d'aide à la décision par l'intelligence économique. Simple, facile et rapide à mettre en œuvre, peu coûteuse, adaptable et non freinante de par une analyse trop lourde, la méthode MADIE® permet de comprendre, analyser, anticiper et entreprendre des actions adaptées à un marché mondial soumis à une forte concurrence et en perpétuelle mutation en apportant des éléments pour nourrir la stratégie de l'entreprise et le pilotage des actions³⁴.

Un exemple simple de veille à la portée des PME : *« Des entreprises hantent les salles d'attente des Mairies car elles ont bien compris que l'information recueillie régulièrement à ces endroits vaut de l'or. L'information en question, peut-être par exemple les annonces de mariages, les fameux « bans » (...). Elles deviennent intégrées dans les bases de données qui vont être utiles à certaines entreprises. Mais qui peut bien s'intéresser aux futurs mariés ? Les agences de voyages, les traiteurs ? Oui bien sûr mais pas seulement eux... D'abord il y a les entreprises qui vendent des produits ou des services pour le mariage en lui-même (robes de mariées, location de costume, orchestre, lieux de réception, fleuriste...). Ensuite, il y a l'après mariage, avec deux catégories : Juste après le mariage (voyage de noce, services bancaires,*

³³ Ouverture des inscriptions à la 21^{ème} session nationale spécialisée « Protection des entreprises et Intelligence économique » de l'INHESJ publié le 17 mars 2017 sur https://www.inhesj.fr/sites/default/files/fichiers_site/formation/candidature_2017-2018_ISE/presentation_21sns.pdf

³⁴ « Intelligence économique : les PME (...) sont concernés ». Entreprendre.fr (En ligne). 05 janvier 2015. Consulté le 01 juin 2017. Disponible sur <http://www.entreprendre.fr/intelligence-economique-des-pme-aux-grands-groupes>

assurances...) et plusieurs mois après le mariage (voiture, puériculture, achat de résidence...)»³⁵.

Enfin, un second exemple sur l'intelligence économique d'une PME : « Une petite entreprise a identifié un nouvel axe de développement sur son marché, et souhaite regarder de plus près la faisabilité de la chose avant d'investir.

Le marché est énorme, mais il subsiste des difficultés techniques. Les premiers tests sont prometteurs, mais comment parler de ce projet sans se le faire piller par un concurrent ?

Dans un premier temps il est décidé à se protéger par le secret pour ne pas éveiller les soupçons. Ensuite, il sera peut-être fait recours à la divulgation en déposant un brevet. Les recherches d'antériorité montrent que des brevets très proches ont été développés. D'après le nombre de brevets déposés par un même inventeur, il est décidé de ne pas attendre un éventuel avis favorable de l'INPI, et de s'engager dans des relations de partenariat avec celui-ci qui semble avoir déjà résolu un des problèmes techniques identifiés.

S'ensuit la mise au point, et le lancement du produit. Hors, en face, la concurrence est déjà très bien implantée et se « partage le marché ». C'est ce que l'on pourrait appeler un marché « protégé ». L'entreprise décide donc de retarder légèrement le lancement du produit et de réaliser une phase de lobbying afin de promouvoir les spécificités de son produit. Ensuite, il y a un dossier à préparer sur chacun des concurrents en cas d'attaque concurrentielle. Chaque dossier contient les points forts et surtout les faiblesses des produits concurrents.

Des experts sont aussi sollicités pour donner leur avis sur le nouveau produit, et la presse est conviée à discuter librement avec ces personnes.

Le produit sort enfin et la concurrence essaie maladroitement de freiner le lancement du produit en reprochant le manque d'expérience de la société récemment positionnée sur ce marché. Ce à quoi il est répondu rapidement et de manière très travaillée que les anciens produits ont des défauts que les nouveaux produits n'ont pas car il a été fait appel à une technologie de pointe. Technologie que les concurrents n'ont pas.

A ce stade, la petite société qui vient de lancer son produit se permet même de proposer à un de ses concurrents, 20 fois plus gros qu'elle, d'utiliser son réseau de distribution, ce qui est un peu le monde à l'envers... »³⁶.

L'IE est avant tout perçue comme un moyen de renforcer la capacité d'anticipation et d'innovation de l'entreprise, avec pour objectif d'anticiper les enjeux pour définir sa stratégie pour 80% d'entre elles, d'être à l'écoute de ses clients (66%), trouver de nouveaux marchés ou se diversifier (60%), surveiller ses concurrents ou nouveaux entrants (59%), développer de nouveaux produits ou services, innover (51%)... La veille demeure le volet où l'Ets accorde le plus d'importance, suivi de la sécurité et de l'influence. Une Ets sur deux déclare avoir mis en place une démarche structurée (55%)³⁷. La recherche d'information privilégie les concurrents et les clients, devant d'autres sujets

³⁵ « Exemples concrets d'intelligence économique ». acrie.unblog.fr (En ligne). Date inconnue. Consulté le 01 juin 2017. Disponible sur <http://acrie.unblog.fr/performance-rentabilite-pragmatisme/demarche-de-veille-cellule-de-veille-veille-strategique/>

³⁶ « Exemples concrets d'intelligence économique ». acrie.unblog.fr (En ligne). Date inconnue. Consulté le 01 juin 2017. Disponible sur <http://acrie.unblog.fr/performance-rentabilite-pragmatisme/demarche-de-veille-cellule-de-veille-veille-strategique/>

³⁷ « Enquête sur les pratiques de Veille & d'Intelligence Economique des entreprises bretonnes, 8^{ème} édition ». Octobre 2015, CCI de Bretagne.

comme les fournisseurs et la réglementation. Concernant la protection de l'information, 44% des entreprises ont mise en place une démarche de sécurisation des données. La sécurisation venant surtout après une fuite d'information (49%), par obligation (44%) après une cyberattaque (26%) et seulement 27% après une action de sensibilisation³⁸. Toutefois, une étude publiée en septembre 2015 par la CCI de Lyon sur les pratiques et usages du numérique dans les TPE et PME, montre que 57% d'entre elles souhaitent améliorer leur sécurité informatique. Enfin, si 60% des entreprises interrogées ne mènent pas d'actions de lobbying celles-ci sont très orientées vers les réseaux professionnels dont réseaux d'entreprises (72%), organisations professionnelles (65%) et consulaires (32%). Les entreprises ont conscience de la nécessité de mener un lobbying d'influence, seule 34% n'en voient pas l'intérêt mais cette action n'est que peut réaliser faute de temps, de compétences ou d'identification des réseaux pertinents pour l'entreprise³⁹.

Bien que son cout soit modéré, de quelques centaines à quelques milliers d'euros, « *Le retour sur investissement est difficile à chiffrer. Il est plus facile de valoriser une marque ou un brevet acquis grâce à la veille d'information* » note Frédéric Martinet, fondateur d'Actulligence Consulting et du site actulligence.com.

Introduite dans les années 90 en France, l'intelligence économique commence à se structurer avec le Rapport Martre dès 1994. S'en suit la création de formations universitaires dédiées comme l'ICOMTEC dès 1996 ou l'IHEDN et l'INHESJ. En 2003, un second rapport structurel sera publié par la Documentation Française, il s'agit du rapport Carayon. La veille réglementaire à travers sa rubrique « exigences légales et autres exigences » était déjà présente dans la norme ISO 14001 version 2004. Les versions 2015 des normes ISO 9001 et ISO 14001 en leurs chapitres 4 « Contexte de l'organisme » et 6 « Planification » des normes ISO 9001 et ISO 14001 font appels aux pratiques et aux analyses apportées par l'Intelligence Économique, en particulier dans le paragraphe « Actions à mettre en œuvre face aux risques et aux opportunités ». Il s'agit en fait d'analyser de façon poussée les risques et les opportunités de chaque processus. Au-delà d'un simple formalisme, il s'agit bien de la montée en puissance d'une certaine « Culture de l'Analyse des Risques » ainsi que d'une « certaine prise de recul » qui apporteront un nouveau souffle et une plus-value particulière à nos revues de direction. L'Intelligence Économique est une discipline managériale et transversale dans l'entreprise (à l'instar de la QSE, de la R&D, la communication, le marketing, ...) qui a pour vocation de permettre à l'entreprise de prendre les bonnes décisions, de protéger ses savoir-faire et ses biens, de comprendre son environnement, d'anticiper certaines de ses évolutions et même, parfois, de pouvoir influencer sur celles-ci. L'un des objectifs est bien d'identifier les Menaces et les Opportunités impactant les processus clefs de nos entités certifiées et qu'elles puissent définir des plans d'actions spécifiques en s'appuyant sur leurs Forces tout en cherchant à progresser sur les

³⁸ « Zoom sur l'intelligence économique, 4^{ème} édition ». Janvier 2015. CCI de la Drôme.

³⁹ « Pratiques et usages du numérique dans les PME et TPE », septembre 2015, CCI de Lyon.

Faiblesses (Outils : SWOT, PESTEL, Xmind et analyse des risques : DUERP, MOSAR, Audits de vulnérabilité, Ishikawa)⁴⁰.

d. La sureté des collaborateurs à l'étranger face au terrorisme

Malgré les risques sociaux, politiques et sécuritaires dont plusieurs territoires du monde sont marqués, les entreprises y compris les PME, n'hésitent plus à parier sur leur installation à l'étranger en vue d'assurer leur développement. Malgré les opportunités et enjeux économiques à développer de nouveaux marchés dans des zones aussi géopolitiquement sensibles, les risques sont aussi réels et les impacts potentiellement néfastes. Des exemples de grandes entreprises, précurseurs dans le domaine, sont là pour apporter leur témoignage aux nouveaux conquérants. « *Le risque géopolitique existe et pèse sur la sécurité des équipes, obligées notamment d'évacuer leur lieu de travail lorsqu'Al Quäida s'est retrouvé proche de notre usine au Yemen* », témoigne Patrick Pouyanné, PDG de total. A côté de ces incidents, le groupe français est devenu la première compagnie occidentale à signer un accord avec l'Iran depuis la levée partielle des sanctions internationales dont est frappé le pays. PSA a également tiré parti de la levée d'une partie de ces sanctions ; sans les bons résultats iraniens, le groupe aurait vu un recul de ses ventes de 2% alors que son chiffre d'affaire a progressé de 4.9% en 2016. A contrario, entre inondations, changement de réglementation, cours du yuan, DANONE n'a pas trouvé l'essor espéré en Chine en 2016. La stratégie des entreprises doit s'adapter à un espace en pleine reconfiguration et mutation. Aussi, un long apprentissage de la culture du pays, de la façon de travailler et de traiter des affaires avec des cultures différentes doit s'opérer pour les entreprises au-delà des contextes sécuritaires⁴¹.

Alors que les entreprises cherchent des relais de croissance dans des pays aux économies dynamiques, les conditions de sécurité se dégradent dramatiquement : 14 janvier 2016, explosions revendiquées par l'Etat Islamique (EI) à Djakarta en Indonésie dans un quartier fréquenté par les expatriés. 15 janvier 2016, un restaurant prisé des ressortissants étrangers est pris pour cible à Ouagadougou au Burkina Faso par Al-Qäida au Maghreb Islamique (AQMI). 20 novembre 2016, prise d'otage au Radison Hôtel à Bamako (Mali) qui hébergeait des collaborateurs d'Engie et Tahles. Menaces et attaques répétées au Nigéria par le groupe terroriste Boko Haram... Plus médiatiques que les agressions de droit commun – plus d'une centaine de voyageurs d'affaires et d'expatriés touchés chaque année – les entreprises prennent conscience de la vulnérabilité de leurs collaborateurs à l'international⁴².

⁴⁰ MATHIE, Jérôme. « L'intelligence économique fait son apparition dans les normes ISO 9001 et 14001 ». LinkedIn. 26 octobre 2016.

⁴¹ LOUSSAIF, Catherine. « Risques géopolitiques : Quels enjeux systémiques pour les entreprises ? ». Actualité & Analyse et Tech & Entreprenariat. 06 mai 2017. Consulté le 01 juin 2017.

⁴² HOLLANDER, Alexandre. « Ce qu'une entreprise devrait faire pour assurer la sureté de ses employés à l'étranger ». Huffingtonpost (En ligne). 23 février 2016. Consulté le 11 mai 2017. Disponible sur http://www.huffingtonpost.fr/alexandre-hollander/surete-expatries-entreprise_b_9297454.html

Malgré la perception de l'insécurité à l'international de plus en plus forte, moins d'une entreprise sur quatre a un dispositif de gestion de crise des déplacements de ses collaborateurs à l'étranger. Cela souligne que les entreprises ne sont pas préparées à un tel risque et font appel à la chance lors de la survenue d'un événement : « *Nous avons eu de la chance* » témoigne le directeur de l'un de ces groupes dont des salariés se trouvaient à l'Hôtel Radisson à Bamako le 20 novembre 2016⁴³. Dans un contexte où la menace a pris racine dans notre quotidien, la sécurité de leur environnement international et national (prise d'otages dans une imprimerie à Dammartin en Goël, voiture bélier remplie d'explosifs contre une usine classée Seveso à St Quentin Fallavier, explosion d'une agence immobilière à Furiani...⁴⁴), les dirigeants doivent faire face aujourd'hui à des questions jusque-là peu ou pas abordées. Toutefois les lignes ont du mal à bouger et beaucoup de chemin reste à parcourir ; faute de moyens, de compétences, d'accompagnement dont l'Etat, les entreprises n'ont pas encore fait une priorité de la sécurité à l'étranger. Il convient de prendre conscience que la sécurité, loin d'être une entrave au développement du business à l'étranger, est une composante stratégique majeure de la performance économique, de la réputation et de l'image des entreprises⁴⁵.

En 2015, le Club des Décideurs de Sécurité des Entreprises (CDSE) avec AXA Assistance commande une enquête à Opinionway sur la « Sécurité des collaborateurs à l'international ». Celle-ci a été réalisée auprès de 303 dirigeants d'entreprises de plus de 50 salariés de tous secteurs d'activité dont 81% de PME. Toutes ont au moins un salarié envoyé hors de France au cours des 12 derniers mois. Ainsi 43% perçoivent comme une menace forte ou avérée (39%) l'insécurité internationale et 43% voient une aggravation de cette situation au cours des 5 prochaines années. Seulement 19% des entreprises se sentent directement exposées à l'international et pour 71%, l'envoi de collaborateurs à l'étranger présente autant de risque que par le passé et un tiers d'entre elles considèrent que la sécurité/sureté de leurs employés en déplacement à l'étranger présente un enjeu de plus en plus important. Toutefois, depuis les attentats de novembre 2015 en France, les chefs d'entreprises jugent désormais plus important le risque d'attentats (45%) que les risques routiers (27%) ou sanitaires (24%). Enfin, le Moyen Orient et l'Afrique demeurent les destinations où le plus de mesures de sécurité sont nécessaires (79% et 78%). Les entreprises non préparées à la crise... car pensant que les problèmes n'arrivent qu'aux autres et pas de conscience du risque pénal qui pèse sur elles pour 33%. Un quart seulement sont dotées d'un dispositif de gestion de crise lors d'un déplacement professionnel à

⁴³ MEDDAH, Assan. « Sécurité des collaborateurs à l'étranger, les entreprises font encore l'autruche ». L'Usine Nouvelle (En ligne). 11 février 2016. Consulté le 11 mai 2017. Disponible sur <http://www.usinenouvelle.com/article/securite-des-collaborateurs-a-l-etranger-les-entreprises-font-encore-l-autruche.N378533>

⁴⁴ WIKIPEDIA, « Chronologie des actes terroristes en France », modifié le 12 juillet 2017 à 10 :30. Consulté le 02 aout 2017. Disponible sur https://fr.wikipedia.org/wiki/Chronologie_des_actes_terroristes_en_France#Ann.C3.A9e_2015

⁴⁵ BEZIERS la FOSSE, Arnaud, FAGE, Sébastien, DARBON, Hubert. « Sécurité des entreprises : Construire une véritable stratégie ». LinkedIn le 23 mars 2017.

l'étranger et juste 25% connaissent et ont consulté le site de conseil aux voyageurs du Ministère des Affaires Etrangères. Enfin, la moitié d'entre elles ont souscrit un contrat spécifique d'assistance mais 50% disposent d'une personne identifiée au sein de l'entreprise en charge de la sûreté/sécurité (Directeur de la sécurité/sûreté ou DRH dans 72% des cas)⁴⁶.

Les fonctions et modes opératoires de la sûreté d'une entreprise à l'international sont sensiblement similaires aux modus operandi militaires (analyse de la menace et de son risque, planification, management de la sûreté, training, contrôle, reporting, RETEX, communication de crise...). Hors on ne passe pas d'une culture de l'uniforme à une culture civile du patrimoine de l'entreprise. Aussi, même si la tentation est grande pour une potentielle opérationnalité immédiate de recruter dans le vivier militaire ou faire appel à un prestataire dont les collaborateurs sont essentiellement issus de ce milieu ou des forces de sécurité internes le « retour sur investissement » n'offre pas forcément le rendu attendu. Outre le mauvais casting, les écueils sont nombreux : compétences réelles, dispositif plombant les actions ou au contraire sous-estimation du risque par la minimisation de ceux-ci, en comparaison du passé opérationnel de ces profils. Interne ou externe, le « Security Manager » a un rôle de conseiller et de responsable opérationnel de la sûreté, la responsabilité juridique, elle, incombe à l'entreprise surtout lorsqu'une faute inexcusable est recherchée (Jurisprudence Karachi, Jolo et Sanofi). Le challenge pour les entreprises est d'avoir « The right man in the right place »⁴⁷.

Les attaques de Bamako et de Ouagadougou ont montré que des failles existaient dans les dispositifs de sécurité des infrastructures hôtelières et de restauration, celles-ci agissant comme de véritables « pots de miel » pour les terroristes. Aussi, des audits et inspections peuvent être diligentés mais il convient en parallèle de former et d'informer les collaborateurs sur les bonnes pratiques, gestes qui sauvent et conduites à tenir en cas d'événements (prise d'otage, fusillade, explosion...). La « Spare House » offre une meilleure garantie de protection : secret des affaires, moins de turn over du personnel de maison et de sécurité, quartiers résidentiels avec plus forte présence des forces de l'ordre, possibilité de définir une « Safe Room » en cas de problème de sécurité et peu de concentration humaine. Alain Juillet, président du CDSE souligne : « *Si la chance sourit aux audacieux, ...elle favorise aussi ceux qui s'y sont préparés* ». Aussi, une réelle politique de gestion des risques s'impose face aux défis sécuritaires pour protéger les entreprises, leurs collaborateurs et leurs intérêts⁴⁸.

⁴⁶ Opinionway, *Le baromètre de la sécurité des collaborateurs à l'international* (En ligne). Vague 2b, Décembre 2015. Consulté le 02 aout 2017. Disponible sur https://www.cdse.fr/IMG/pdf/deuxieme_barometre_cdse_de_la_securite_des_collaborateurs_a_l_international.pdf

⁴⁷ LEFEVRE, Richard. « Passer du management de la sûreté sous l'uniforme, à celui de la sûreté de l'entreprise expatriée : « The right man in the right place ». *Carrière & Leadership*. 17 janvier 2017.

⁴⁸ HORNUS, David. « Sécurité des collaborateurs à l'international : les entreprises françaises mal placées ». *Experts de l'entreprise* (En ligne). 31 mai 2016. Consulté le 19 mai 2017. Disponible sur

Et pour la France ? La question du risque attentat semblait réservée aux sociétés implantées ou ayant des activités à l'étranger avec des collaborateurs expatriés ou voyageurs d'affaires dans des zones instables. Aussi, les chefs d'entreprises françaises voyaient ce risque comme improbable en France et reportaient la gestion par l'Etat de la sécurité sur les risques terroristes. Les exemples récents et précédemment cités ont changé la donne et nul dirigeant ne peut écarter la menace, directe ou indirecte, qui pèse sur les entreprises. Même si peu d'actions ont été menées contre des entreprises, les actes terroristes visant plus à marquer psychologiquement l'opinion publique que d'affaiblir l'économie du pays, le niveau d'entraînement et les capacités opérationnelles des organisations terroristes n'ont pas encore permis de s'attaquer à des cibles industrielles massives avec un fort potentiel de victimes. Toutefois, l'Etat est débordé et n'a pas les moyens d'intervenir et son aide n'est que très réduite (hors sites SEVESO). De plus, les contraintes de l'entreprise ne font pas partie de sa culture... Le transfert de compétence en termes de surveillance est en train de s'opérer vers des sociétés privées de sécurité avec des agents spécialement entraînés et armés. La CGPME et le syndicat national des entreprises de sécurité privée ont publié une liste de 10 mesures applicables aux PME, la première visant à « *évaluer les risques et identifier les menaces et leurs probabilités, les suivantes visant l'intégration de la sûreté en amont de l'organisation* ». Aussi, il n'est plus possible pour les entreprises de dire « Je ne savais pas ». Rappelons le, le dirigeant (personne physique) et l'entreprise (personne morale) sont responsables au civil et au pénal et les risques de mises en cause réels ; Article L. 421-1 du Code du travail, Article L. 452-1 du Code de la Sécurité Sociale et jurisprudence des arrêtés Jolo (2000) et DCN (2002). Toutefois, la prise en compte du risque sécuritaire attentat a un coût économique qu'il convient d'optimiser par une évaluation et un audit adéquat au même titre que tout autre investissement ou engagement de fonds par l'entreprise⁴⁹.

e. La santé et sécurité au travail

Depuis 1991, le Code du travail oblige les employeurs à prendre les mesures nécessaires pour protéger la santé physique et mentale des salariés (article L-4121-1). Cette obligation générale fonde la démarche de prévention dans l'entreprise. Ainsi, les employeurs doivent agir :

- Par des actions de prévention des risques professionnels et de la pénibilité au travail
- Par des actions d'information et de formation
- Par la mise en place d'une organisation de moyens adaptés en respectant les principes généraux de prévention (article L-4121-2)*

<http://www.expertsdelentreprise.com/Securite-des-collaborateurs-a-l-international-les-entreprises-francaises-mal>

⁴⁹ LEBOIS, Laurent. « Les dirigeants de PME-PME face au risque terroriste en France ». Journal de l'Economie.fr (En ligne). 04 avril 2017. Consulté le 11 mai 2017. Disponible sur http://www.journaldeconomie.fr/Les-dirigeants-de-PME-PMI-face-au-risque-terroriste-en-France_a4595.html

Depuis 2002, cette obligation de protection s'accompagne d'une obligation de résultat qui se traduit par l'ensemble des actions prises par l'employeur. Le résultat n'est pas l'absence d'atteintes physiques et mentale mais l'ensemble des mesures prises effectivement par l'employeur dont la rationalité, la pertinence et l'adéquation pourront être analysées et appréciées par le juge (PY Verkindt, 2007).

La cour de cassation de la chambre sociale, dans son arrêt du 28 février 2002 (arrêt n°835) précise « En vertu du contrat de travail le liant à son salarié, l'employeur est tenu en vers celui-ci d'une obligation de sécurité de résultat, notamment en ce qui concerne les maladies professionnelles contractées du fait des produits utilisés ou fabriqués par l'entreprise ».

Enfin, toujours depuis 2002, le manquement à l'obligation de sécurité et de résultat constitue une faute inexcusable. L'employeur peut être sanctionné pour une infraction aux règles de sécurité civile et au pénal. La cours de cassation de la Chambre sociale (arrêt n°835) définit la faute inexcusable comme un manquement de l'employeur à son obligation de sécurité de résultat lorsqu'il avait (ou aurait dû avoir) conscience du danger auquel était exposé le salarié et qu'il n'a pas pris les mesures nécessaires pour le protéger.

* Une démarche de prévention des risques professionnels se construit en impliquant tous les acteurs concernés et en tenant compte des spécificités de l'entreprise (taille, moyens mobilisables, organisation, sous-traitance, co-traitance, intérim, filialisation, implantation géographique multiple, présence de tiers externes comme du public ou des clients...). Pour mettre en place une démarche de prévention, il est nécessaire de s'appuyer sur les **neuf grands principes généraux** qui régissent l'organisation de la prévention⁵⁰.

- **Éviter les risques, c'est supprimer le danger ou l'exposition au danger.**

- **Évaluer les risques**, c'est apprécier l'exposition au danger et l'importance du risque afin de prioriser les actions de prévention à mener.

- **Combattre les risques à la source**, c'est intégrer la prévention le plus en amont possible, notamment dès la conception des lieux de travail, des équipements ou des modes opératoires.

- **Adapter le travail à l'Homme**, en tenant compte des différences interindividuelles, dans le but de réduire les effets du travail sur la santé.

⁵⁰ INRS. « Introduction à la prévention ». Site web de l'INRS Consulté le 04 aout 2017. Disponible sur <http://www.inrs.fr/demarche/principes-generaux/introduction.html>

- **Tenir compte de l'évolution de la technique**, c'est adapter la prévention aux évolutions techniques et organisationnelles.
- **Remplacer ce qui est dangereux par ce qui l'est moins**, c'est éviter l'utilisation de procédés ou de produits dangereux lorsqu'un même résultat peut être obtenu avec une méthode présentant des dangers moindres.
- **Planifier la prévention** en intégrant technique, organisation et conditions de travail, relations sociales et environnement.
- **Donner la priorité aux mesures de protection collective** et n'utiliser les équipements de protection individuelle qu'en complément des protections collectives si elles se révèlent insuffisantes.
- **Donner les instructions appropriées aux salariés**, c'est former et informer les salariés afin qu'ils connaissent les risques et les mesures de prévention.

Depuis 1991 et la transposition de la directive européenne visant l'amélioration de la sécurité et de la santé au travail, le champ réglementaire ne cesse de croître. On recense aujourd'hui plus de 2040 obligations réglementaires dans le champ de la santé au travail⁵¹

L'Etat (DIRRECT Ministère du Travail...), les organisations professionnelles patronales (CPME, MEDEF, OPPBTP...) et salariées (syndicats), les organismes consulaires (CCI) et professionnels (chambres des métiers), les organismes privés (INRS, CARSAT) participent à aider les entreprises dans leurs démarches de prévention. Le site officiel de l'administration française reprend notamment l'ensemble des obligations de l'employeur en terme de santé sécurité au travail⁵².

A ces obligations réglementaires de moyens et de résultats, les entreprises sont redevables auprès de l'URSSAF d'une cotisation au titre des accidents du travail et des maladies professionnelles avec un principe où plus il survient d'accident du travail (AT) et de maladies professionnelles (MP) dans l'entreprise, plus la cotisation est élevée. Pour les entreprises de moins de 20 salariés, celle-ci est calculée sur la base d'un taux collectif variant selon l'activité et fixé indépendamment du nombre d'AT/MP touchant leurs salariés. Par exemple, ce taux est fixé à 2% dans le secteur de la coiffure et à 6% dans celui de la fabrication de produits en béton. Pour les entreprises dont l'effectif est compris entre 20 et 149 salariés, celles-ci cotisent sur la base d'un taux mixte comprenant une part du taux collectif applicable à leur

⁵¹ BDO. « Evolution des principales obligations réglementaires dans le domaine de la santé au travail ». Malakoff Mederic (En ligne). Consulté le 31 mai 2017. Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/evolution-des-principales-obligations-reglementaires>

⁵² Service-Public. « Sécurité et santé au travail : obligations de l'employeur ». Service-Public.fr (En ligne). Consulté le 31 mai 2017. Disponible sur <https://www.service-public.fr/particuliers/vosdroits/F2210>

activité et une part de leur taux individuel qui est défini en fonction du nombre d'AT/MP survenus dans l'entreprise au cours des 3 dernières années⁵³.

Au-delà des obligations réglementaires (Ex. Pénibilité physique et mentale, risques psychosociaux, risques physiques, incendie, secours à personne, affichage et informations obligatoires, obligations en droit du travail pour les entreprises ayant un effectif jusqu'à 500 salariés, DUERP...⁵⁴), l'engagement des chefs d'entreprises est la première condition fondamentale à toute démarche de prévention. Il est le seul à pouvoir impulser celle-ci et définir son intégration dans l'entreprise, présenter les enjeux et la légitimer. La prévention doit faire partie de la stratégie de l'entreprise et doit être traitée comme tout autre projet. Toutefois, une démarche de prévention ne se prépare, ni ne s'effectue seul. Tous les acteurs de l'entreprise ont un rôle à jouer, du simple opérateur au cadre dirigeant. Charge au chef d'entreprise de mobiliser ses équipes mais aussi les acteurs externes de la prévention (CARSAT, DIRRECT, Sapeurs-Pompiers...). « *Nous avons une accidentologie élevée liée à la préparation de commandes. L'objectif de la démarche était de réduire les risques liés à la manutention manuelle. Tous les acteurs de l'entreprise se sont impliqués et nous avons amélioré à la fois notre productivité, diminué la sinistralité mais également amélioré le climat social de notre entrepôt* » témoigne Monsieur F., Directeur d'un entrepôt dans le secteur de la logistique alimentaire.⁵⁵ Pour Johan Galliano, responsable QHSE chez BLH PIM, Concilier réglementation et dimension TPE/PME est possible mais cela demande un vrai engagement de la part de l'entreprise. La majorité des actions passent par la formation (risque chimique, routier, gestes et postures...), l'organisation de réunions internes pour faire des points sur la réglementation et la sensibilisation des nouveaux arrivants. Dans une entreprise familiale, le dialogue est de mise plus que l'injonction et l'implication des salariés comme par exemple dans le choix des EPI⁵⁶.

Selon une enquête commandée par l'INRS à l'Institut Viavoice sur les risques professionnels dans les entreprises de moins de 50 salariés et réalisée entre novembre 2014 et janvier 2015 auprès de 1002 chefs d'entreprises, celle-ci montre cependant un net recul des questions de SST par rapports aux enquêtes de 2007 et 2010. Ainsi, 35% des chefs d'entreprises de structures de 10 à 49 salariés citent la SST comme faisant partie des 2 préoccupations

⁵³ SOUSTRE, Coralie. « De l'intérêt de prévenir les accidents du travail et les maladies professionnelles ». Business les Echos (En ligne). 23 mars 2017. Consulté le 11 mai 2017. Disponible sur <https://business.lesechos.fr/entrepreneurs/ressources-humaines/9550936-de-l-interet-de-prevenir-les-accidents-du-travail-et-les-maladies-professionnelles-307711.php>

⁵⁴ Malakoff-Médéric. « Répondre aux obligations réglementaires en santé et sécurité ». Malakoff-Médéric Entreprises (En ligne). Consulté le 31 mai 2017. Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires>

⁵⁵ Malakoff Médéric. « Mettre en place une démarche de prévention ». Malakoff Médéric (En ligne). Consulté le 31 mai 2017. Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/mettre-en-place-une-demarche-de-prevention>

⁵⁶ Agir Mag. « La santé sécurité dans une PME ». Magazine Agir Mag N°48. Parution Septembre/Octobre 2013. Consulté le 01 juin 2017. Disponible sur <http://www.agir-mag.com/sante-securite-sante-securite-au-travail-pme.html>

principales (37% en 2010) et ce, loin devant les préoccupations financières. 9% des petites entreprises considèrent que leur activité ne présente pas de risque particulier et ne voient pas l'intérêt de la mise en place du Document Unique d'Évaluation des Risques Professionnel (DUERP) contre 11% en 2010 et seulement 46% ont rédigé ce document. 84% des petites entreprises déclarent disposer d'outils pour faire le DUERP et 43% ne manquer de rien pour prendre des décisions en termes de SST. Pour les entreprises qui identifient des manques, ce sont les problèmes de temps et de financement qui ne permettent pas de rentrer dans la démarche. Toutefois, l'INRS relève que sur la période écoulée, les dirigeants de petites entreprises sont plus nombreux à déclarer avoir mis en œuvre des mesures de prévention ; 93% pour des moyens de protection individuelle, 81% sur des actions d'information, 71% pour des actions de formation, 68% des interventions sur l'organisation et le management et 67% sur des moyens de protection collective. A l'INRS de conclure que « *la prévention est principalement perçue par les chefs d'entreprise comme une contrainte* » et que « *le minimum est perçu comme suffisant* »⁵⁷.

Obligatoire depuis 2001 pour toutes les entreprises à partir de 1 salarié, le Document Unique d'Évaluation des Risques Professionnels⁵⁸ permet d'analyser les risques encourus au sein de l'entreprise (dont en annexe l'évaluation des expositions individuelles liées à la pénibilité : loi du 20/01/2014) et de mettre en place les plans d'actions adaptés. Véritable outil de prévention, souple et évolutif, le DUERP, établi par les différents acteurs de l'entreprise (dirigeants, salariés, CHSCT...), permet de formaliser la mise en place d'une démarche de prévention des risques professionnels et d'évaluer les actions mises en place. Celui-ci doit être mis à jour au moins une fois tous les ans. Depuis 2008, le DUERP doit être accessible à tous les salariés, élus du personnel et acteurs de la santé au travail. Au-delà d'une obligation réglementaire, le DUERP contribue au dialogue social, l'amélioration des conditions de travail et s'inscrit ainsi dans une démarche au service de la performance de l'entreprise. A ce jour, ¾ des entreprises ont réalisé leur DUERP⁵⁹. « *Il faut démystifier le DU : ce n'est pas un exercice complexe pour l'entreprise, ni une paperasse administrative de plus. Réaliser un DU est une démarche collective, vivante, qui permet de parler du travail dans l'entreprise sous un angle de la sécurité, de la santé et du bien-être ? C'est une démarche source de progrès et de performance pour les collaborateurs comme pour l'entreprise* » (Dr Marie Christine MARIE-SOULA, médecin du travail, intervenant en prévention des risques professionnels).

Pour un euro investi en santé sécurité au travail, le retour sur investissement est de 2 à 5 euros, voir 13 euros pour les risques psycho-sociaux et ce, avec un retour sur investissement

⁵⁷ RADISSON, Laurent. « La santé sécurité au travail de moins en moins prioritaire pour les TPE-PME ». Actu-environnement.com (En ligne). 13 mars 2015. Consulté le 01 juin 2017. Disponible sur <https://www.actu-environnement.com/ae/news/sante-securite-travail-sst-tpe-pme-recul-inrs-24092.php4>

⁵⁸ Directive cadre 89/391/CEE, loi n°91-1414 du 31 décembre 1991, Décret n°2001-1016 du 05 novembre 2001 et circulaire n°6 du 18 avril 2002

⁵⁹ Malakoff Médéric. « Obligatoire : Réaliser le document unique ». Malakoff Médéric (En ligne). Consulté le 31 mai 2017. Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/le-document-unique-une-obligation>

de 1,5 an ont conclu plusieurs études provenant des USA ou d'Europe du Nord (Allemagne, Scandinavie, Pays Bas), quelle que soit l'activité, les résultats sont là ; en clair, si vous dépensez en santé sécurité au travail, vous gagnez de l'argent ! C'est une bonne entrée en matière car dans tous les cas, il faut parler leur langage et répondre à leurs préoccupations. En parallèle de rares études sur ce sujet ont été conduites en France (INRS et OPPBTP) montrant une approche de la SST par la morale et non l'angle économique. Ces résultats s'expliquent par la combinaison de plusieurs résultantes comme une baisse de l'absentéisme, du turn over, meilleure motivation des salariés par le signal envoyé par le dirigeant en termes de bienveillance à leur égard. L'étude menée par l'OPPBTP a révélé un gain par salarié de PME de 1600 à 8200 € selon le nombre de salariés. Ainsi, le retour sur investissement est plus important pour une TPE, par rapport à une PME⁶⁰.

f. Quelle réponse des entreprises face aux situations de crise ?

Accident à la centrale de Fukushima-Daiichi (2011), événements dans le secteur pétrolier et l'aéronautique en 2010, effondrement de l'économie en 2008, explosion de l'usine AZF en 2001... sont autant de situations qualifiées de crise. La diversification, multiplication et amplification de ces événements s'accompagnent intrinsèquement avec des phénomènes de déstabilisation, sur-médiatisation et atomisation des systèmes. Avec une sensibilité propre, la pensée occidentale considère que nous évoluons dans un écosystème qui se maintient en équilibre et que nous cherchons de façon perpétuel à garder cet équilibre tout en essayant de revenir continuellement à cet état ancien. *La pensée orientale quant à elle voit plutôt dans toute modification d'équilibre une opportunité de changement donnant la possibilité de créer un nouvel équilibre.* Le dénominateur commun à ces deux philosophies est qu'il n'est possible de résoudre un problème qu'en connaissance sa nature et son mécanisme. Aussi, le mot crise, pourrait se définir « *comme étant les modifications de l'état d'équilibre propre à un système ou une organisation, pouvant amener à sa rupture* » (Cormier et Donet-Mary, 2011) mais aussi, selon les mêmes auteurs comme les variations de l'état d'équilibre propre à un système ou une organisation, avec 3 niveaux de variations : perturbation, déséquilibre, rupture. De même elle comporte des modalités de cinétique, courte ou longue, et peut se déclencher soit de manière prévisible (risque non maîtrisé) ou inopiné (...). Cette dernière définition rapproche le modèle scientifique de Gilbert Boutté (2006), au management. Celui-ci a adapté le modèle générique en 2D de Nioche (1985) qui intègre le processus décisionnel et la prise en compte de l'environnement. Plus tard, les recherches de Dufès et Ratinaud (2013) ajouteront la contrainte du temps créant ainsi un modèle tridimensionnel ou « 3D ». Une des erreurs des trente années passées, est d'avoir pris les situations de crise comme des événements isolés et non abordés comme des situations complexes issues d'un monde globalisé, pouvant toucher toute organisation à

⁶⁰ RICHER, Martin. « Pour un euro investi en santé sécurité au travail, le retour sur investissement est de 2 à 5 euros ». Management et RSE (En ligne). 06 juin 2016. Consulté le 04 aout 2017. Disponible sur <http://management-rse.com/2016/06/06/euro-investi-sante-securite-travail-retour-investissement-de-2-a-5-euros/>

chaque instant et partout. Les diverses situations de crises que nous connaissons sont des alertes lancés aux dirigeants. La pire des choses serait de ne pas prendre en considération celles-ci, de rester dans une posture attentiste et refuser toute préparation ; anticipation, prévention, formation, entraînement, organisation... Déjà en 1976, Jean Monnet citait dans ses mémoires : « *Les hommes n'acceptent le changement que dans la nécessité et ils ne voient la nécessité que dans la crise* ». Cependant l'embarra à aborder la notion même de crise serait aussi avouer ses faiblesses et vulnérabilités réelles ou supposées⁶¹.

Pour certains la crise provient « *d'un événement qu'il est vain de vouloir toujours prévoir* »⁶² et qu'à ce titre « *anticiper une gestion de crise résulte de l'utopie et seule la compétence, la réactivité et l'abnégation seront plus efficaces qu'un plan inapplicable* »⁶³ et donc, que quel que soit la préparation pouvant être faite en prévision d'une crise, celle-ci ne répondra jamais à la situation. Même si il y a autant de situations de gestion de crise que de crise, rien faire ne serait que le résultat d'une vision fataliste et d'immobilisme. Pour d'autres, la crise est vue comme une « *situation sortant du cadre habituel des incidents connus, avec la nécessité⁶⁴ de prendre en urgence des décisions stratégiques et d'organisation* » marquant l'importance voir l'indispensabilité de la préparation à la gestion de crise.

Pour Le Roy Ladurie (1976), la notion de situation de crise « *représente une phase de rupture, négative et momentanée* ». Les phénomènes amenant à une situation de crise se positionne dans un paradigme où ils ne relèvent plus de l'imprévisibilité, instabilité, génératrice et sporadique, mais visent un ensemble de phénomènes variables considérés comme interconnectés et interdépendants. Ainsi, pour Dautun (2009), les situations de crise sont de nos jours « *avant tout systémiques* ». *Les différences de racines, transmissions et évolutions sociales marquent des différences dans le niveau d'équilibre recherché par chaque groupe, communauté, institution ou organisation. La combinaison des enjeux, cultures, normes, valeurs et éthiques de chaque acteur constitue un système qui entraîne des variations de niveau d'équilibre. Toutes ces tensions oppositions et combinaisons des équilibres vulnérables entraînent un équilibre fragile d'un système⁶⁵*. L'équilibre correspondrait alors à un « *état idéal, instable, fait d'oscillations et de mouvements constants* » (Pauchant et Mitroff, 1995). Dans une évolution permanente, tout système tend à atteindre, à vivre et à pérenniser un état d'équilibre précaire pour lui-même sans basculer. Ainsi le phénomène de situation de crise étudié ici renvoie à la notion de déséquilibre. Pour Dufès et Ratinaud (2013), une situation de crise est « *consécutive à une rupture d'équilibre avérée des fondamentaux d'un ou plusieurs systèmes, une situation de crise s'observe par un*

⁶¹ DONET-MARY L. DUFES E, RATINAUD C, TORMOS G « La crise : du minimum requis au minimum commun ». Dossier ENSOSP.

⁶² LIBAERT, Thierry. Crise de 1 à 150. OIC éditions, Collection 360°. 2007. Page 6.

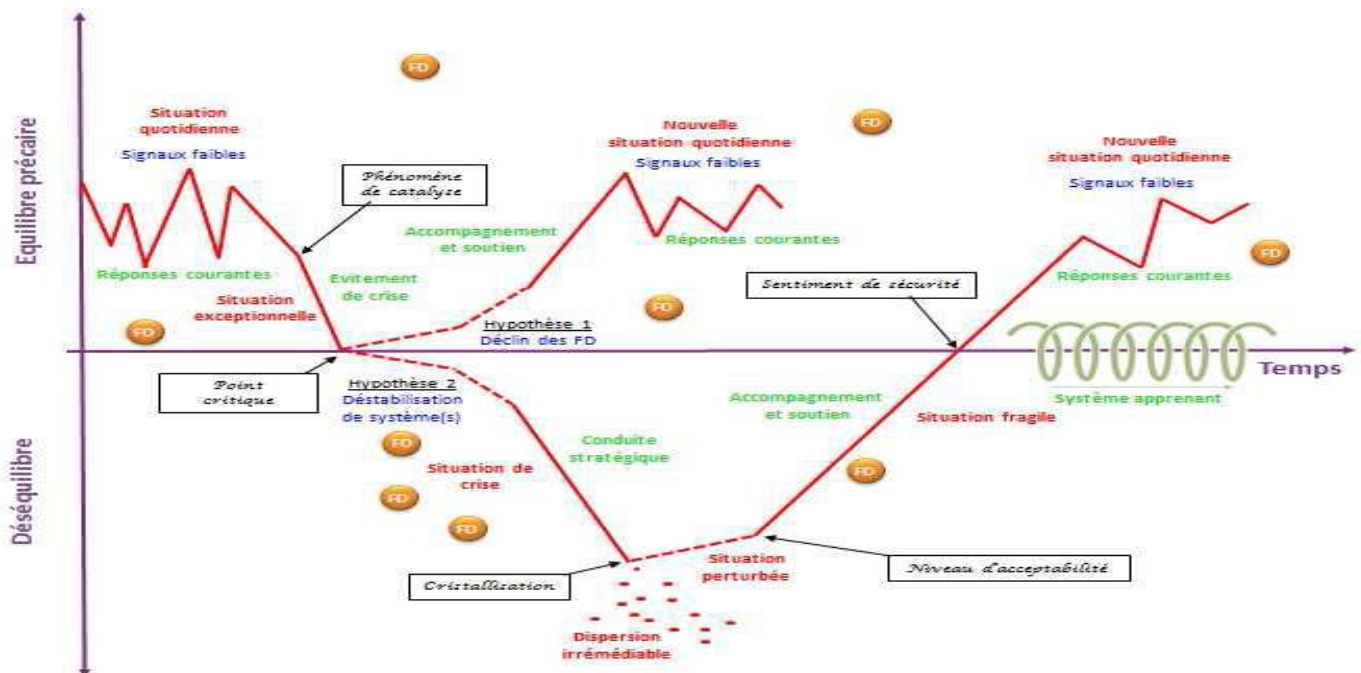
⁶³ Propos recueillis dans les réponses du questionnaire « votre entreprise a-t-elle un plan de continuité d'activité ? »

⁶⁴ COMBALBERT, Laurent. Management des situations de crise. ESF Editeur. Série « Entreprise » Paris. 2005. Page 23.

⁶⁵ DUFES et RATINAUD, « Situations de crise : une réponse modélisée en 3D » Dossier ENSOSP 2013.

état de désordre profond de ses acteurs et/ou de désintégration organisationnelle, impliquant des dommages et générant des nécessaires prises de décision dans un contexte d'ambiguïtés et d'incertitudes, le tout influencé par une maille temporelle contrainte ». Ainsi, une situation de crise représente une rupture d'équilibre d'un ou plusieurs systèmes. Tout système est vivant et donc sujet à un cycle de vie. Ramené à la notion de situation de crise, nous parlerons du « cycle de vie d'un processus de déséquilibre » dont le développement de sa manifestation peut être modélisé. Ce modèle met en relation deux dimensions : la temporalité (abscisse) et les facteurs d'équilibre et de déséquilibre (ordonnée). La présentation des deux dimensions donne les points de départ et de sortie d'une situation de crise lors de vie d'un déséquilibre systémique. Ce graphique permet de visualiser cinq autres périodes :

- Vie quotidienne : Equilibre précaire
- Moments instables, compliqué et d'urgence : Situation exceptionnelle
- Post crise : Situation perturbée
- Instants de reconstruction : Situation fragile
- Reprise de la vie ordinaire, journalière : Nouvel équilibre précaire



Cycle de vie d'un processus de déséquilibre - (Dufès et Ratinaud, 2013)

Sur l'inspiration des systèmes de management de la santé et de la sécurité au travail (INRS, 2009) il est possible d'organiser les facteurs de déséquilibre en quatre catégories :

- **H**umain
- **O**rganisation
- **M**oyens
- **E**nvironnement (et/ou **E**conomique)

L'acronyme généré par cette déclinaison des facteurs de déséquilibre illustre la place dominante de l'**HOMME** dans leur production. Accidents explosion de la navette Challenger, naufrage du Costa Concordia...), sinistres (explosion au gaz d'immeubles...) le facteur humain prime et ce, jusqu'à 90% des cas pour les sites industriels classés selon le Bureau Analyse des Risques et Pollutions Industrielles.

Citons quelques exemples de facteurs de déséquilibres concernant plus spécifiquement le monde de l'entreprise :

Humain	Concurrence au niveau du pouvoir, manque de flexibilité dans le processus de prise de décision, Méconnaissance, in-expérimentation, non formation des acteurs, défaut de culture de sécurité , absence d'anticipation, absence de confiance au sein de l'équipe...
Organisation	Pas d'organigramme, organisation trop normée, complexité organisationnelle, absence de décideur, difficulté à s'adapter...
Moyens	Manques de ressources disponibles, inadaptation des moyens...
Environnement et/ou Economique	Soudaineté, cascade d'événements, effets domino, géographie, pression médiatique, des actionnaires, des syndicats, des financeurs, des clients...

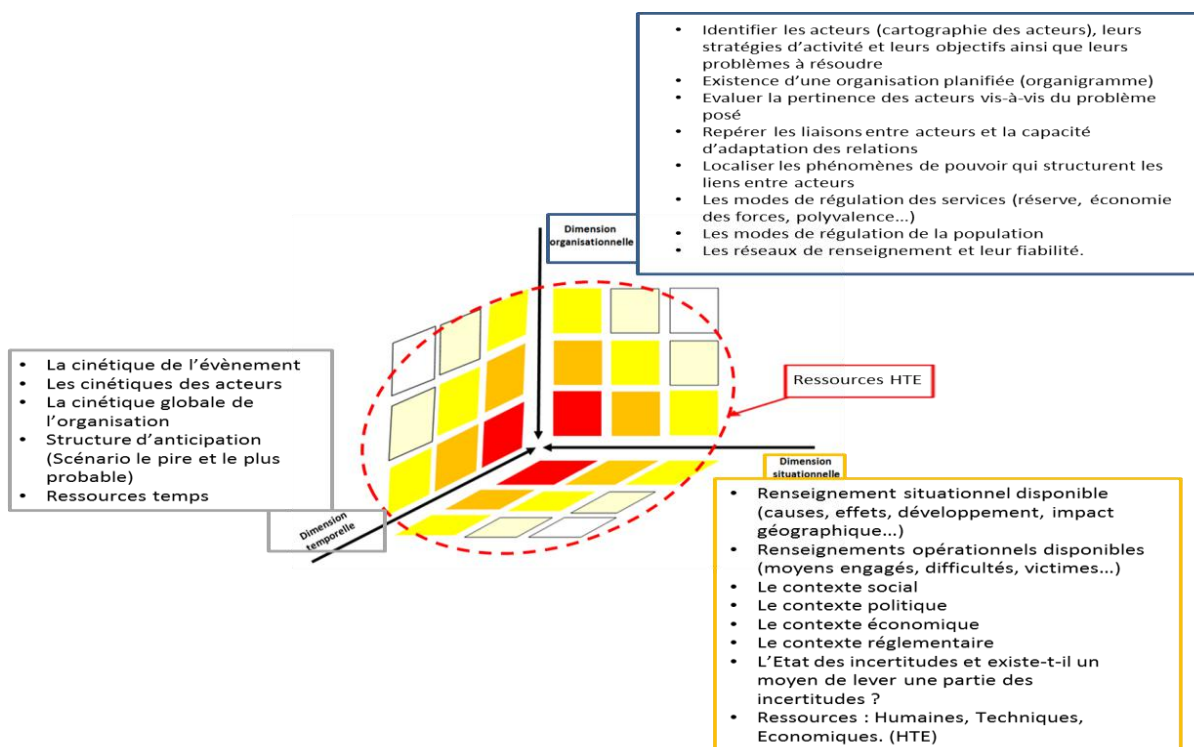
Jean Pierre Nioche (Anastassopoulos et al., 1985, 1988) donne un modèle de « management stratégique » intégrant la complexité et définit les mécanismes tendant à faire basculer une situation en « crise ». Vingt ans plus tard, ce modèle est revu par le colonel Gilbert Boutté (2006). Les bases de la modélisation sont posées... Leur modèle permet de reconnaître et comprendre le processus décisionnel en situation de crise en prenant deux dimensions : « ENVIRONNEMENT – SITUATION » et « POUVOIR – DECISION ».

		ENVIRONNEMENT REEL ET/OU PERCU				
		Stable	Prévisible	Turbulent		
		SITUATIONS DE DECISION				
POUVOIR	MODELES DE DECISION	Émergente	Anticipée	Occurrente		
		Concentré	ACTEUR UNIQUE COGNITIF	Ajustement	Rationalisation	« Règles de Part »
		Réparti	ORGANISATIONNEL	Adaptation administrative	Plan de secours et Processus formalisé	Plan de secours
Disputé	POLITIQUE	Ajustement consensuel	« Jeu politique »	Crise		



Modèle de Nioche appliqué au processus décisionnel en situation de crise (Boutté, 2006)

Les principes d'évitement de crise consistent donc à éviter le basculement de l'une des huit situations vers la case « crise ». Pour Dufès et Ratinaud (2013), la pression du temps paraît un facteur de déséquilibre qui en matière de crise impacte le monde de l'entreprise (et de la sécurité civile). Cette notion de temps est évoquée dans les études de Lagadec (1991), Boutté (2006) ou encore Heiderich (2010). Aussi un troisième axe au modèle est apparu comme une évidence. Ces trois dimensions combinées ont donné naissance à un modèle en 3 dimensions, appelé « modèle 3D de la déstabilisation de système (s) en situations de crise ».



Le 3D de la déstabilisation de système (s) en situations de crise - Dufès et Ratinaud, 2013

Nous retrouvons 27 situations de déstabilisation de systèmes représentées en cinq couleurs :

- **Blanc ivoire** : Situations équilibre précaire - **Jaune** : Situations exceptionnelles
- **Orange** : Hypothèses de déclin ou de déstabilisation - **Rouge** : Situations de crise

Ce modèle intègre le facteur humain car générateur principal comme nous l'avons vu précédemment, de facteurs de déséquilibre. Pour la partie « situationnelle et organisationnelle », les décisions prises pour répondre à une situation inédite, se basent sur l'expérience de celui qui les prends. La dimension « temporelle et organisationnelle » met l'organisation aux prises d'une forte pression du temps. Dans ce cas, une situation de crise peut naître alors que l'événement initial n'était qu'un phénomène « majeur ». Enfin la face alliant la dimension « situationnelle et temporelle » il est admis qu'une situation de crise puisse survenir sans qu'il y ait un pouvoir disputé dans l'organisation. La modélisation du cycle de vie d'un processus de déséquilibre, de la déstabilisation de système(s) et du management des situations de crise offre l'opportunité aux acteurs de mieux se préparer pour faire face aux déséquilibres récurrents qui menacent les organisations dans le monde incertain actuel. Les paroles de Kurt Lewin (1951) « *Il n'y a rien de plus pratique qu'une bonne théorie* » rassureront les décideurs les plus pragmatiques face à de tels outils, mis à disposition des gestionnaires de crises. Le décideur peut orienter sa stratégie pour atteindre un nouvel équilibre. Celle-ci se construira alors soit sur une adaptation de l'organisation, soit une meilleure compréhension de l'environnement visant à réduire les incertitudes, soit à faire face aux aléas du temps⁶⁶.

L'impact d'une situation exceptionnelle sur une entreprise peut engendrer une perte partielle ou totale de son activité, véhiculer une image négative, faire perdre en notoriété et avoir des conséquences financières voir juridiques lourdes. Aussi il convient à chaque entreprise, quel que soit sa taille ou son secteur d'activité, de se préparer à une telle situation. Plan de gestion de crise, formation des collaborateurs qui seront impliqués, plan de continuité d'activité... sont autant de dispositifs permettant une réaction rapide et sereine permettant un traitement rapide de la situation en vue d'un retour à la normale. Faire appel à l'expérience ne suffit pas ou ne peut être considéré de part une faible occurrence de gestion de situation de crise. Les principes de gestion de crise sont encore embryonnaires. Peu de méthodes d'évaluation faisant consensus existent tant sur les pratiques que sur le cout de cette gestion et de ses conséquences.

Une des difficultés pour les dirigeants « convaincus », est d'amener leurs collaborateurs et leurs partenaires (clients, fournisseurs...) à prendre conscience qu'un accident grave est susceptible de créer une situation de crise. Toutefois, imprévisible, l'événement nécessite de

⁶⁶ DUFES et RATINAUD, « Situations de crise : une réponse modélisée en 3D » Dossier ENSOSP 2013.

la part de l'entreprise une organisation spécifique de circonstance : une gestion de crise⁶⁷. La problématique des interactions de moyens et de leur compatibilité nécessite un minimum de culture commune entre les acteurs. Les managers devraient connaître les différents acteurs concourant à la gestion de crise afin de partager leurs spécificités et diversités mais aussi leurs limites. Cette dimension s'applique également au manager lui-même.

Ainsi, l'une des composantes à la gestion de crise que nous verrons ici, est de la préparer. L'entreprise doit affronter un événement majeur mettant en péril la poursuite de son activité. La préparation de la gestion de crise se fait au sein même de l'entreprise et nécessite un engagement jusqu'au plus haut niveau du management. Celui-ci doit identifier les parties prenantes (collaborateurs, médias, pouvoirs publics, partenaires sociaux...) et nouer des liens pour apprécier les sensibilités de chacun et seuil d'acceptabilité du risque. En tout état de cause la préparation de la crise doit être générale pour être efficace ; elle doit s'adapter à toute survenance d'événement majeur venant impacter l'activité de l'entreprise. L'indisponibilité, la disparition ou l'altération de ces ressources peut entraîner le dysfonctionnement de l'entreprise d'où la nécessité de mettre en place un Plan de Continuité d'Activité (PCA) afin que l'entreprise puisse poursuivre à minima son activité ou la reprendre dans les meilleurs délais et de façon graduelle. Il convient donc de mesurer les conséquences de la survenue de crise. Aussi, au-delà de leur propre vulnérabilité, les entreprises doivent se préoccuper de la capacité de leurs partenaires ou prestataires critiques car la défaillance de l'un d'entre eux affecterait de fait le fonctionnement de celles-ci. Aussi, la problématique de la gestion de crise doit être appréhendée comme une véritable stratégie d'entreprise⁶⁸.

La rencontre entre entreprises, organisations professionnelles, acteurs de la gestion de crise (publics et privés) doit permettre de créer de véritables moments de partages de points de vues, d'échanges, de débats afin de favoriser l'émergence de bonnes pratiques « d'évitement de crise » et par extension de « gestion de crise ». Des cursus de formation et d'entraînements et une planification associée pourront naître de cette dynamique faire gagner en efficacité et efficience. Mais finalement, à la vue des éléments abordés, sommes-nous toujours dans une démarche de gestion de crise ? Parler au 21^{ème} siècle de gestion de crise semblerait être galvaudé. Globalisation des organisations et des menaces, effondrements des systèmes réputés stables et immuables, révolutions politiques, sociales, culturelles, nouveaux visages des situations de crise amenant de nécessaires réponses adaptées de sécurité, en terme de capacité à se préparer, à comprendre la complexité de l'événement et à s'adapter à celui-ci, ne correspondraient ils pas à parler de « Management

⁶⁷ MERCADAL, Laurent. « Préparer ses collaborateurs à la crise, la vraie... » LinkedIn. 31 mai 2016. Consulté le 27 juillet 2017.

⁶⁸ LEVINE, Jehna, VRAIE, Benoit. « Gestion de Crise et continuité d'activité : la survie de l'activité entreprise suite à la survenue d'un incident ». Portail de l'Intelligence Economique - Jeudis du Risque (En ligne). 23 février 2017. Disponible sur <https://portail-ie.fr/analysis/1549/jdr-gestion-de-crise-et-continuite-dactivite-la-survie-de-lactivite-entreprise-suite-a-la-survenance-dun-incident>

de crise ». A la fin du 16^{ème} siècle, manager est défini comme « *l'action de conduire, de diriger, d'entraîner* » (Rey, 2010). Partant de cette définition, le terme de management des situations de crise se traduit par l'art de définir, préparer, gérer, diriger, décider et organiser les ressources à l'aide de stratégies, principes, méthodes, techniques et outils. Elément consolidant ce principe, le glossaire 2009 du droit du danger précise que le « *management concerne la stratégie, la politique et ses objectifs, les décisions portant sur un programme ou un plan. Le management de crise se positionne déjà en amont de la gestion, défini l'organisation et amène à la prise de décisions* ». L'origine étymologique du mot crise du grec et latin « crisis » qui signifie « décider » donne ou du moins renforce tout son sens. L'art du management ne peut donc être normalisé mais seulement son organisation (Seillan, 2008). Pour Dufès et Ratinaud (2013), le management des situations de crise se définit « **comme la politique, la stratégie, la tactique et les opérations dans la préparation et la gestion aux situations de crise portant sur sept domaines d'activité : l'analyse des risques, la planification, l'évitement de crise, la conduite de crise, la stabilisation et l'organisation apprenante, le tout accompagné d'une stratégie de communication de crise** ».



Dans son livre « *Le Management des Situations de Crise* », Laurent Combalbert insiste sur la communication comme élément capital de la gestion de crise car si elle n'est pas bien préparée ou gérée, peut être dangereuse pour l'entreprise en terme d'image, voire pire, être « crisogène ». A l'ère de l'internet et des réseaux sociaux, une bonne gestion de crise nécessite de la lumière et de l'information portés par ces vecteurs. Pour Leslie Graine-Ross, « *le silence n'est aujourd'hui plus une option et la proactivité est désormais de mise en telle situation* »⁶⁹. Pour le grand public, les deux facteurs les plus importants quant à la perception d'une entreprise, sont l'opinion que les consommateurs ont de celle-ci (88%) et

⁶⁹ GRAINES-ROSS, Leslie. « *What CEOs Should Know About Speaking Up on Political Issues* ». Harvard Business Review (En ligne). 2017. Consulté le 11 mai 2017. Disponible sur <https://hbr.org/2017/02/what-ceos-should-know-about-speaking-up-on-political-issues>

la manière dont elle réagit à une crise (85%) aussi, tout dirigeant se doit de prendre en considération cette dimension médiatique qui peut se révéler salvatrice ou délétère⁷⁰. Pas d'actions sans réactions ! Quelques règles simples sont à intégrer pour les dirigeants :

- Dire quelque chose : Prendre position sur l'affaire en court
- Etre prêt à toute éventualité : le temps moyen de réponse d'une entreprise lancée au cœur d'un imbroglio médiatique est de 38 heures ce qui est beaucoup trop long d'où la nécessité de se préparer en amont et parer rapidement
- Humaniser le discours : Conjuguer habilement le relationnel et l'émotif est une formule gagnante
- Chercher des appuis : Mobiliser les entreprises ou organisations qui vous accompagnent
- Etre cohérent avec les valeurs de l'entreprise : Communiquer en interne et externe

Et tout cela, sans jamais laisser les médias et médias sociaux occuper l'espace à sa place⁷¹.

Poussées par la nécessité de ne pas être dépassées par la concurrence, les entreprises pensent à ce qui n'a pas été pensé pour trouver de nouveaux produits ou services. Le management de situations de crises se voudrait évoluer dans une dynamique de sécurité répondant au même principe « penser ce qui n'a pas été pensé ». Il est nécessaire d'agir de manière adaptée pour infléchir le cours des événements : « *il faut agir en homme de pensée et penser en homme d'action* » (Gergson, 1969) et agréger cette intelligence pour qu'une intelligence collective naisse au service des phénomènes à venir. Aussi, rendre l'individu plus responsable et proactif semble être un progrès important tout comme l'adaptabilité individuelle permettrait de renforcer la réactivité des organisations dans le management de situations de crise. Ainsi, la culture de sécurité est une importante contributrice au développement des capacités d'anticipation, de compréhension, d'accompagnement et d'exploitation de ces situations et faciliter la résolution de crise.⁷²

⁷⁰ Etude de Weber Shandwick et KRC Research « *The Company behind the Brand II : In Goodness We trust* » 2017. Consulté le 11 mai 2017. Disponible sur <http://www.webershandwick.com/uploads/news/files/company-behind-the-brand-in-goodness-we-trust.pdf>

⁷¹ NORMANDIN, François. « Communication de crise : quand le silence tue... ». Revue gestion.ca (En ligne). 20 février 2017. Consultée le 11 mai 2017. Disponible sur <http://www.revuegestion.ca/agir/communication-de-crise-silence-tue/>

⁷² DONET-MARY L. DUFES E, RATINAUD C, TORMOS G « La crise : du minimum requis au minimum commun ». Dossier de l'ENSOSP.

3) Qu'est-ce que la culture de sécurité d'entreprise en France ?

a. Définition du concept de culture

En français, le mot « culture » possède plusieurs sens, tous issus de sa racine latine : *cultus*, action de prendre soin. Par exemple, les agriculteurs « prennent soin » de la terre et exploitent son potentiel à travers un ensemble d'opérations appelées la culture. Les croyants « prennent soin » de leurs dieux et entretiennent leur relation avec eux par le culte. Les êtres humains « prennent soin » et développent le potentiel de leur corps et de leur esprit par diverses activités regroupées sous les termes de « culture physique » et de « culture de l'esprit ».

Dans les approches multiples définissant la culture, j'aborderais celles-ci par le champ de l'**anthropologie** et du **management**. Ces approches sont pour moi les plus adaptées au thème du présent travail traitant de culture de sécurité globale par le prisme de l'Homme et l'Entreprise. Ces deux champs ont des connexions en termes de rapprochement d'éléments de définition avec des distinctions permettant une approche contradictoire différenciée. L'anthropologie s'intéresse à la culture et la vie des sociétés humaines et le management tient compte de la spécificité de l'entreprise comme société humaine.

Une approche anthropologique...

Les anthropologues ont conceptualisé, étudié et défini la culture, celle que *Le petit Robert* définit comme étant : « *L'ensemble des aspects intellectuels propres à une civilisation, une nation* » et « *L'ensemble des formes acquises de comportement* ». Certains accordent plus d'importance aux manifestations intellectuelles, d'autres aux productions matérielles.

Dans les années 1870, Edward Burnett Tylor donne une des premières définitions anthropologiques de la culture : « *Ensemble complexe qui englobe les connaissances, les croyances, les arts, la morale, les lois, les coutumes, et tout autre capacité et habitude acquise par l'Homme en tant que membre d'une société* ». Cet ensemble de *patterns* (de pensée, de comportements, de sentiments, de croyances, de modes de production et de reproduction, etc.) socialement appris et globalement partagés, à un moment donné, par un groupe de personnes formant un peuple ou une société.

Tylor est novateur en considérant la culture comme un fait universel, et se détache du sens français originel de culture comme marque de distinction, comme dans l'expression « un être cultivé ». Il innove aussi en appliquant la notion de culture à certaines populations uniquement. Enfin il insiste sur le caractère acquis de la culture, ce qui n'était pas évident dans une société très naturalisante.

De cette caractérisation anthropologique de la culture, il est important de retenir son caractère socialement appris et transmis, de même que le fait qu'elle soit commune à un

groupe de personnes partageant des origines et/ou un habitat. De plus, une culture n'est pas figée dans le temps, elle est vivante et sans cesse façonnée par ses membres. C'est pourquoi on associe une culture à une époque donnée : la culture québécoise n'est pas ce qu'elle était il y a 50 ans, non plus que la culture malienne, par exemple. Enfin, il faut souligner que les patterns ne sont pas totalement, mais plutôt globalement partagés par les individus, et ce, à différents degrés plus ou moins conscients. Cela est particulièrement marqué dans les sociétés modernes et les sociétés occidentales, où l'on observe davantage de sous-groupes et de déviants par rapport aux normes culturelles et moins d'uniformité de la culture que dans les sociétés traditionnelles^{73 74}.

Plus contemporaine, S. Sackman⁷⁵ (1991) apporte une autre approche théorique anthropologique de la culture. Selon lui, la culture se distingue en cinq catégories théoriques :

- *Evolution culturelle* : Recherche des lois des origines et de l'évolution des cultures depuis leurs formes les plus primitives à celles les plus évoluées. La culture englobe les comportements humains et les créations de l'homme. La culture se matérialise en quelque chose d'observable et est un phénomène collectif propre aux sociétés humaines.
- *Particularisme historique* : Ici l'histoire est privilégiée par rapport aux lois universelles de l'évolution culturelle. Chaque culture est spécifique et il convient de découvrir les fils conducteurs de ces spécificités. *Des cultures nombreuses et variées peuvent se développer dans toute société humaine. C'est en travaillant sur la diversité des « matériaux culturels » et sur l'histoire, que l'on trouve des fils conducteurs. Ainsi, c'est la caractéristique de déterminant des comportements qui est privilégié.*
- *Fonctionnalisme* : La culture regroupe l'ensemble des règles et besoins des individus permettant à un groupe de fonctionner comme un système et évoluer ensemble dans un système social. La culture remplit une fonction dans la société.
- *Matérialisme culturel* : Les facteurs environnementaux influencent l'origine de la culture et prennent une place importante car stimulant pour les réactions de groupe car. Le collectivisme prime sur l'individu et les comportements de groupe sont observables.

⁷³ MH. Côté, *Une approche anthropologique*. Revue A Babord N°12 de déc.2005/janv.2006 « Dossiers les non lieux de la culture ». Consulté le 14/09/2017. Disponible sur <https://www.ababord.org/Une-approche-anthropologique>

⁷⁴ WIKIPEDIA, « *Edward Burnett Tylor* », modifié le 09 septembre 2017 à 13:32. Consulté 14 septembre 2017. Disponible sur https://fr.wikipedia.org/wiki/Edward_Tylor

⁷⁵ S.A. Sackman, *Cultural knowledge in organization*. Sage, 1991.

- *Idéalisme culturel* : Connaissances, schémas mentaux et modes de pensées ce qui sont partagés avec cohérence par les membres d'un groupe. La culture intervient inconsciemment dans la manière d'agir des personnes.

Pour Sackman toutes ces théories sont reliées par un fils conducteur décliné en quatre points. Le premier est le travail mené sur les sociétés humaines à forte unicité (tribus...) dotées d'une histoire et concernés par les caractéristiques de la vie humaine (nourriture, naissance, mort, relations entre sexe, générations...). En second point, concerne les matériaux communs qui sont étudiés (rites, langages...). Le troisième point concerne la ou les caractéristiques de la société humaine et ce qui est propre au groupe. Enfin, le quatrième et dernier point, est la recherche d'explication entre les rapports de la collectivité et de l'individu.

A l'opposé, les différences entre ces cinq théories tiennent sur les relations entre la culture et l'action individuelle, relations entre la culture et son environnement et relations entre la culture et le fonctionnement des sociétés humaines.

Une approche par le management...

En 1983, l'*Administrative Science Quarterly* publiait le premier numéro spécial d'une revue de management sur la culture dont un article traitant d'une approche où l'entreprise A et EST une organisation ; la culture se distingue comme une variable et une métaphore⁷⁶.

L'organisation est caractérisée par une culture qui lui est propre. La culture est une variable du système d'entreprise comme peut l'être son système de gestion ou sa démarche commerciale. Sa fonction est de contrôler les comportements individuels, de les unifier et de les orienter vers les objectifs de l'organisation. La culture est forte lorsqu'elle oriente fortement les comportements. Considérer la culture comme une variable conduit à la faire agir dans le sens de l'entreprise. Aussi, pour le manager, la culture est-elle assez forte pour canaliser les comportements individuels ? Comment la renforcer ? Comment créer une culture permettant l'atteinte des objectifs ou la changer si celle en place ne tend pas assez vers le sens souhaité ?

L'entreprise est aussi une culture comme n'importe quelle société ; elle décrit les organisations avec les acteurs et leurs stratégies. Pour Smircich, plusieurs courants abordent la culture :

- Cognitive : Connaissances, croyances et représentations communes aux individus et qui sont partagés, aidant ceux-ci à fonctionner dans leurs systèmes.
- Symbolique : Sens donné aux faits ou événements
- Psycho dynamique : Développement d'une collectivité ayant sa propre psychologie.

⁷⁶ L. Smircich, *Concepts of Culture and Organizational Analysis*. Administrative Science Quarterly n°28, 1983.

Aussi, Frost et al.⁷⁷ considèrent qu'il y a une culture, idéale pour le management lorsque celle-ci amène flexibilité, souplesse, réactivité et vision, éléments phare pour le modèle actuel d'entreprise afin de faire face aux défis contemporains. La culture est une partie de la réalité de l'organisation à prendre en compte. Celle-ci peut être créée, changée ou renforcée et donne ainsi un levier d'action aux managers pouvant amener des « révolutions culturelles » afin de mettre en place une bonne culture, favorable au fonctionnement de l'organisation. Godelier⁷⁸ met en évidence l'impact de la culture sur le fonctionnement de l'organisation et en particulier sur sa capacité de changement. Enfin, pour Moran et Volkwein⁷⁹ et Schein, la culture résulte des interactions entre les individus de l'organisation menant à un processus social en développement. Elle englobe aussi les interactions entre l'organisation et son environnement. Ces phénomènes permettent de faire face à ses problèmes (marché, valeur ajoutée, management...) en développant des réponses adaptées. La culture est un processus d'apprentissage avec son origine et son évolution en fonction des relations à l'environnement et des interactions entre ses membres.

b. Définition du concept de culture nationale

La culture nationale est définie comme l'ensemble des éléments propres à un groupe humain spécifique, qui expliquent les façons de penser et d'agir des membres qui le constituent.

Plusieurs définitions cherchent à expliquer le concept de culture nationale et à montrer la dépendance du fonctionnement social (rôle de l'état, des institutions) envers les valeurs culturelles. Ainsi, la notion de culture est-elle perçue comme générale et partagée, c'est à dire qu'elle explique le comportement de l'ensemble du corps social. Ces valeurs peuvent être stéréotypées et mal interprétées par un autre groupe social qui ne les connaît pas. Ces images déformées sont révélatrices des barrières culturelles et des sentiments de rejet que peuvent exprimer des individus appartenant à des groupes sociaux différents. La connaissance de la culture de l'autre procure une meilleure compréhension des valeurs convergentes et divergentes qui s'établissent entre deux groupes. Connaître l'autre, c'est connaître sa culture, son identité en tant que membre d'un corps social spécifique. Vouloir imposer ses propres valeurs, c'est établir une relation de domination qui se manifeste dans à l'intérieur d'une même société. Les membres des groupes minoritaires doivent adopter ces valeurs jugées " normales ".

La culture nationale englobe l'ensemble des valeurs, des mythes, des rites et des signes partagés par la majorité du corps social.

⁷⁷ Frost et al. *Reframing corporate culture*. Sage, 1991.

⁷⁸ Godelier. E, *La Culture d'entreprise, Source de pérennité ou source d'inertie ?* Revue Française de Gestion 2009/02, n°192, pages 95-111.

⁷⁹ Moran. ET et Kwein JF, *The Cultural approach to the formation of organizational climate*. Human Relations Vol. 45, n°1, 1992, pages 19-47.

Les valeurs représentent les idées, les croyances fondamentales, la morale (le sacré, le profane) qui sont transmises d'une génération à l'autre. Les valeurs conditionnent les comportements admis, acceptés. La religion en tant que croyance, fait partie des valeurs culturelles et dans les sociétés religieuses elle devient la valeur centrale.

Les mythes sont associés à l'histoire nationale et fabriqués pour renforcer les valeurs admises.

Quant aux rites, ce sont toutes les cérémonies qui font revivre les valeurs et les mythes. Les fêtes nationales, les mariages, les funérailles sont commémorées d'une façon spécifique par les différents groupes sociaux. Le rituel de la représentation du pouvoir est un rite fondamental dans la mesure où il conditionne les rapports de force instaurés dans la société.

Les signes sont des émetteurs qui permettent à ceux qui ne font pas partie du groupe social de référence de capter certains éléments de la culture du groupe. Le langage, les symboles nationaux, la danse et la musique, les vêtements folkloriques sont des exemples de ces signes émis par un groupe spécifique.

La bonne réception du message dépend de la volonté de comprendre l'autre avant de porter un jugement de valeur.

La culture nationale n'est pas figée. Elle est évolutive. L'introduction de nouvelles valeurs, l'apparition de nouveaux mythes ou rites sont fortement marqués par l'ouverture de la société sur l'environnement.

La culture est vitale pour la survie d'un groupe qui a besoin d'être structuré, c'est à dire d'avoir des règles, des normes qui guident les actes de leurs membres et servent à résoudre les conflits internes.

Elle apparaît comme le lien social à partir duquel le groupe bâtit son identité. Le partage des tâches entre les membres du groupe, les relations de domination (de pouvoir) admises, les symboles et plus particulièrement le langage sont les traces visibles de la culture d'une société.

La culture nationale est un constituant essentiel de la culture d'entreprise⁸⁰. Gert Van Hofstede, spécialiste du management inter culturel a largement montré dans quelle mesure les cultures nationales sont une des sources de la culture d'une entreprise. Il définit en effet cinq dimensions majeures qui vont servir de critères de différenciation : La distance au pouvoir, l'évitement de l'incertitude, la masculinité/féminité,

⁸⁰ C. Durand, JF. Fili, A. Henault, *Culture d'entreprise*. Culture d'entreprise free (en ligne), 2014. Consulté le 14 septembre 2017. Disponible sur <http://culture.entreprise.free.fr/>

l'individualisme/collectivisme⁸¹. Bien que actuellement remises en question, pour Tellis et Al. les différences culturelles nationales expliqueraient plus des comportements que les cultures d'entreprises⁸². Cette notion se traduit par le succès visible dans les organisations pour le management interculturel.

Toutefois, pour Gordon⁸³, la culture nationale ne prend pas le pas sur le contexte extérieur à l'entreprise. Celui-ci insiste sur l'importance du secteur d'activité qui influence la culture d'entreprise car lui sont associées des éléments en lien avec la concurrence ou les demandes clients/consommateurs. Ainsi France, les grands secteurs de fabrication ou de distribution ont énormément codifié et normalisé les produits et/ou process managériaux de gestion de personnel, influant les comportements des entreprises.

c. Définition du concept de culture d'entreprise

La notion de « culture d'entreprise » est en France tout du moins, une idée contemporaine apparue avec l'approche de la thématique culturelle chez les sociologues des organisations.

L'origine de la formule « culture d'entreprise » remonte à 1952 et est attribuée à Jacques Elliott, fondateur du Tavistock Institute. Celui-ci la définit comme « *un mode habituel et traditionnel de penser et de réaliser les choses. Elle est partagée, de manière plus ou moins importante, par tous ces membres. Tout nouveau membre doit l'apprendre et, tout au moins partiellement, l'admettre, afin d'être accepté dans l'entreprise* ». Son idée est qu'il y a dans le fonctionnement normal des rapports de travail dans l'entreprise, une part d'habitudes plus ou moins rationnelle et consciente, dont l'origine n'est pas forcément identifiée⁸⁴.

Dans les années 50 et 60, les études américaines sur le management s'intéressent aux différences de mode de gestion RH dans différents pays. Celles-ci mettent en avant la notion de « facteur culturel » : par exemple au Japon, ces facteurs culturels, à l'origine des succès des entreprises modernes, sont basés sur les valeurs traditionnelles de solidarité, d'abnégation et de respect de la hiérarchie. De cet exemple japonais, naîtra le terme de « corporate culture » ou traduit dans le texte, de « culture d'entreprise » ou encore de « culture organisationnelle ».

⁸¹ C. Henriot, *Culture d'entreprise et motivation des salariés*. Mémoire de fin d'étude, 2007. Consulté le 14/09/2017. Disponible sur http://www.uprt.fr/mesimages/fichiers-uprt/so-social/so-management/so-henriet_c.pdf

⁸² Laurent A, *The cultural diversity of western conceptions of management*. International Studies of Management and Organization. Vol. 13, n°1-2 printemps/été 1983, p. 75-96

⁸³ Gordon, GG, Industry determinants of organizational culture. *Academy of Management Review*, 1991. Vol. 16, n°2, p. 396-415.

⁸⁴ J. Elliot, *The Changing culture of a factory*. Tavistock, 1952.

Les années 80 verront naître de cette notion et seront l'âge d'or de la culture d'entreprise⁸⁵. Un grand nombre d'expériences managériales seront conduites tel que les groupes d'expression, les cercles qualité, projets d'entreprise, histoire des entreprises... Toutefois la réduction des bénéfices des entreprises, l'instabilité des emplois, l'usure de la notion, l'usage parfois superficiel de ses usages managériaux, les surcharges de travail, la compétition inter individuelle dans les organisations remettent en question ce concept de « culture d'entreprise » même si il est bon d'être « corporate » au sein de son entreprise.

Des études telles que celle menée au début des années 1990 par John P. Kotter et James L. Heskett ont en effet démontré qu'il existe une relation de causalité entre la culture d'entreprise et ses résultats. Selon ces deux chercheurs américains de la Harvard Business School, les entreprises qui sont les plus rentables dans des environnements fortement concurrentiels, ont une culture forte. En France, des entreprises comme IBM, Valéo ou Cofely Ineo peuvent être citées en exemple. Une culture forte est facteur de compétitivité, mais pas automatiquement gage de survie. Pour cela, l'ensemble des valeurs diffusées au sein de l'entreprise doit être évolutif. Ce qui est vrai à l'échelle d'un pays l'est également à l'échelle d'une entreprise : la culture doit être ouverte pour éviter toute forme d'asphyxie⁸⁶. Denison, part d'une définition de la culture comme quelque chose de mesurable et changeable. Suite à l'analyse de 34 entreprises, il considère que la performance est issue d'une culture d'adaptabilité, d'implication et de cohérence⁸⁷.

D'autres définitions existent et varient selon les écoles de pensée et tendances mais on toutes comme dénominateur commun, que l'entreprise est une entité sociale qui est capable de générer des règles, des coutumes, des préférences, des « langages » et des croyances qui lui sont intrinsèquement spécifiques. Du moment où celles-ci sont partagées par ses dirigeants et employés, elles deviennent l'ADN et le ciment de l'organisation et de son bon fonctionnement. Les cultures d'entreprise s'expriment de façon très variées certains mettant l'accent sur les valeurs et comportements alors que d'autres seront sur les symboles, les représentations ou les compétences communes. Isabelle Francfort, Florence Osty, Renaud Sainsaulieu et Marc Uhalde⁸⁸ font la distinction entre 3 composantes :

- Les rites, symboles, codes vestimentaires et linguistiques
- La mémoire collective, résultant d'une histoire vécue ou mythique
- Les attitudes partagées

⁸⁵ T.J. Peters, R.H. Waterman, *Le Prix de l'excellence*, InterEditions, 1983 (rééd. Dunod, 1999), W.G. Ouchi, *Théorie Z*, InterEditions, 1982 (rééd. 1989)

⁸⁶ La culture d'entreprise, facteur de compétitivité ? Les Echos (en ligne), le 27 septembre 2012. Consulté le 14/09/2017. Consultable sur http://archives.lesechos.fr/archives/cercle/2012/09/27/cercle_55079.htm

⁸⁷ Denison DR. *Corporate culture and organizational effectiveness* New York. Wiley, 1990.

⁸⁸ I. Francfort, F. Osty, R. Sainsaulieu et M. Uhalde *Les mondes sociaux de l'entreprise*, Desclée de Brouwer, 1995.

D'autres auteurs insistent sur le contenu des connaissances communes sur lequel repose la culture de l'entreprise. Ainsi, tout ce qui fait partie des habitudes communes, peut être intégré à la culture de l'entreprise tout en tenant compte des influences liées à la profession, culture régional...⁸⁹ Les interprétations varient également selon les degrés d'importance accordée au « corporate ». Certains y perçoivent comme un levier d'adaptation à l'écosystème social et économique⁹⁰ alors que pour d'autres, la culture est le fondement même de l'entreprise et est son principal facteur de réussite et de performance. William G. Ouchi défend le concept d'entreprise-clan qui sert à la performance de l'entreprise et à sa cohérence organisationnelle (1980) et Gareth Morgan, souligne l'importance du symbolique et des représentations comme supports de valeurs communes⁹¹.

Qu'en est-il des différentes approches culturelles des organisations ?

La **contingence culturelle** regroupe toutes les études menées sur les contraintes culturelles externes à l'entreprise et qui influent sur la vie des organisations. Il peut s'agir de facteurs historiques, professionnels, régionaux, nationaux ou éducatifs. Une enquête menée en 1980 par Geert Hofstede dans les filiales d'une multinationale fait apparaître des mentalités différentes selon les pays dans les domaines de la prise de risque, du management, relation inter sexes, distance au pouvoir... De cette étude, naîtront les modèles dits scandinaves, américains ou encore japonais. En 1989, Philippe d'Iribarne souligne l'importance de traditions professionnelles dans les entreprises françaises, héritées de l'Ancien Régime, perpétuant une répartition des fonctions en tâches nobles et moins nobles⁹².

Marc Maurice, François Sellier et Jean-Jacques Sylvestre développent une **approche sociétale** dans laquelle les effets cumulés des structures éducatives, des pratiques syndicales, des représentants du personnel et des partis politiques influent sur les rapports au travail dans l'entreprise. Il en ressort des différences qui caractérisent des styles d'entreprises liés à la société ou « écosystème » environnant et non par une culture nationale⁹³.

La **sociologie des groupes de travail et des professions** est un autre type d'études basé sur l'histoire et la sociologie sur des groupes de métier, ou des unités de travail plus restreintes tel qu'ateliers ou bureaux. Ces travaux ont fait apparaître des cultures professionnelles

⁸⁹ N. Journet, *La culture, de l'universel au particulier*. Editions Presses Universitaires de France, 2002. Page 291.

⁹⁰ C. Handy, *L'Olympe des managers*, éditions d'Organisations, 1986. D. Graves, *Corporate Culture*, St Martin's Press, 1986.

⁹¹ G. Morgan, *Images of organization*, Beverly Hills, CA, USA, Sage, 1986.

⁹² P. d'Iribarne, *La Logique de l'honneur*, Editions du Seuil, réédition 1998.

⁹³ M. Maurice, F. Sellier et J.J. Sylvestre, *Politique d'éducation et organisation industrielle en France et en Allemagne*. Editions Puf, 1982.

spécifiques facteurs de solidarités. Nous pouvons citer Georges Ribeill sur les cheminots⁹⁴ ou Michel Liu sur des ateliers de métallurgie⁹⁵.

Des études sociologiques réalisées dans le secteur de l'industrie, ont mis en avant que la **culture ouvrière** n'est pas seulement organisée autour de la défense des intérêts des salariés mais bien aussi autour de l'**entreprise**. Maryse Tripier prend en exemple un conflit dans une PME où l'identité de l'entreprise l'a emporté sur d'autres considérations dont syndicales⁹⁶.

L'approche institutionnelle, développée par Renaud Sainsaulieu et Denis Segrestin, part de l'idée que l'entreprise est génératrice de sociabilité, d'identités et de valeurs capables d'agir sur ses membres mais aussi sur la société environnante même si la culture de l'entreprise ne se réduit pas à des symboles de fusion mais aussi à l'existence de différents niveaux d'identification tel que l'équipe, l'établissement ou la profession⁹⁷.

Dans sa webconférence pour la société Vadequa, spécialisée en audit sur la culture d'entreprise et le recrutement, Robert Marnette (consultant senior chez Management Consulting at Work) apporte une réponse contemporaine aux questions « C'est quoi une culture d'entreprise ? » et « Pourquoi avoir une culture d'entreprise ? »⁹⁸ :

*« La culture d'entreprise c'est avant tout **des valeurs que vous souhaitez partager avec vos collaborateurs**, ces valeurs servent de guide, de repère, de mécanisme pour tout un chacun. La culture d'entreprise se définit aussi comme un ensemble de critères, de rites, de mythes à travers l'espace et le temps; c'est **l'histoire de votre entreprise et c'est ce qui constitue son identité**. C'est à vous, au départ, de construire cette histoire, puis aux collaborateurs qui vous rejoindront, l'important est que tous regardent dans la même direction. La culture d'entreprise est donc constituée de plusieurs composantes :*

- **des normes:** Faire des choix (par ex: répondre en 24h),
- **des rites:** rituels autour desquels se réunissent les collaborateurs (faire un petit déjeuner une fois par mois),
- **des mythes:** histoires qui ont marqué l'entreprise (des cas difficiles, des retournements de situations, des histoires qui sont arrivées dans l'entreprise)
- **des symboles:** un logo, ce qu'il représente le lion chez Peugeot par exemple)

⁹⁴ G. Ribeill, *Les Cheminots*. La découverte, 1984.

⁹⁵ M.Liu, *Approche sociotechnique des organisations*. Editions d'Organisations, 1982.

⁹⁶ M. Tripier, Culture ouvrière et culture d'entreprise. Sociologie du travail N°3, 1986.

⁹⁷ R. Sainsaulieu, D. Segrestin, Vers une théorie sociologique de l'entreprise. Sociologie du travail N°3, 1986.

⁹⁸ R. Marnette, *Qu'est-ce qu'une culture d'entreprise ?* Neocamino (en ligne). Publié le 02/12/2013. Consultable en ligne sur <http://blog.neocamino.com/quest-ce-quune-culture-dentreprise/>. Consulté le 14/09/2017.

- ***l'histoire de l'entreprise et de ses fondateurs*** : comment elle a été fondée (Apple dans un garage, ou Facebook dans une chambre d'étudiant)

- ***le temps et l'espace*** : ce qu'elle était, ce qu'elle est aujourd'hui, ce qu'elle sera demain.

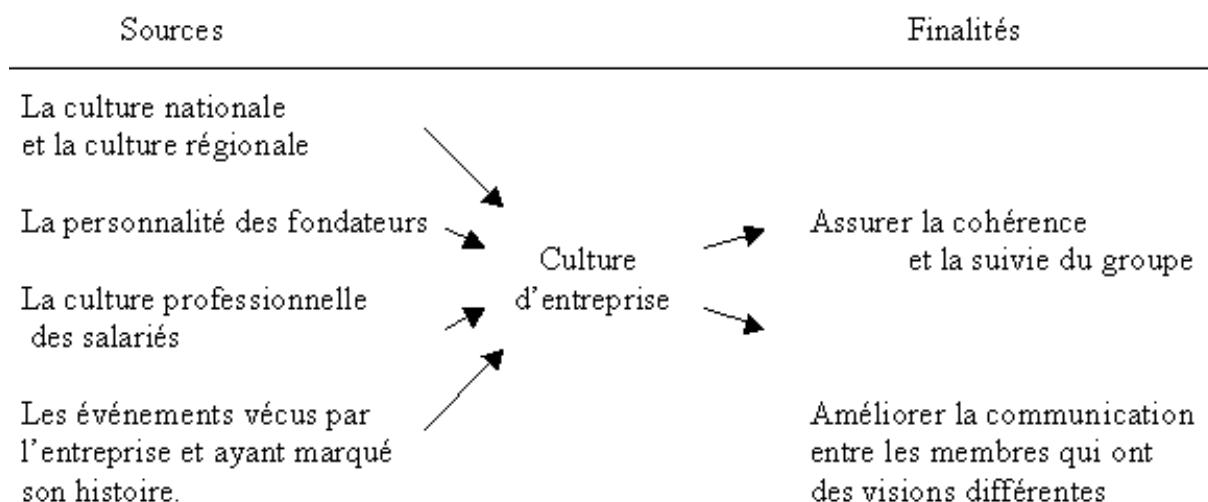
Ces différents éléments marquent la culture d'entreprise.

*La culture d'entreprise est une partie intégrante de l'entreprise, elle génère des valeurs et **fabrique des sentiments et des ressentiments**, parfois il y a une différence notable entre les valeurs annoncées et les valeurs perçues. Je m'explique; si vous voulez faire passer dans vos valeurs d'entreprise que chaque collaborateur est un membre à part entière d'une "grande famille", que vous souhaitez "partager" mais qu'en réalité les managers ne se mélangent jamais aux employés, alors la valeur de "famille" perçue sera contradictoire avec la valeur annoncée et par conséquent instaurera un mauvais climat de travail. Il n'est pas facile de faire des choix sur les valeurs que vous souhaitez partager parce qu'elles **dépendent de la perception de chacun**, mais il est important de réunir un maximum de collaborateurs autour de valeurs commune ou congruence.*

*La culture d'entreprise sera **le moteur de développement et de performances de votre entreprise**. Elle participe à l'attraction de nouveaux collaborateurs, à la motivation et à la fidélité de ceux déjà présents. On peut voir l'entreprise comme un produit à vendre, pas à des clients mais à des futurs collaborateurs, extérieurement certaines entreprises dégagent des valeurs attractives (les légendes autour des bureaux Google), plus votre entreprise sera attractive, plus vous aurez de profils à forte valeur ajoutée qui souhaiteront postuler chez vous. Elle vous sert également à motiver et fidéliser vos collaborateurs. Un salarié ressent deux types de motivations, celui lié au plaisir de travailler dans un endroit, et celui lié à la récompense et reconnaissance. **Les entreprises qui ont une forte culture d'entreprise sont six fois plus performantes** que les autres. De même elles fidélisent plus les salariés à compétences ajoutées, ce qui vous évite de recruter de nouveaux collaborateurs trop souvent. Avoir une forte culture d'entreprise est donc important, vous avez tout à y gagner; **de meilleurs profils, des salariés plus investis, une performance accrue**. N'oubliez pas que nous passons la plus grande partie de notre vie au travail, c'est donc un besoin essentiel pour chaque employé de se sentir épanoui et bien dans son travail. Des salariés plus heureux font une entreprise heureuse, mais c'est vrai dans l'autre sens aussi ».*

A ces éléments de réponse quant aux définitions de culture d'entreprise, il est bon de se questionner sur la genèse des cultures d'entreprise et comment celles-ci naissent-elles ?

Nous avons vu que la culture d'entreprise est la combinaison de différents composants culturels, chacun ayant ses propres caractéristiques. Le schéma ci-dessous présente les différentes sources contribuant à l'apparition et à l'évolution de la culture d'entreprise.



La personnalité des fondateurs de l'entreprise est un mythe majeur (mythe d'origine). Dans le groupe Apple, la vision de son fondateur Steve Jobs est toujours une référence primordiale dans la conduite du groupe ; l'innovation, le meilleur produit, la passion de la vente. Lors de la création de l'entreprise, l'entrepreneur est plus qu'un apporteur de capitaux, c'est LA personne qui prépare l'avenir de l'entreprise selon ses compétences, mais également en fonction de ses propres croyances, de sa personnalité et de sa philosophie.

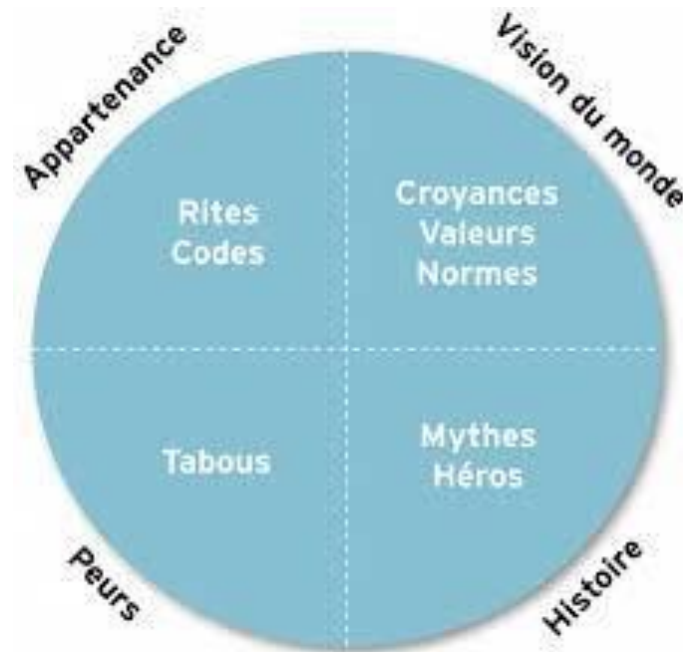
En ce qui concerne la culture professionnelle, certains travaux montrent que, dans une même entreprise, il y a des profils culturels différents. La culture professionnelle étant la culture au travail acquise dans une autre entreprise.

Les événements marquants, ce sont les mythes « héroïques », c'est à dire, les moments de gloire vécus par l'entreprise (OPA réussie, nouveaux marchés, implantation internationale, innovation sur un produit...). L'histoire unique de l'entreprise forge les mythes et les rituels qui y sont admis.

Il faut souligner qu'il arrive qu'un individu ne s'identifie pas à la culture de son entreprise. S'il a un esprit de " leadership ", il peut essayer de la faire évoluer. S'il échoue dans cette tentative, il sera marginalisé par le groupe (postes de voie de garage). Il se peut qu'un individu refusant les valeurs de l'organisation décide d'y rester exclusivement pour son épanouissement financier. Il ne sera jamais mobilisé par les discours de l'entreprise. Ce comportement ne peut être valable qu'à court terme car un rejet naturel tant personnel que du collectif fera partir ce type de profil de l'entreprise⁹⁹.

⁹⁹ C. Durand, JF. Fili, A. Henault, *Culture d'entreprise*. Culture d'entreprise free (en ligne), 2014. Consulté le 14 septembre 2017. Disponible sur <http://culture.entreprise.free.fr/>

Le schéma ci-dessous apporte une autre vision illustrant les composantes de la culture d'entreprise.



La culture d'entreprise serait un ensemble de **références** (1), **partagées** (2) dans l'organisation construites tout au long de son **histoire** (3), en réponse aux problèmes rencontrés¹⁰⁰.

- a. Permet de trouver des réactions appropriées d'action et de contrôle face à des événements. Les références incluent aussi les émotions communes face à ces situations. Ainsi, Schein opte pour une **approche anthropologique** en catégorisant celles-ci : Relation de l'organisation face à son environnement, nature de l'activité humaine, nature de la réalité et de la vérité, nature du temps, nature humaine, nature des relations humaines et degré d'homogénéité du groupe. Sackman caractérise ces références par une approche plus **managériale** : Ce qui est (buts, stratégie, structure...), comment cela marche (accomplissement du travail, relations interpersonnelles, changement...), ce qui devrait être et pourquoi cela marche ainsi.
- b. Cet aspect est le plus ancré ! Il est idéalisé car répond au manager de partager ses objectifs avec l'ensemble de l'entreprise. Il y voit la solution à tous les problèmes : motivations, revendications, ajustements quotidiens au groupe. Il convient toutefois de tenir compte des sous cultures dans les entreprises : professions, formations des collaborateurs, d'établissements... Toutefois, la culture d'entreprise met en évidence les références opérant au niveau global de l'entreprise.

¹⁰⁰ Thevenet, M. *Culture d'entreprise : une définition*. CAIRN.INFO, 14/09/2017 p.32-54.

- c. La culture se construit selon un processus d'apprentissage et est issu d'un système apprenant. Chaque entreprise est confrontée à des problèmes spécifiques au monde de l'entreprise tel que défini par Lawrence et Lorsch.

L'entreprise est soumise à des situations pour lesquelles elle doit trouver des solutions. Les modes de réponse appropriés génèrent des schémas de références.

Pour conclure sur le concept de culture d'entreprise, des exemples et des avis de professionnels illustrent concrètement par une vision terrain ce qui a pu être développé.

Le premier exemple est le cas de la société Marquet qui fabrique et commercialise des pantoufles. Les dirigeants ont voulu imposer un management à flux tendu. Le climat social à l'intérieur de l'entreprise s'est vite détérioré même si les salariés ont reconnu les avantages de ce mode de fonctionnement, mais ils n'ont pas accepté qu'on leur impose le progrès d'une façon autoritaire à la « japonaise ».

Dans un autre contexte, pour Jean-Marie Albertini, lors d'une OPA (Offre Publique d'Achat) qui amène à une fusion des structures, les dirigeants ont tendance à minimiser le choc des cultures. Selon lui, toute démarche d'acquisition ou fusion/acquisition d'une entreprise doit prévoir un audit financier mais aussi social.

De la même façon quand une société change subitement et radicalement de culture d'entreprise, l'impact sur les individus du groupe n'est pas négligeable. La Poste en est un excellent exemple ; ses agents très ancrés dans une culture de service public ont dû s'adapter un management de logique de rationalité et de rentabilité. Le choc des cultures sur les salariés a été sous-estimé avec toutes les conséquences dramatiques qui en ont résulté dont l'impact néfaste au bon fonctionnement de l'entreprise.

Il est difficile de dire si la culture d'entreprise est une bonne ou une mauvaise chose. Elle peut à la fois favoriser ou détériorer le climat social selon son utilisation. La culture peut en effet être bénéfique à la mobilisation des salariés, à leur efficacité et être source de performance, mais une culture trop forte et figée peut devenir une contrainte importante rendant difficile le management.

Dans l'environnement économique actuel où la mondialisation est globale, où les fusions et les rachats de grands groupes et PME sont légions, la culture d'entreprise sera un enjeu stratégique pour les entreprises devant subir ces restructurations devenues aujourd'hui inévitables.

d. Définition de la culture de sécurité d'entreprise

La prise de risques pour faire évoluer, progresser, développer les activités industrielles, de travaux publics, agricoles, de services et commerciales est la logique qui fait naître la notion de « risques acceptables ». Si celle-ci a permis de faire progresser et favoriser l'innovation dans ces domaines, l'objectif est d'éviter malgré tout, les accidents et dommages. « Le prix à payer », chère à la révolution industrielle où le « sacrifice » semblait nécessaire pour faire avancer le progrès¹⁰¹. Même si les évolutions des mentalités autour des questions de sécurité ont conduit à des améliorations sans commune mesure, la notion de « sacrifice » reste toutefois d'actualité, toute proportion gardée ; elle se perçoit notamment dans les termes employés tels que « risque acceptable » ou encore « le risque zéro n'existe pas » bien que ceux-ci se doivent d'être maîtrisés par les organisations. Ces éléments sont d'ailleurs un des fondements de la réglementation en matière de prévention des risques¹⁰². Le principe de responsabilité concerne en premier le chef d'entreprise, tenu à une obligation de sécurité de moyens et de résultat. Toutefois, les salariés sont tenus eux aussi, de « prendre soin de sa sécurité et de sa santé ainsi que de celles des autres personnes concernées du fait de ses actes ou de ses omissions de travail », ce qui a amené le slogan « la sécurité est l'affaire de tous ». Enfin, autre principe « managérial », celui où la maîtrise des risques doit intervenir le plus en amont possible et où aucune priorité ne peut s'exercer au détriment de la sécurité ». Comme nous avons pu le voir avec certaines problématiques de sécurité globales des entreprises, les moyens pour se prémunir de celles-ci sont légions. Toutefois et fort des constats sus cités, qu'elle marge d'insécurité tolérable acceptons nous dans les organisations, ne serait ce que pour des raisons économiques avec le coût qu'imposerait le « risque zéro ». La maîtrise des risques que l'on peut traduire par « le maintien des risques à l'intérieur de limites considérées comme acceptables »¹⁰³ est devenue une exigence sociétale forte. A titre d'exemple parlant, les autorités avioniques de certification, placent le niveau acceptable de crash d'un avion à une probabilité inférieure à 10^{-9} par heure de vol. En combinant le nombre au nombre d'heures de vol du trafic aérien et au nombre de passagers transportés dans chacun de ces vols, nous pouvons déduire le nombre maximal probable de personnes tuées que nous acceptons dans le trafic aérien. Aussi, nous pouvons l'admettre « tout n'est pas sous contrôle » même si les entreprises veulent tendre vers le « zéro accident ». Dans le même esprit et au-delà de contraintes réglementaires citées plus haut, le développement de la responsabilité sociale des entreprises a favorisé « l'intégration volontaire par les entreprises de préoccupations sociales et environnementales à leurs activités commerciales et leurs relations avec les parties prenantes »¹⁰⁴. Malgré les efforts pour prévenir l'occurrence de dommage (humains,

¹⁰¹ FRESSOZ JB, *L'apocalypse joyeuse : Une histoire du risque technologique*. Seuil, 2012

¹⁰² Principe de **responsabilité**, directive 89/391/CEE du 12/06/1989, articles L.230-3 et L. 263 du Code du travail, arrêté de la Cour de cassation du 28/02/2002 et principe de **prévention**, article L. 230-2 du Code du travail.

¹⁰³ Leroy et Signoret, 1992, p.109

¹⁰⁴ Commission des Communautés Européennes, *Promouvoir un cadre européen pour la responsabilité sociale des entreprises*. Livre Vert, 18/07/2001, p. 7.

matériels, systèmes, organisations...) tel que processus de management des risques, formations, EPI... les accidents surviennent de nos *capacités humaines perfectibles et intrinsèquement limitées à maîtriser les risques*. Ainsi, ce sont nos capacités à éviter les dommages qu'il faudrait pouvoir faire évoluer et évaluer afin de les améliorer¹⁰⁵. Cette démarche, ne s'inscrit elle pas dans la culture de sécurité des entreprises ?

Suite à la catastrophe de Tchernobyl en 1986 et à l'occasion de son 30^{ème} anniversaire, l'Agence Internationale de l'Energie Atomique (AIEA) définit la notion de culture de sécurité par « *l'ensemble des caractéristiques et des attitudes qui, dans les organismes et chez les individus, font que les questions relatives à la sécurité bénéficient, en priorité, de l'attention qu'elles méritent en raison de leur importance* » (INSAG, 1991). Cette notion de culture de sécurité, connaît une forte hausse d'utilisation et d'intérêt que ce soit sur un plan managérial ou scientifique. Au niveau **management**, en 2002, l'Institut pour une culture de sécurité industrielle est créé à Toulouse avec pour fonction de « *favoriser le développement de la culture de sécurité à travers des rencontres et des échanges entre l'ensemble des partenaires* »¹⁰⁶. Cette notion de culture de sécurité est reprise de la notion de culture d'entreprise, apparu dans le management occidental dans les années 80 et **consiste à agir sur la culture pour influencer sur la sécurité** (Guldenmund, 2000, Gauthey et Gibeault, 2005). Pour Chevreau (2006a) la culture de sécurité est un projet stratégique qui englobe les différents principes managériaux et techniques :



Figure 1 La culture de sécurité comme stratégie de maîtrise des risques

¹⁰⁵ MOTET Gilles, *Risque acceptable : un permis de tuer ?* Tribunes de la sécurité industrielle, 2013, n°2, p.2

¹⁰⁶ www.icsi-eu.org

Renforcer la culture de sécurité (responsabilité, prévention, analyse et acceptation des risques, défense et sûreté, résilience) revient à rendre cohérents les discours et les pratiques de la maîtrise des risques. Pour cela, la formation des managers doit changer les discours sur la culture de sécurité et ne plus présenter celle-ci comme un outil mais comme une manière de concevoir les problèmes de maîtrise des risques et de les aider à mieux comprendre sur quoi repose cette maîtrise et ce, par une approche pratique pour qu'elle puisse devenir opérationnelle¹⁰⁷. Ainsi par exemple, l'APAVE propose aux entreprises d'améliorer leur performance globale en travaillant sur la culture et les comportements sécurité. Celle-ci part du principe que les entreprises ont mis en place des actions (techniques, organisationnelles et humaines) pour répondre aux obligations de sécurité. Toutefois, bien que l'accidentologie ait baissé grâce à ces actions, les organisations peuvent constater une stagnation ou remonté (taux de fréquence, taux de gravité) des résultats, un manque d'implication des managers et/ou une analyse des origines des accidents dues à des problèmes comportementaux. Ainsi l'organisme de formation propose d'accompagner les entreprises à identifier et mettre en œuvre des solutions dans les domaines des comportements sécurité, des facteurs humains et organisationnels et de... la culture de sécurité. L'APAVE reprend comme définition de la culture de sécurité comme « *l'ensemble des valeurs et des pratiques intégrées par les personnels (management compris) pour maîtriser les risques de leurs activités. La culture sécurité est toujours dépendante de la culture d'entreprise et représente l'excellence de la sécurité mais est rarement au niveau souhaité* »¹⁰⁸. **Cette approche idéaliste est intéressante mais ne traite que de la spécificité de la Santé Sécurité au Travail et pourrait facilement être étendue, de par sa philosophie, à la sécurité globale des organisations (Cybersécurité, intelligence économique, sûreté/malveillance...).**

Alors comment les organisations pourraient-elles améliorer leur culture de sécurité ? Le principe voudrait, comme pour une étude marché ou d'opportunité, de benchmarker les bonnes pratiques mises en place, ainsi que les leviers et outils utilisés par les entreprises faisant référence en terme de sécurité (cyber, santé sécurité, intelligence économique, malveillance...) et de les transposer à son entreprise. Toutefois, des paramètres cruciaux déterminent ce qui réalisable ou non, dont le secteur d'activité, l'implantation géographique, l'histoire de l'entreprise, le contexte socio-économique... L'ambition de l'organisation doit être en cohésion avec les éléments sus cités ainsi que les moyens et ressources pouvant être engagés. De plus l'évolution de la culture de sécurité adaptée à son écosystème, devra contribuer positivement à l'activité de la structure :

- Questionner l'apport de la sécurité à sa santé économique
- Choisir des axes d'investissement flexibles, adaptés à l'évolution possible de l'activité
- Concevoir des options de repli lorsque l'activité diminue

¹⁰⁷ Chevreau F.R et Wybo J.L, *Approche pratique de la culture de sécurité*. CAIRN.INFO 171-189 (En ligne)

¹⁰⁸ APAVE, Culture et Comportements Sécurité. www.apave.com

Ainsi, la culture de sécurité n'a de sens que si elle contribue directement à la santé économique de l'entreprise par la réduction de jours de productions perdus par des d'arrêts de travail ou des pertes de données essentielles suite à un piratage informatique par exemples. A contrario, la visibilité des échecs de sécurité peut rapidement affecter le bon fonctionnement de l'entreprise mais aussi son économie ; baisse de sa notoriété, mise à mal de son image, couts directs et indirects des « accidents »... voir de se branche d'activité (filière de la viande par exemple avec les scandales sanitaires). Les organisations devront pour définir leurs ambitions de culture de sécurité adaptée à leur contexte :

- Définir des engagements de sécurité aux standards des meilleurs secteurs
- Définir des plans d'investissements de sécurité à long terme
- Défendre une stratégie qui protège la sécurité des effets directs des fluctuations d'activité ou des pressions de la production

Il convient aux entreprises de s'engager sur un niveau de culture de sécurité adapté à son contexte sans forcément réaliser un copier/coller de bonnes pratiques au risque de mettre son activité en péril. Des ambitions de culture de sécurité trop précoces, trop élevées ou au contraire trop basses peuvent être délétères¹⁰⁹.

Aussi même si la sécurité est l'affaire de tous, elle se veut « professionnelle » et les acteurs se doivent de se former ! La sécurité apparait comme liée aux compétences et savoir-faire que les acteurs acquièrent à travers les métiers et/ou les fonctions pour lesquelles ils ont été initialement formés mais aussi des une résultante d'actions, de formations spécifiques, distinctes des formations initiales. Elle fait partie du bloc de compétences des acteurs intervenants, quel que soit son niveau dans l'organigramme. La sécurité repose aussi sur des actions spécifiques telles que les journées sécurités ou la minute sécurité. Ces actions visent à ce que les questions de sécurité soit « l'affaire de tous les jours ». Une autre approche managériale considère au contraire que la sécurité relève de l'exceptionnel et quelle ne peut être acquise que volontairement et de façon répété, en dehors « du cours des choses » de façon à maintenir une attention particulière à ce sujet. Ici, la routine des pratiques et processus est perçue comme un danger. La première approche apparait comme la plus en phase avec la réalité des faits au sein des entreprises La seconde quant à elle, est plus en adéquation avec le sens commun et la façon dont sont envisagées des actions de sécurité au sein des entreprises. Très contrastées ces approches conduisent à s'interroger sur le fondement réel de la sécurité : des pratiques ? Des processus inscrits dans la routine ? Des actions de communication sous forme d'injonctions ? Des formations ? Des certifications ? Tout cela visant à provoquer une vigilance particulière et introduire ou entretenir une culture de sécurité partagée ? Dans tous les cas, les entreprises doivent donner la preuve qu'elles font de la sécurité une priorité absolue et les actions menées doivent satisfaire aux

¹⁰⁹ TAZI, Dounia, *Avoir des ambitions de culture de sécurité cohérentes avec le contexte de son activité*. Conviction n°18, février 2016.

exigences internes et externes. Cependant, le paradoxe est que les actions de fonds sont les moins visibles (plus près des pratiques et processus tenant compte des aspects multi factoriels) alors que les actions de forme sont les plus exposées car en lien avec le discours public (respect des valeurs, sens des responsabilités, éthique, formalisation...) et utiles pour la communication de l'entreprise. De là né la difficulté pour les DRH et responsables formation, de définir la politique formation sécurité, l'offre étant grandement axée sur ce qui est attendu des entreprises de « l'extérieur » en matière de sécurité. Les formations spécifiques en matière de sécurité se trouvent de diverses façons en porte-à-faux :

- Professionnalisation de la sécurité et des métiers de la sécurité contribuant à masquer la mise en œuvre d'une sécurité ordinaire avec des formations trop théoriques ne préparant pas suffisamment les salariés aux situations diverses susceptibles d'être rencontrées en réalité au sein de leurs organisations et ainsi de ne pas acquérir de connaissances suffisantes pour y développer une culture d'activité permanente
- Des actions de formations qui abordent la sécurité sous l'angle de l'exception comme si peu concevables hors d'actions spécifiques réservées « aux spécialistes » et déconnectées du « cours des choses »
- Des actions de formations servant à donner la preuve que l'entreprise est dans une démarche volontaire de priorisation de la sécurité, dans un objectif moins basé sur l'efficacité et pertinence de celles-ci que par l'affichage et justification des efforts réalisés

Partant de tous ces constats, il est nécessaire d'effectuer un retour au réel en rapprochant les formations à la sécurité et la sécurité telle que réellement mise en œuvre au sein des entreprises. Il est important de favoriser les échanges (débat, RETEX, analyse) entre professionnels sur les situations rencontrées. Il convient aussi d'avoir une approche pragmatique, en phase avec notre monde de communication, sur le fait que les formations doivent participer à la justification des actions menées par les entreprises en matière de sécurité. Il est ainsi possible de concilier ces deux approches pour l'amélioration de la sécurité¹¹⁰.

Mais les actions de formation ne sont qu'une composante de l'évolution de la culture de sécurité et celle-ci passe par l'implication de tous et se construit par les relations sociales entre les acteurs de l'entreprise. Une bonne dynamique de ces relations permet aux « façons de penser et d'agir » de devenir collectives et donc partagées et acceptées par le plus grand nombre, du management aux employés ou ouvriers. Pour réussir cette évolution et ou acculturation de la sécurité l'implication de la direction est indispensable ; elle doit impulser la dynamique, la rendre visible, la faire vivre par son leadership et par des pratiques participatives. Enfin, la direction doit fixer le cap sur l'attendu et/ou sa vision de la culture de

¹¹⁰ GILBERT, Claude, *La sécurité : une affaire de professionnels ?* Tribunes de la sécurité industrielle, 2015, n°6

sécurité à atteindre. Ce projet d'entreprise nécessite également la participation active de toutes les forces humaines de l'organisation qui doivent se l'approprier et le porter. Il n'est possible d'imaginer une gestion unique de la part du dirigeant ou du département HSE ou DSI pour les questions cyber par exemple. Trois bénéfices en sont tirés par l'entreprise par l'engagement des acteurs de terrain¹¹¹ & ¹¹² :

Phase de justification	Phase de construction	Phase de déploiement
Donner la parole, écouter les préoccupations sur les changements possibles du travail des acteurs.	Booster les engagements	Les salariés sont des acteurs et non des destinataires simples
Gestion des mécanismes psychologiques générateurs de résistances individuelles ou collectives	Appropriation de l'attendu	Suppression de la notion de « subir »

Cependant, cette implication a besoin d'être organisée et animée et peut se concrétiser par des consultations d'opinion, la co-construction du plan d'action, voire à la délégation d'actions ou de responsabilité. Ces pratiques s'inspirent du style de leadership directif-participatif, amenant aussi un accompagnement et gestion de l'encadrement car celles-ci s'apprennent et ne se décrètent pas¹¹³. Le regard du syndicaliste Jean-Paul CRESSY, délégué fédéral de la FCE-CFDT est tout à propos quant au dialogue social et intègre la place des organisations syndicales : « Déployer réellement dans l'entreprise la culture de sécurité ne se décrète pas et ne sera pas non plus l'effet d'une génération spontanée (...). Dans cette démarche, le dialogue social sera essentiel et les organisations syndicales ont toute leur place. Pour être efficace aujourd'hui, le dialogue social doit s'appuyer sur trois piliers : la direction, les salariés et les organisations syndicales. Force est de constater aujourd'hui que la culture de sécurité est à la mode dans les orientations mais que les recettes de mise en œuvre restent imparfaites. Pour atteindre cet objectif, il faut accepter un profond changement de la gouvernance. Il faut oser associer les représentants du personnel dans un comité de pilotage. Une fois lancée, la démarche ne peut s'arrêter et doit être marquée par des évolutions visibles »¹¹⁴. Ce mode de management favorise les initiatives des salariés et renforcent la sécurité. Elles doivent être traitées comme des compléments au prescrit et non comme des écarts.

¹¹¹ DANIELLOU F, SIMARD M, BOISSIERES L, *Les facteurs humains et organisationnels de la sécurité industrielle : un état de l'art*. Les cahiers de la sécurité Industrielle, Février 2010.

¹¹² BAREIL C, *Modèle diagnostique des phases de préoccupations : une approche utile dans la gestion des changements*. 1999, Ecole des Hautes Etudes Commerciales.

¹¹³ BRUNEL, C, *Promouvoir les comportements proactifs en sécurité est incontournable pour développer la culture de sécurité*. Nos Convictions, 2014, ICSI, Toulouse.

¹¹⁴ CRESSY Jean-Paul, *Dialogue social : Incontournable pour la culture de sécurité*. Tribunes de la sécurité industrielle, 2016, n°6.

Aussi, deux grands types d'initiatives peuvent être décrits :

Initiatives co-régulées	Initiatives auto-régulées
Définies par l'organisation et les conditions dans lesquelles elles peuvent et doivent être déclenchées sont connues	Comportements de sécurité qui reposent sur le professionnalisme et qui ne sont pas forcément connues ou encadrées.
<p>Initiatives auto-régulées :</p> <ul style="list-style-type: none"> - Adaptent les opérations aux conditions en cours - Comblent une absence de procédure - Augmentent le niveau de sécurité d'une procédure existante - Compensent les effets non prévus d'une procédure 	

Les initiatives bénéfiques la plupart du temps à la sécurité se traduisent par des actions de bon sens réalisées par des personnes ayant une bonne maîtrise de leurs métiers. Toutefois, celles-ci doivent rester sûres mais ne se décrètent pas comme fiable, il convient au management d'anticiper les erreurs possibles et leurs causes. Des leviers peuvent être actionnés :

- Assurer un haut niveau de compréhension de l'activité pour anticiper les conséquences de ses propres actions ou celle des collègues,
- Maintenir des conditions de travail saines
- Demander l'avis des pairs, adopter une attitude interrogative et cultiver le doute

Ainsi le management doit définir un cadre d'engagement des initiatives, positiver le rôle des équipes dans la sécurité globale, mettre celles-ci en avant et considérer les initiatives malheureuses comme un épiphénomène. Sans des dénier, les conditions dans lesquelles les choses se sont passée doivent être analysées et nourrir le RETEX. Enfin, celles-ci ne doivent pas engendrer le bannissement de toutes futures initiatives¹¹⁵.

Dans le domaine des **sciences**, la base bibliographique Business Source Elite référence près de cent trente articles touchant la notion de culture de sécurité, tout domaine d'activité confondue, de 2000 à 2006. Les travaux des anthropologues, transposés au management donne une lecture de la notion de culture de sécurité s'intéressant aux normes ou aux symboles partagés par l'entreprise, supposés liés à la sécurité puis à la définition de bonnes pratiques, permettant ainsi d'agir sur ces éléments culturels pour développer une « bonne culture de sécurité » (Godelier, 2006). Cette notion de culture implique un socle de savoirs et de valeurs partagés par les individus d'un groupe. Ces éléments diffusent dans le groupe à travers l'expérience vécue des individus les uns avec les autres et leur permet souvent de construire une vision commune des situations qu'ils rencontrent : « développer cette connaissance, la partager entre les intervenants et valoriser ceux qui la possèdent, sont (...)

¹¹⁵ BESNARD Denis, *Les opérateurs qui prennent des initiatives renforcent la sécurité*. Conviction n°21, mai 2016.

des moyens efficaces pour augmenter la résilience des organisations aux situations de danger » (Wybo, 2004, p. 29). Le partage d'éléments culturels implique une certaine normalisation des pratiques quotidiennes des personnes : « *A un modèle correspond une conduite où tous les individus conforment en général cette conduite à leur modèle* » (Vinsonneau, 2003, p. 60). Les retours d'expériences¹¹⁶ permettent le partage de connaissances issues de situations vécues par les organisations dans lesquelles de bonnes pratiques ont pu être identifiées et les failles corrigées par le collectif de la structure. Ces éléments s'inscrivent ainsi dans la mémoire institutionnelle de l'entreprise et viennent nourrir la culture de sécurité de celle-ci.

Mais à ces cultures de sécurité d'entreprise quelle place pour l'influence locale ? Dounia Tazi, spécialiste dans la prise en compte des facteurs humains et organisationnels dans la culture de sécurité, relate la phrase récurrente lors d'intervention auprès de grands groupes industriels ou de PME sous-traitantes, « Oh mais ici c'est spécial, vous ne pouvez pas comparer ou obtenir les mêmes pratiques qu'ailleurs, c'est notre culture ». Cette notion d'ailleurs peut s'appliquer à un département, une région, une grande zone géographique (exemple le sud et le nord de la France) ou encore à un autre pays voire continent...¹¹⁷ De 2008 à 2013, l'Institut pour une Culture de Sécurité Industrielle (ICSI) a mené une étude où trois facteurs d'influence des perceptions de croyances et pratiques de sécurité ont été testés¹¹⁸ : le secteur d'activité, la zone géographique, le niveau hiérarchiques des répondants. Les résultats ont montré que le facteur qui influence le plus les perceptions de culture de sécurité est le secteur d'activité, bien devant la zone géographique (3^{ème} position) et le niveau hiérarchique (2^{ème} position). Ainsi, la culture locale n'a que peu d'influence et c'est bien le secteur d'activité qui prime en terme de perception et de pratiques de culture de sécurité. Toutefois, les organisations ne doivent pas négliger le facteur local pour mieux comprendre les perceptions et pratiques des acteurs.

¹¹⁶ Vérot, 1998 : « *Démarche organisée et systématique pour analyser les anomalies, les incidents, les accidents, rechercher les causes et les enchainements, en tirer les divers enseignements et définir les mesures de correction et d'amélioration, assurer l'information pertinentes aux parties intéressées* ».

¹¹⁷ TAZI Dounia, *La culture locale n'est pas le facteur d'influence majeur de la culture de sécurité*. Conviction n°10, Avril 2015.

¹¹⁸ Besnard, D et al, *A worldwide meta-analysis of 21 safety culture surveys in oil, gas transport facilities & storage and services compagnies*. APS conference Singapour, 2013. Enquête ICSI menée auprès de 21 structures de 4 continents, dans les secteurs d'activité du pétrole, services, transports et stockage de gaz). Cette enquête a traité plus de 21 000 réponses.

Pour Camille Brunel¹¹⁹, c'est la perception des conséquences de nos actions qui influence nos comportements de sécurité. Le modèle ABC explique les comportements humains selon deux déterminants que sont les antécédents et les conséquences :

A	Antécédents (A ctivators)	Ce qui précède et déclenche le comportement
B	Comportement (B ehaviour)	Un acte qui peut être observé
C	Conséquences (C onséquences)	Le résultat de l'acte

Les individus se comportent en fonction des conséquences perçues de leurs comportements. Ils agissent après une analyse, très rapide et inconsciente, des conséquences de leurs actions. Les conséquences perçues pourront être positives (qualité du résultat, atteinte rapide d'objectif...) ou négatives (fatigue, baisse de la vigilance, erreur...). Les comportements que nous recherchons le plus sont ceux pour lesquels nous percevons des conséquences immédiates, certaines et positives et non pas un risque de blessure, de sanction, de défaillance... dont les conséquences sont perçues comme ultérieures, incertaines et négatives. Les individus agissent donc pour gagner en temps, en confort ou en satisfaction.

I	Immédiates	U	Ultérieures
C	Certaines	In	Incertaines
+	Positives	-	Négatives
IC+		UIn-	

Nous agissons à l'encontre de la prévention parce que les conséquences perçues comme le plus bénéfiques et plus probables ne sont pas toujours celles issues de comportements surs. Ainsi ? Si une organisation n'agit pas sur la perception des conséquences, la sécurité est toujours perdante. Valoriser les comportements de sécurité transforme les conséquences perçues comme immédiate et positive. Une autre approche développée par Denis BESNARD¹²⁰ considère que les Hommes ont une vision très partielle de la réalité et sont limités par ce que leurs sens, connaissances et expérience permettent d'en saisir la substance. La prise de risque obéit plus à la perception de leur exposition par les individus ou les groupes d'individus que par une analyse logique. Les individus agissent spontanément en accord avec leurs perceptions et leur demander d'avoir des comportements qui s'accordent avec ces perceptions est un levier de réussite. A contrario, leur demander d'opter pour des comportements allant à l'inverse de leurs perceptions impose de lever les résistances induites.

¹¹⁹ Brunel Camille, La perception des conséquences de nos actions influence nos comportements de sécurité. Conviction n°17, janvier 2016.

¹²⁰ BESNARD Denis, *Les individus agissent, adhèrent et résistent en accord avec leurs perceptions*. Conviction n°5, octobre 2014.

Chaque programme d'organisation visant à faire évoluer la culture de sécurité, provoque adhésion et résistance. Cela implique de :

- Reconnaître le poids qu'ont les perceptions sur la décision des individus et des groupes
- Evaluer le degré de convergence et de divergences des perceptions d'un groupe sur les sujets qui influent sur la culture de sécurité
- Anticiper l'effet des perceptions des groupes sur l'adhésion ou la résistance au programme d'évolution de la culture de sécurité

Pour le chef d'entreprise Philippe Balzer, les bonnes pratiques au travail doivent trouver une suite logique dans la vie privée. Il reprend que, « *c'est le signe que la culture de sécurité est enfin dans la tête de tous* ». Ainsi chaque salarié a une valeur intrinsèque de sécurité. Leurs croyances et valeurs les amènent ainsi naturellement vers les comportements adéquats et idéals : prudence, vigilance, respect des règles... Aussi, si je suis prudent dans ma vie privée, je le suis dans ma vie professionnelle. Toutefois, l'exposition au danger dans le cadre d'une activité de loisir (chasse, escalade, plongée, sports motorisés, jeu en ligne...) ou de la vie courante (réseaux sociaux, cuisine, repassage...) est choisie mais imposé par l'entreprise de par la nature de son activité (environnement avec produits chimiques, radioactifs, inflammables, voyages d'affaires, implantation géographique...). Ce que les règles de l'entreprise (consignes sécurité, règlement intérieur, réglementation...) impose, la gestion de sa vie privée en « bon père de famille » impose implicitement une culture de sécurité.

Croyances et valeurs	+	Situation	=	Comportement
« ce que je pense »		« ce que je vis, ce qui m'est demandé »		« ce que je fais »

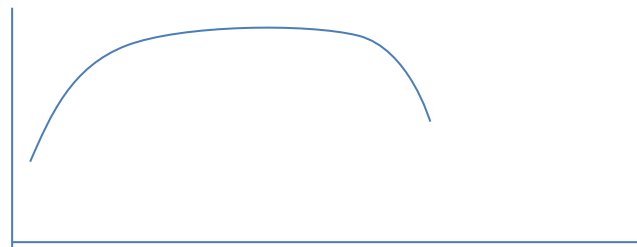
« Les accidents n'arrivent pas toujours aux personnes les moins expérimentées » titre le sociologue et ergonome Jesus Villena-Lopez¹²¹. Dans l'imaginaire populaire, il est courant d'entendre que « *ceux qui sont le moins expérimentés sont ceux qui souffrent le plus d'accidents* ». Ors cette affirmation n'est qu'une croyance ou expression idéologique. Des études en anthropologie et sociologie expliquent que dans une entreprise des croyances s'expriment en tant qu'idéologies défensives face aux risques. Les salariés débutant, en cours d'acquisition de compétences propres à leur métier, ont des « accidents » (à prendre au sens large dans le concept de sécurité globale : accident du travail, ouverture d'un mail avec malware, victime d'ingénierie sociale ou d'agression par exemples). Toutefois des collègues expérimentés peuvent eux aussi subir ces « accidents » ; nous retrouvons dans chaque grande catastrophe des opérateurs très expérimentés ! Pour le modèle psychologique « SRK » (skills, rules, knowledge)¹²², L'expérience construit peu à peu des

¹²¹ VILLENA-LOPEZ Jesús, *Les accidents n'arrivent pas toujours aux personnes les moins expérimentées*. Conviction n°8, février 2015.

¹²² RASMUSSEN Jens. *Skills rules and knowledge ; signals, signs and symbols, and distinctions in human performance models*. 1983, IFSE Transactions on Systems. Man and Cybernetics, MC-13, 257-266.

associations directes entre problèmes et solutions qui aident à la réalisation efficace des tâches. Les experts, atouts de production et de qualité, connaissent la réponse à un grand nombre de situations à problème. Ils ont pour eux la conviction de la maîtrise du volet technique de leurs tâches et la maîtrise des risques associés. Toutefois, ces experts ne sont pas infailibles et peuvent être aussi victime d'accident ou source d'accident à cause de leur excès d'expérience (Par exemple en déclenchant automatiquement une solution à un problème qu'ils pensent à tort avoir reconnu) ou même de leurs comportements non sûrs¹²³. Pour les collaborateurs moins expérimentés, les erreurs et accidents proviennent de connaissances incomplètes ou erronées. La théorie de la gestion des risques de René Amalberti¹²⁴, renforce le fait que le manque de connaissance peut mener à l'accident et l'excès de connaissance peut dériver vers une normalisation de la déviance, dépasser les limites du système et avoir pour conséquence un accident.

Niveau de sécurité



Expérience & Connaissances

L'histoire de l'industrialisation, montre que la seule protection des ouvriers était leur propre professionnalisme et expérience même si avec l'avènement des systèmes de management de la sécurité cette croyance de « culture de métier » comme la nomme l'ICSI, reste présente dans la culture des organisations¹²⁵.

Que pouvons-nous retenir de ce qu'est la culture de sécurité ; celle-ci est un ensemble de manière de faire et de manières de penser largement partagées par les acteurs d'une organisation à propos de la maîtrise des risques les plus importants liés à ses activités.

Les comportements en matière de sécurité ne peuvent changer de façon pérenne sans une évolution du regard et surtout une **compréhension**, portés par tous les protagonistes de l'entreprise sur la sécurité et son importance. De la même façon, il n'est possible de faire évoluer les mentalités sans signes forts et concrets donnés par le management et en premier lieu, la Direction.

La culture de sécurité se construit par les **interactions** entre les acteurs d'une organisation qui s'adapte à la fois à son écosystème et l'intégration de ses membres. Elle est le reflet de

¹²³ BESNARD Denis, *Les personnes les plus expérimentées peuvent être trop sûres d'elles*. Conviction n°12, juin 2015.

¹²⁴ AMALBERT René, *Piloter la sécurité : théories et pratiques sur les compromis et les arbitrages nécessaires*. Springer, 2012, Paris.

¹²⁵ SIMARD Marcel, *Culture et gestion de la sécurité*. Encyclopédie de la santé et sécurité au travail, OIT Ginebra, 1989.

l'importance donnée par l'organisation à la sécurité, en l'intégrant dans toutes les décisions, tous les services, tous les métiers et tous les niveaux hiérarchiques. Les entreprises doivent axer leurs efforts de sécurité sur une maîtrise des risques les plus graves de leurs activités, menaçant directement la survie de l'organisation. Cette approche consensuelle permet de mobiliser les acteurs dans une dynamique ayant un effet direct sur les risques les moins graves.

Cette conscience **partagée** sur les risques majeurs, constitue le socle de la culture de sécurité de l'entreprise. Ces risques, propres aux activités, sites, métiers, se doivent d'être connus par tous au sein des entreprises. Pour agir sur les performances de sécurité de l'entreprise, des actions cohérentes intégrant les dimensions techniques, managériales, humaines et organisationnelles se doivent d'être mises en place.

Une approche de culture de sécurité ne peut se concevoir sans actions suffisantes sur ces **trois piliers**, avec une insistance particulière sur les facteurs humains et organisationnels.

Pour les entreprises ayant les pratiques les plus avancées en termes de sécurité l'enjeu est d'évoluer vers une culture intégrée de la sécurité. Chacun doit se sentir responsable de la sécurité de son organisation de par son activité et des interactions avec tous les acteurs concernés. Cette démarche favorise une forte **implication** de la ligne managériale et des opérateurs. Chaque structure se doit de faire des choix stratégiques pour être la plus vertueuse possible dans son modèle de fonctionnement et non chercher à importer des *modus operandi* d'autres contextes ; « ce qui est bon pour les autres ne l'est pas forcément pour moi ».

Un juste équilibre pertinent est à **trouver** entre sécurité réglée et sécurité gérée. Celles-ci se doivent d'avoir une réciprocité catalysante et non antagoniste. Alors que la sécurité réglée est majoritairement issue du résultat d'une démarche centralisée et réglementaire, consolider la sécurité gérée suppose un investissement de la part de l'organisation dans les compétences des managers et des agents et favorise les marges de manœuvre du management de proximité, les échanges entre professionnels et une discussion collective autour du retour d'expérience.

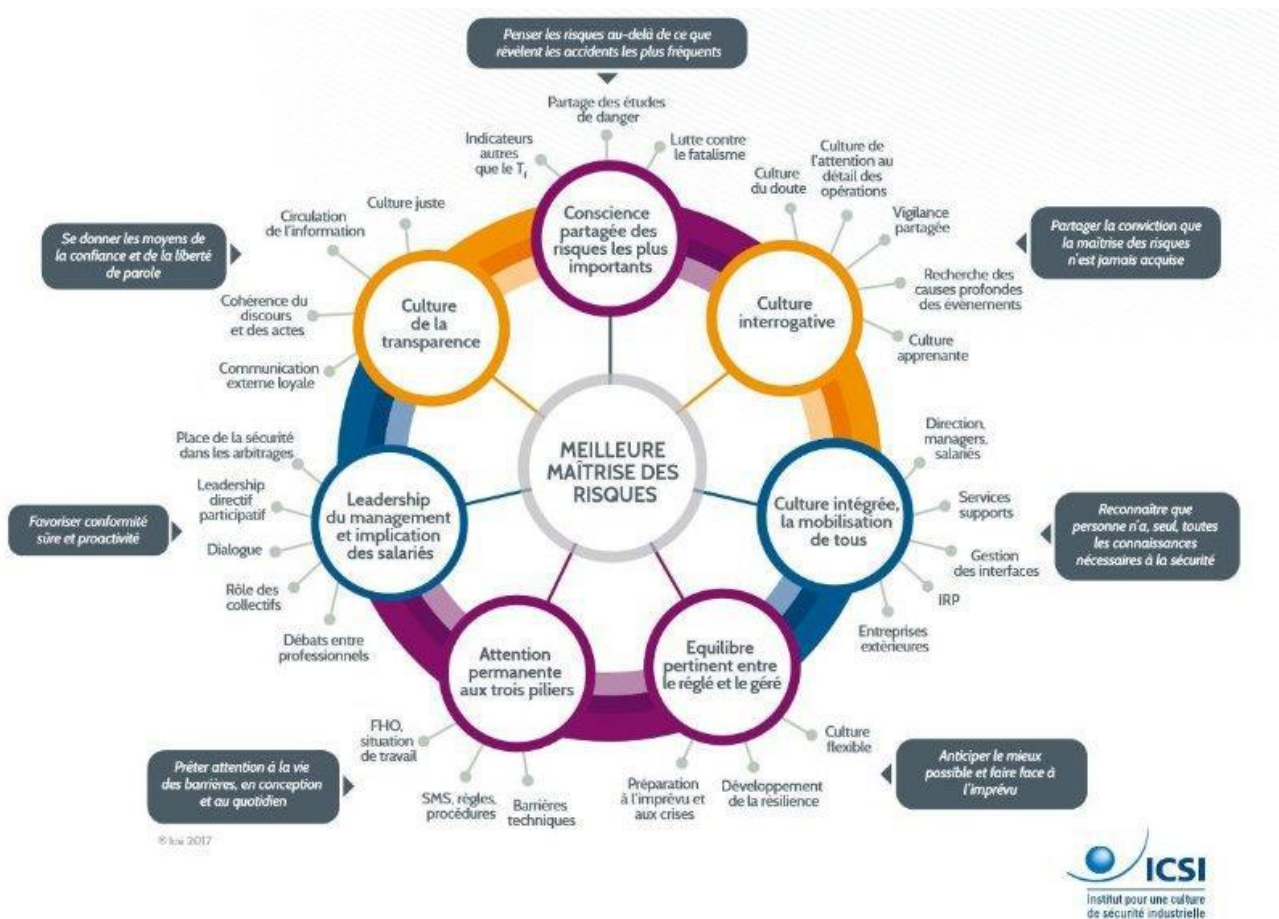
Faire évoluer la culture de sécurité de sa structure passe par une **évaluation** portant à la fois sur un diagnostic des différentes catégories d'acteurs et sur leurs perceptions de la gestion de la sécurité. Là encore, plus ce diagnostic est partagé avec tous les acteurs de l'entreprise, plus les chances de mobilisation par la suite, sont élevées. Cependant, cette évaluation n'est pas une fin en soi. Celle-ci ne doit être mise en œuvre que si l'organisation est mûre pour affronter collectivement et traiter les problèmes, aussi profonds soient-ils, que ferait remonter le diagnostic.

Faire évoluer sa culture de sécurité est un projet à long terme et un véritable projet de changement. Il ne s'agit pas d'une compilation ou accumulation d'actions hétéroclites mises

en place de façon exclusivement descendante. Ce projet passe par l'accord sur l'état initial diagnostiqué et une vision partagée du niveau de sécurité souhaité. L'évolution de cette culture ne se limite pas seulement à la sécurité mais doit être étendue à des transformations profondes de l'organisation et de sa ligne managériale. Elle s'inscrit dans une démarche continue, nécessitant un engagement permanent de tous les acteurs.

Se diriger vers une culture de sécurité intégrée et s'en **fixer l'ambition**, passe par une combinaison d'approche stratégique, de volonté de mobiliser tous les acteurs et par un choix limité de processus clés.

La culture de sécurité n'est pas un coût mais un investissement et un levier de développement. Son amélioration induit l'amélioration de l'**organisation** en travaillant sur les fondements de son fonctionnement. C'est un levier stratégique pour renforcer la performance globale de l'entreprise, car consensuelle, la sécurité est un point d'entrée pour travailler sur l'organisation où toute avancée aura un impact global dans tous les domaines de l'entreprise¹²⁶.



Aussi, qu'en est-il maintenant de la sensibilité des chefs d'entreprises sur la culture de sécurité globale et la gestion de crise au sein de leurs structures ?

¹²⁶ICSI, L'Essentiel de la culture de sécurité, Avril 2017. Collection Les Essentiels de la Sécurité Industrielle.

4) Hypothèses

a. Méthodologie de travail

i. Le processus de recherche

Le présent mémoire s'inscrit dans les champs des sciences humaines, disciplines qui étudient les phénomènes humains, et des sciences sociales, qui étudient les comportements et les évolutions des groupes humains en faisant appel à différentes disciplines : politique, sociologie, histoire, anthropologie, économie, management... Le but de ces sciences est de trouver des explications aux phénomènes qui nous entourent et que nous observons. Ces recherches fondamentales permettent une meilleure connaissance de l'Homme sur l'Homme et de fait, contribuent à faire évoluer des pratiques, techniques, comportements... de façon directe ou indirectes.

La démarche scientifique est un ensemble d'étapes ordonnées et logiques permettant de parvenir à un résultat en respectant des principes de recherche et des règles méthodologiques, en utilisant des techniques et outils et par l'adoption d'une attitude de chercheur. Son but est d'apporter des éléments de réponse à la question de recherche en recueillant des données sur le terrain, en appuyant toute affirmation par une recherche, en décortiquant la complexité de la réalité et en répondant aux hypothèses posées.

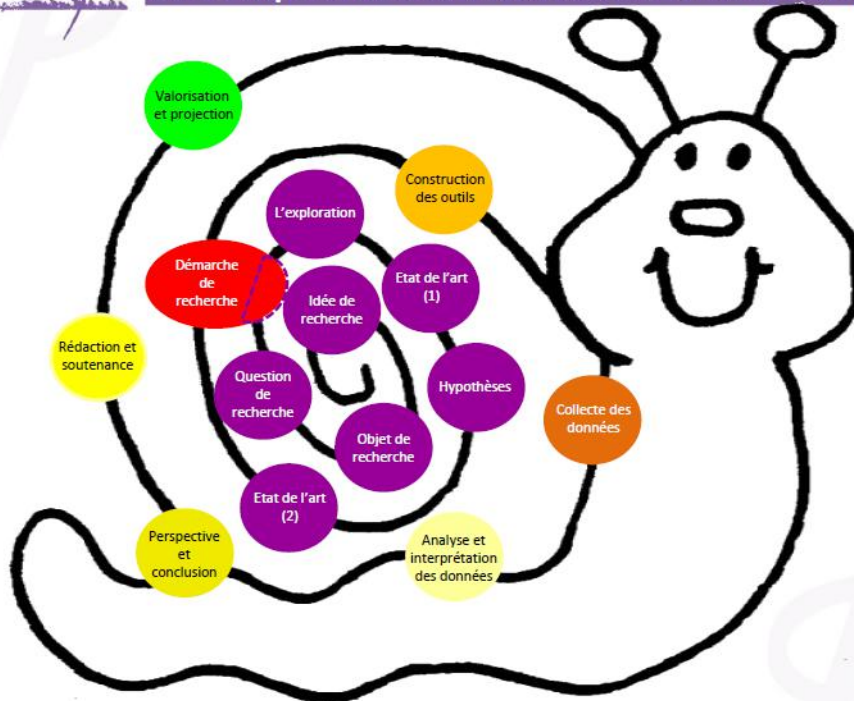
Pour cela la recherche scientifique a à sa disposition des méthodologies de travail et un arsenal de méthodes (documentaliste, pré-enquête, expérimentation, enquête, analyse de trace) et de techniques (observation, questionnement, entretien, analyse de contenu auprès d'un échantillonnage ciblé). Aussi, plusieurs outils peuvent être utilisés dans le cadre de la recherche scientifique : Questionnaires, sondages, journaux, revues, médias sociaux, livres, thèses, mémoires, sites web, grilles d'observation, grilles d'évaluations, grilles d'entretiens...).

Une fois la matière collectée il s'agit de pouvoir en faire une analyse et une interprétation.

L'analyse des données va consister à scruter les particularités des données recueillies, établir des liens entre ces données et confirmer ou infirmer les hypothèses. Enfin, l'interprétation permettra de répondre à la question de départ et de suggérer de nouvelles façons d'aborder le phénomène.

ii. La démarche scientifique

Les composantes de la conduite d'une recherche peuvent se regrouper selon une disposition en colimaçon, illustrée par le schéma de la partie 3 « La démarche scientifique » et 4 « Les étapes de la démarche » du cours du Commandant Eric DUFES (17/03/2015) « Recherche en Sciences Humaines et Sociales », du département de prospective et de professionnalisation, division des formations supérieures de l'ENSOSP :



Les étapes fondamentales premières vont graviter autour de la définition de l'idée de recherche (sur quoi je veux travailler ?), l'objet de recherche (Qu'est-ce que je veux observer ?) et sur quelle échelle d'observation (Quelle limite je me fixe ?).

Une fois les réponses apportées à ces questions, le schéma des étapes de la recherche va s'articuler autour de 7 étapes clés :

La question de recherche :

Objectif :

Critères de qualité : Exempte de toute présupposition, circonscrite, ne pas porter sur des situations hypothétiques, clair, réalisable, pertinente

L'exploration - Les lectures :

Objectif : Faire le point sur les connaissances intéressant la question de départ en exploitant au maximum le fond de celles-ci

Critères de qualité : Sélectionner les textes, variés les sources, lire de façon attentive, résumer chaque lecture ou noter les éléments important des textes, comparer les textes

Les hypothèses :

Définition : Prédiction émise par le chercheur quant aux résultats de sa recherche

Critères de qualité : Construire les hypothèses et le modèle en précisant les relations entre les concepts, les relations entre les hypothèses. Construire les concepts en précisant les dimensions et les indicateurs.

Les cadres théoriques mobilisés :

Précise sous quelles disciplines scientifiques vont s'orienter les axes de recherche

Stratégie de recherche :

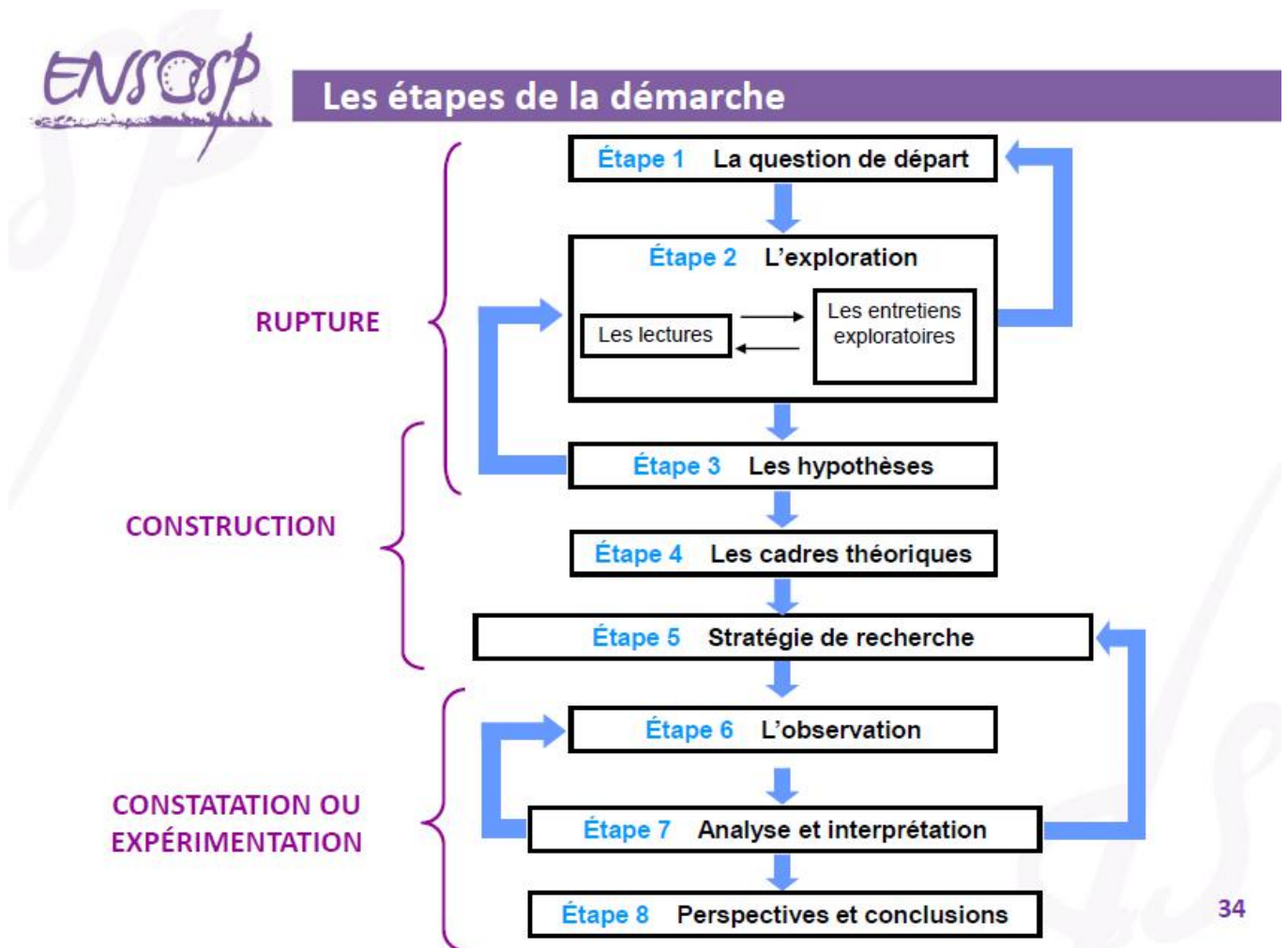
Délimiter le champ d'observation et conception des outils d'observation

L'observation :

Tester l'outil d'observation puis réaliser la collecte des informations

Analyse et interprétation :

Décrire et préparer les données pour l'analyse - Mesure les relations entre les variables – Comparer les résultats attendus et les résultats observés – Rechercher la signification des écarts

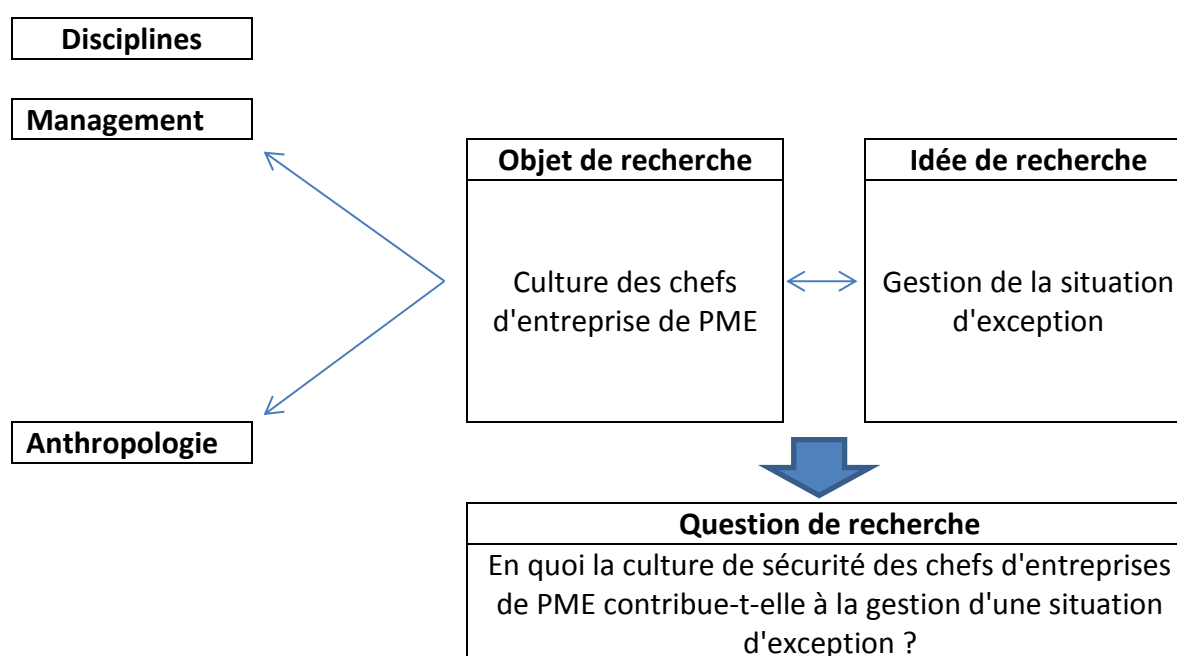


iii. Méthodologie personnelle appliquée

La première étape pour la réalisation de ce mémoire fut de **définir l'objet et l'idée de recherche** qui m'ont **amené à la question de recherche**. De là je me suis **positionné sur les angles disciplinaires** sur lesquels je voulais réaliser l'étude.

Mon passé de chef d'entreprise, mon quotidien professionnel en tant que chargé de développement qui me fait évoluer dans les écosystèmes entrepreneuriaux, mon implication associative de « Conseiller Technique National Opérationnel (CTNO) »¹²⁷, l'objet du Master en Sécurité Globale Appliquée avec spécialité Gestion de Crise et les orientations à terme sur une offre de formations spécialisées aux entreprises en élargissement de la gamme actuelle, m'ont naturellement amené à m'intéresser à la sécurité globale des entreprises avec un focus sur la culture des chefs d'entreprises en ce domaine.

Le schéma conducteur de l'étude a été défini :



Une fois le socle de la démarche posée, la construction du plan du mémoire a pu être conçu avec une articulation autour de deux grandes parties. La première est consacrée à un **travail exploratoire** sur trois thèmes :

- 1) Le panorama des PME avec pour objectif d'avoir une vision sur ce qu'est une petite et moyenne entreprise en France avec ses éléments caractérisant, ses forces et vulnérabilités. Cette partie doit permettre de comprendre le fonctionnement d'une PME et de ce fait, quel impact sur la culture de sécurité globale de ses dirigeants.

¹²⁷ Groupe des experts de la Croix-Rouge française sur la gestion de situations exceptionnelles (catastrophes naturelles, technologiques, sociétales, dispositifs de secours de grandes envergures) en France et à l'international, en soutien des équipes départementales ou intégré à la direction des opérations conduites par la Direction de l'Urgence et des Opérations. Au quotidien, les CTNO travaillent sur des dossiers nationaux.

- 2) Une vision des problématiques qui me sont apparues comme majeures de par leurs actualités en termes de problématiques de sécurité globale ; Cybersécurité, Intelligence économique, Sûreté des voyageurs d'affaires et expatriés et Santé Sécurité au Travail. Ce choix a été arbitré en tenant compte de l'actualité médiatique, nationale, internationale, une vision empirique et des échanges formels et informels avec mon écosystème professionnel. Ces éléments doivent permettre de comprendre de façon focale ce que représentent ces vulnérabilités pour les PME et en quoi celles-ci impactent elles ces entreprises. Enfin, j'ai voulu observer la représentation du concept de sécurité globale et la gestion de crise dans les entreprises et en quoi ce concept et démarche ce traduit pour les PME.
- 3) Une définition allant du concept général de culture pour arriver au focus sur la culture de sécurité en entreprise. Cette dernière partie explorée doit permettre de cibler les marqueurs communs et spécifiques à l'étude en termes de culture, culture d'entreprise et culture d'entreprise de sécurité globale. De plus cette partie doit permettre de construire les outils qui seront utilisés dans la recherche de l'origine de la culture (ou inculture) des chefs d'entreprise sur la sécurité globale et l'intégration par ceux-ci de la gestion d'une situation exceptionnelle ou de crise.

Ce travail exploratoire m'a permis de réaliser l'étude de **l'état de l'art**¹²⁸ sur la question de recherche et fut possible grâce aux lectures que réalisées. La première étape fut de benchmarker des documents en open source ou achetés. Ceux-ci se déclinent en quatre types d'origines :

Sites web	Réseaux sociaux	Revues	Publications
www.foncsi.org www.apave.com www.cairn.info www.revuegestion.ca www.actu-environnement.com www.entreprise-territoire-de-sante-malakoffmederic.com www.service-public.fr www.pistes.revues.org	LinkedIn	Observatoire des PME Cahiers de l'ENSOSP AGIR Mag	L'essentiel de la culture de sécurité de l'ICSI Conviction de l'ICSI Tribunes de la sécurité Industrielle du Foncsi

¹²⁸ Wikipédia : L'**état de l'art** est l'état des connaissances et des règles existantes sur un sujet d'étude dans tout domaine des sciences, techniques, arts et métiers. *Faire l'état de l'art* consiste à rechercher toutes les informations, publications formelles ou informelles, découvertes, nouveautés et inventions sur toutes les dernières avancées scientifiques, techniques, économiques ainsi que sur les travaux antérieurs ayant un lien avec le domaine sur lequel on s'apprête à travailler. Cette démarche est préliminaire à tout travail de recherche ou d'application. L'emploi du terme est à relier à celui d'**état des connaissances** dans les domaines de la recherche scientifique ou de la recherche médicale, ainsi qu'à celui de **règles de l'art** en architecture, en ingénierie et dans le bâtiment et les travaux publics.

www.expertsdelentreprise.com www.usinenouvelle.com www.lenouveleconomiste.fr www.acrie.unblog.fr www.entreprendre.fr www.inhesj.fr www.bienpublic.com www.lentreprise.com www.constructif.fr www.ideas.microsoft.fr www.theconversation.com www.champpenal.revues.org www.fr.wikipedia.org www.lesechos.fr		Cadre et Dirigeant Magazine	Baromètre de la sécurité des collaborateurs à l'international (CDSE et AXA)
--	--	-----------------------------	---

La majorité sont issues de sites, publications et réseaux sociaux professionnels axés « entreprises » et ce dans un choix délibéré pour coller au plus près de l'écosystème de ces organisations ; une étude issue du monde de l'entreprise pour les chefs d'entreprises et par extension de l'intérêt scientifique, pouvoir être sensibilisateur, réveilleur de conscience et questionneur sur les pratiques pour les dirigeants de PME. Fort de ces éléments incluant témoignages de chefs d'entreprises et d'experts ainsi que des références issues de la recherche scientifique la rédaction renseignée de chaque chapitre a pu être possible.

L'hypothèse bi variée où « la culture de sécurité des chefs d'entreprises de PME n'est pas assez développée alors que celle-ci pourrait améliorer la gestion d'une situation d'exception ou de crise » se nourrit des lectures réalisées lors de la phase exploratoire et intègre aussi la méthode de l'enquête menée auprès d'organisations professionnelles et consulaires, et d'organismes de formation de type « Business School ». La méthode de l'enquête consiste à mesurer des conditions objectives d'existence auprès des enquêtés afin d'établir une ou plusieurs relations d'association entre un phénomène et ses déterminants. Son principe est de découvrir des résultats tangibles en tissant des liens afin de pouvoir éclairer les hypothèses. La technique mise en œuvre est celle de l'entretien et consiste à recueillir le point de vue personnel des participants sur un sujet donné au moyen d'un échange verbal personnalisé entre ceux-ci et « l'enquêteur ». Ceux réalisés sont individuels et semi-directifs, et permettent de sonder qualitativement des interlocuteurs différents. Les personnes faisant l'objet de l'entretien sont issues de mon entourage professionnel direct (partenaires, clients, réseaux) ou de mises en relations par des prescripteurs (Sophie Nanin Conseil, partenaires, réseaux). Pour les organisations professionnelles et consulaires, les personnes appartiennent au MEDEF¹²⁹, Union Patronale¹³⁰, CPME¹³¹, CCI¹³², CJD¹³³ et pour les « Business School » à

¹²⁹ MEDEF : Le Mouvement des Entreprises de France est une organisation patronale fondée en 1998, représentant des entreprises françaises (Wikipédia).

¹³⁰ Union patronale : Syndicat patronal interprofessionnel regroupant les adhérents du MEDEF et de la CPME.

¹³¹ CPME : La Confédération des Petites et Moyennes Entreprises, créée en 1994, est une organisation patronale française représentant les petites et moyennes entreprises (Wikipédia).

des écoles de Haute Garonne (LIMAYRAC, ISG) et de l'Aveyron (Centre de Formation de la CCI). Le choix s'est porté sur ces structures pour connaître en amont du « métier » de chef d'entreprise si les écoles de Management préparaient les futurs dirigeants aux problématiques de sécurité globales et pour les organisations professionnelles si celles-ci contribuent à la naissance ou l'émergence ou l'entretien de la culture de sécurité globale des chefs d'entreprises. Les entretiens ont été réalisés en présentiels sur sites ou en distanciel par téléphone. Les personnes ont été sollicitées par mail avec un message type et adapté à leur appartenance (organisation ou business school). L'objet du mail et les éléments de langage se veulent marketés pour optimiser l'incitation des destinataires à répondre favorablement à la sollicitation. Des relances téléphoniques ont permis de concrétiser les rendez-vous. Les questions et argumentaires figurent en annexe.

La seconde partie se décline en deux axes avec une approche anthropologique pour l'une portant sur « L'acculturation des chefs d'entreprises sur la sécurité globale » et managériale pour l'autre avec « L'intégration des PME de la gestion d'une situation d'exception ou de crise ». Le travail sur ces axes a été rendu possible grâce au résultat des lectures des documentations de la phase exploratoire et de l'étude de l'art mais surtout grâce à la méthode de l'enquête et de la technique du questionnement que j'ai choisi d'utiliser. La technique du questionnement quant à elle, a l'avantage d'être souple permettant de collecter assez facilement et rapidement toutes sortes d'indicateurs¹³⁴. Le questionnement s'est fait grâce à un questionnaire dématérialisé réalisé via la plateforme internet www.askabox.fr. Le choix s'est porté sur cette plateforme pour sa facilité d'utilisation (ergonomique, intuitive), les fonctionnalités proposées (exportation des résultats, synthèse des résultats, suivi des réponses...) et son coût (24,00 € net pour 2 mois de validité). Le questionnaire intitulé « La culture de sécurité des chefs d'entreprises de TPE/PME » porte sur 28 questions ouvertes ou fermées dont 26 demandent une réponse obligatoire. Celles-ci intègrent les champs du management et de l'anthropologie, axes de l'approche du thème du présent mémoire. Celui-ci a été envoyé par courriel depuis ma boîte mail professionnelle. Le corps du mail contient les éléments contextuels de cette enquête : Cadre et objet, confidentialité et utilisation des réponses, temps nécessaire pour répondre aux questions et le lien permettant d'accéder directement aux questions. L'objet du mail et les éléments de langage se veulent marketés pour optimiser l'incitation des destinataires à répondre au questionnaire. L'enquête, introduction et questions, figure en annexe. Le questionnaire a été envoyé à des entreprises privées des secteurs de l'industrie, bâtiment, commerce, service, agricole, et établissements privés du sanitaire, social et médico-social avec l'objectif que celles-ci répondent directement. Les PME destinataires, sont essentiellement issues du fichier clients et prospects, et fichier fournisseurs utilisés par le Centre Régional de

¹³² CCI : La Chambres de Commerce et d'industrie est un organisme chargé de représenter les intérêts des entreprises commerciales, industrielles et de service (Wikipédia).

¹³³ CJD : Le Centre des Jeunes Dirigeants, créé en 1938, est une organisation non partisane et se veut force de proposition pour l'emploi et la pérennité des entreprises (www.cjd.net).

¹³⁴ DUFES E. « Le processus de la recherche » cours DEPRO – FORSUP de l'ENSOSP (19/02/2016) – Méthode de l'enquête et techniques du questionnement et de l'entretien.

Formation Professionnel (CRFP Occitanie). Le secteur géographique est majoritairement l'ex région Midi Pyrénées auquel se rajoutent d'autres départements où se trouvent les sièges de certaines entreprises. Les autres cibles sont les prescripteurs servant de relais pour diffusion auprès de leurs adhérents ou contacts. J'ai ciblé pour cela les trois organisations professionnelles patronales principales que sont la CPME, le MEDEF et le CJD du territoire (coordonnées des responsables régionaux et départementaux trouvées sur leurs sites internet), les pépinières d'entreprises de Midi Pyrénées et mobilisé les partenaires du CRFP Occitanie (CCI 46 et 82, Synéthic, Aéqualis Prévention, CDG82, APREVAT...) et réseaux professionnels auxquels le Centre est adhérent ou en relation (DYNABUY, Réseau Dirigeant PME, Club de la Com', BNI, CAMP, Club Ricochen...). Un message spécifique accompagne le mail et explique l'objet de leur sollicitation. L'autre canal de diffusion fut la publication sur les réseaux sociaux, invitant les professionnels à répondre à l'enquête : comptes LinkedIn personnel, comptes twitter des pôles Santé Sécurité au Travail et Sanitaire & Social du CRFP Occitanie. Enfin, mon entourage personnel (amis, collègues, bénévoles Croix-Rouge) a été mis à contribution soit en tant que prescripteur, soit en tant que destinataire direct.

b. La culture de sécurité des chefs d'entreprises n'est pas assez développée alors que celle-ci pourrait améliorer la gestion d'une situation d'exception

Il est coutume d'entendre que les chefs d'entreprises de PME ont une sensibilité somme toute relative quant aux préoccupations de sécurité globale, occupés ou préoccupés à d'autres problématiques plus opérationnelles, sur le développement de leur activité. Au mieux les contraintes réglementaires et les obligations en Santé Sécurité au Travail les sensibiliseraient à minima. De plus, face à un monde globalisé, en mouvement et très concurrentiel leur action serait de piloter au cap leurs organisations alors que la réalité de terrain est marqué par un pilotage à vue. L'anticipation est au mieux axée sur du développement produit mais plus généralement sur de la captation d'opportunité et leur approche systémique gravite de façon focale autour de la trilogie *Commercialisation* – Trouver de nouveaux clients et de nouveaux produits/services à vendre, *Gestion* – Optimiser les couts et sauver les marges, *Ressources Humaines* – Recruter les bons collaborateurs, optimiser la masse salariale et éviter le Turn Over. Il serait aisé de dire que le manque de temps est l'alibi à nombre de champs non ou partiellement abordés dont la sécurité et pour lequel seul un événement majeur viendrait éveiller la conscience des chefs d'entreprises (accident grave, attaque du réseau informatique, vol de secret de fabrication...). Sur la même fibre, leur attention est portée sur 80% de leurs préoccupations de terrain à impact direct sur leurs organisations, occultant les 20% restant pouvant engendrer 80% de conséquences lourdes. La notion de « ça n'arrive qu'aux autres ou ça ne peut pas m'arriver vu mon entreprise (NDRL : taille, activité, situation géographique...) » est-elle un mythe ou une réalité de dénis ou d'occultation ? Ces comportements pourraient aussi se traduire par un excès de confiance telle que portée envers la main invisible qui vient réguler les marchés. Enfin, leur ADN n'est-il pas uniquement un code dont le programme se porte sur la trilogie

Commerce/Gestion/RH, transmis dans leurs cursus, de formation initiale et continue ? Nous pouvons enfin penser qu'être chef d'entreprise c'est accepté le risque et l'inconnue (risque de se tromper, évolution du marché, risque d'une plus faible qualité de vie) et de fait, la notion de sécurité est paradoxalement la zone d'inconfort de ceux-ci. Aussi, qu'en est-il de l'état de culture de sécurité des chefs d'entreprises de PME ?

Dérèglement climatique et accentuations des accidents météorologiques, menace terroriste, mondialisation des marchés, évolution sociétale avec une société de plus en plus procédurière, hacking à la portée de tous, arnaques de plus en plus élaborées.... Les entreprises évoluent dans un univers où les menaces sont 360°. A tout moment celles-ci peuvent avoir à gérer une situation exceptionnelle, les sortants de leur état d'équilibre précaire du quotidien. La non préparation à ce type de situation, une non réaction ou réaction trop tardive peuvent rapidement les amener à une situation de crise souvent fatale pour des organisations fragiles par nature pour la majorité. Une simple tempête associée à une pluie importante venant emporter un toit et inonder les locaux, occasionnent la perte des matériels informatiques dont les données non sauvegardées sur un serveur et c'est l'entreprise qui disparaît en même temps. Un voyageur d'affaire envoyé en zone à risque sans mesure particulière de sécurité et victime d'un enlèvement et c'est, au-delà du drame humain, l'entreprise qui voit son image se dégrader. Les conséquences sont directes et immédiates : perte de confiance et accès au concours bancaire plus difficile, résiliation de contrats ou conditions tarifaires plus élevées pour les assurances, délais de paiement plus courts demandés par les fournisseurs, fuite de clients ne voulant pas être associés à l'image de l'entreprise... Faire face à des situations exceptionnelles, (levier bancaire pour palier un trou de trésorerie, adaptation à un pic de demande...) est un savoir-faire qu'ont les chefs d'entreprises et qu'ils utilisent au quotidien. Celui-ci pourrait facilement être transposé au domaine de la sécurité. Aussi, qu'en est-il de l'état de préparation et d'organisation des PME à gérer une situation d'exception ou de crise ?

Au risque d'enfoncer des portes ouvertes sur la réponse à l'interrogation ou affirmation selon la sensibilité de chacun « La culture de sécurité des chefs d'entreprises n'est pas assez développée alors que celle-ci pourrait améliorer la gestion d'une situation d'exception », la prétention ici est de chercher à connaître ce qu'il en ait de l'état de la culture de sécurité des chefs d'entreprises et leur capacité induite à faire face à une situation exceptionnelle ou de crise. Ainsi, par le biais de témoignages de professionnels en lien direct avec le monde de l'entrepreneuriat (organisation professionnelles, consulaires et business school), j'ai cherché à savoir comment cette culture était perçue et objectivée, et comment dans les faits les PME se préparent-elles, ou pas à faire face à une situation d'exception ou de crise de sécurité globale.

Plusieurs interlocuteurs du réseau du Centre Régional de Formation Professionnelle de la Croix Rouge Occitanie ont été sollicités et des entretiens physiques ou téléphoniques ont été réalisés. Ceux-ci constituent l'échantillon de la pré enquête (**annexe 1**) :

Organisations professionnelles :

Prénom Nom	Organisation	Fonction
Audrey PRAT	Office de l'Artisanat et du Commerce du Centre (ODAC) de Montauban	Coordinatrice
Carole DULION	MEDEF de Haute Garonne	Chargée de Communication
Commission Sécurité	CPME de Tarn et Garonne	Conseil aux adhérents
Corinne MAZENC	MEDEF de Tarn et Garonne	Déléguée Générale
Dominique SATGE	Union Patronale du Lot	Directrice
Fabienne ROULLEAU	CPME de Tarn et Garonne	Secrétaire Générale
Julien LECLERQ	Centre des Jeunes Dirigeants du Lot et Garonne	Président
Michel VIGIER	Union Patronale de l'Ariège	Délégué Général
Olivier ASPE	Chambre de Commerce et d'Industrie de Montauban et de Tarn et Garonne	Sécurité au Travail, QSE, Club RH, Développement International
Yan BRUGAROLAS	Chambre de Commerce et d'Industrie de Toulouse et de Haute Garonne	Chargé de Mission Sécurité et RSE

Le premier élément constaté est la disparité de matière apportée par les interlocuteurs avec des organisations ayant une approche, sensibilité et engagement très disparate des problématiques de sécurité. Le plus flagrant est de constater que celles issues d'un bassin économique fort et très urbain ne semble pas les plus impliquées alors que des territoires plus ruraux ont un dynamisme en la matière allant de engagé à très engagé. Les indicateurs permettant de donner corps à ces propos sont le temps consacré à l'entretien (de quelques minutes au téléphone à plus d'une heure en présentiel ou distanciel), la facilité d'accès aux interlocuteurs (de très simple à entretien obtenus avec forte insistance), la matière fournie (de quelques lignes pauvres à deux pages de notes qualitatives), la perception des problématiques de sécurité des adhérents (de méconnaissance à forte connaissance) et les actions menées de soutien et d'information/formation. Une première remarque ; **comment les chefs d'entreprises peuvent-ils construire ou développer leurs cultures de sécurité si leurs organisations professionnelles ou consulaires ne sont-elles même pas engagées ou sensibles à ce thème ?** Passé ce premier constat l'autre élément marquant concernant ces structures est de constater que pour leur majorité, le premier réflexe lorsque l'on parle de sécurité est de faire le lien direct avec la Santé Sécurité au Travail. Les autres thématiques ne venant qu'avec un rappel du champ de l'étude sur la « Sécurité Globale » : cybersécurité, sureté/malveillance, intelligence économique... Nous pourrions voir que cette dominance pour ce thème pourrait s'expliquer car en lien avec une sensibilité similaire pour les entreprises.

La perception des interlocuteurs sur la culture de sécurité est convergente. Les chefs d'entreprises ne seraient que peu concernés par la sécurité et ce même lors de leur installation. Ceux connaissent peu la réglementation ou ne s'y intéressent pas. Ce constat est aussi palpable lors de rassemblement de chefs d'entreprises où le sujet n'est que peu présent dans les conversations. Ceci est d'autant plus vrai pour les micros entrepreneurs « Je suis seul donc pas concerné » ou des questions paraissant ne pas les atteindre de par leur activité, taille ou zone géographique. Un prospect de l'ADEM, conseil en sûreté et terrorisme, s'est ainsi exprimé « je ne suis pas concerné par le terrorisme donc pas de besoins » alors même que Montauban a été le théâtre d'un attentat perpétré par Mohamed Merah en 2012 ou un adhérent de la CCI 82, exportateur de fruits et légumes concernant la sûreté de ses voyages d'affaires à l'étranger en zones sensibles « Je ne fais pas de pétrole, je n'intéresse personne ». Enfin encore plus optimiste... « Ça ne nous touchera pas » laissant ainsi l'Union Patronale de l'Ariège dire que « les chefs d'entreprises ne se rendent pas compte et font preuve de naïveté » face aux problématiques de sécurité. Tant que l'entreprise n'est pas confrontée à un problème de sécurité (accident grave, attaque cyber, vol, ransomware...), celle-ci ne se sent pas concernée. Un membre de la commission sécurité de la CPME 82 parle de « syndrome du passage à niveau non protégé ». Lors des entretiens, les entreprises ont perçu le danger des cyberattaques après avoir été victime d'un virus avec demande de rançon de la part des hackers. Les dirigeants ne prennent pas ou peu de temps pour se pencher sur les aspects de sécurité (process, formation, information...) car contraints à des actions plus opérationnelles (gestion, production, commercialisation, communication/marketing). Ce constat peut s'expliquer par les tensions des environnements économiques et concurrentiels des entreprises. Ainsi, le rapport bénéfice/cout ne joue pas en faveur de la sécurité d'un premier abord mais est-ce une démarche bien calculée tant les dommages peuvent être importants lors de la survenue d'un événement comme nous avons déjà pu le voir. De plus, si nous nous basons sur des aspects uniquement financiers, il a été montré que pour 1 euro investi, le gain est de 2 euros sur un an ! Un bémol est toutefois mis pour les PMI à risques ou à technologie sensible (sous traitance aéronautique par exemple) ; où ainsi le secteur d'activité serait un marqueur de sensibilité aux problématiques de sécurité globale. Enfin la Santé Sécurité au Travail est LE domaine qui se démarque de part... son côté réglementaire et obligations des chefs d'entreprises en matière de moyens et résultats sur la santé et sécurité physique et mentale des salariés. De plus, les coûts directs et indirects générés par les accidents du travail et maladies professionnelles, le financement des formations sécurité, et l'impact des conditions de travail sur la productivité et le maintien des salariés dans les entreprises contribuent à ce constat. Des secteurs d'activité ont aussi des obligations pour leurs clients tels que les hôtels et entreprises de transport (incendie) avec des contrôles fréquents et sanctions à la clé allant de l'amende à la fermeture administrative. Deux entretiens me sont apparus particulièrement intéressants pour illustrer les éléments sus cités.

Julien LECLERCQ, Président du Comité des Jeunes Dirigeants du Lot et Garonne : « Les chefs d'entreprises ne pensent pas à tout et se focalisent sur leur projet. On se rend compte des problématiques, quelles qu'elles soient au fur et à mesure que l'on progresse. Cependant et à notre décharge nous ne disposons que peu d'informations sur les contraintes administratives et juridiques. Les aides disparaissent au bout de 3 ans et ensuite, c'est là que les contrôles apparaissent et que nous prenons conscience de tous ces éléments. Il y a trop de réglementation et peu de temps pour nous de tout absorber. Cependant nous ne pensons pas à tous les risques et contraintes sinon personne n'irait dans l'entrepreneuriat. Des organisations telles que la Chambre de Commerce et d'Industrie proposent des séances d'informations mais celles-ci se font dans leurs locaux et pas pratique pour les chefs d'entreprises que de se déplacer pour assister. Les aides disparaissent au bout de 3 ans et ensuite, c'est là que les contrôles apparaissent et que nous prenons conscience de tous ces éléments. Des formations sont à développer pour leur culture encore faut-il que ceux-ci prennent le temps pour le suivre. A ma connaissance notre organisation ne propose pas de sessions de formation ou d'information sur les questions liées à la sécurité si ce n'est une soirée thématique sur la santé sécurité au travail. Il faut du temps pour que ces notions de sécurité entre dans les mentalités. Les chefs d'entreprises de TPE et PME ne se sentent pas concernés et pensent que beaucoup de questions de sécurité ne touchent que « les gros » notamment en cybersécurité et intelligence économique. Pour faire évoluer les mentalités et donner une culture de sécurité, des séances de sensibilisation avec des exemples concrets de terrain et témoignages de chefs d'entreprises seraient intéressantes ainsi qu'un accompagnement par des pairs en plus des experts sur cette thématique ».

Dominique SATGE, Directrice de l'Union Patronale du Lot : « Le rajeunissement des chefs d'entreprises et des événements dramatiques survenus dans le département avec des suicides de chefs d'entreprises et d'accidents graves de salariés, ont contribué à faire évoluer les cultures de sécurité. En santé sécurité au travail, cette culture commence à arriver grâce à l'angle pris par la prévention et non plus par le concept du salarié apte ou inapte. Les chefs d'entreprises gardent cette réaction épidermique s'ils se sentent mis en accusation. Globalement intégrée dans les grandes structures, elle est plus compliquée pour les PME même si au cœur des sensibilités notamment par le fait que la santé des salariés influe la santé de l'entreprise. De plus les bons salariés n'hésitent pas à quitter l'entreprise s'il y a de mauvaises conditions de travail. Les jeunes, mais aussi moins jeunes chefs d'entreprises ont conscience qu'il faut faire quelque chose et n'hésitent pas à faire des groupes de travail thématiques. Concernant la cybersécurité, il y a un réel défaut de mesure de danger. Le niveau de confiance est trop haut, les entreprises ne se sentent pas concernées de par le territoire alors que des faits (attaques) existent. La CCI a cependant mis en place une sensibilisation sur ce sujet. Les problèmes de sûreté et malveillance sont sur une autre notion et parce qu'ils sont assurés contre le vol, peut d'actions sont entreprises. Seul une succession de vols sur le secteur de Biars (Nord du département) a engagé une demande particulière et des opérations de sécurité menées avec la CCI du Lot a permis de faire cesser les délits. Paradoxalement, le terrorisme et phénomène de radicalisation commencent à les interpeller

même si nous n'avons dans le département que de rares cas de radicalisation. Enfin les entreprises sont plutôt bien sensibilisées sur l'intelligence économique et prennent des précautions surtout pour les PME à activités sensibles. Alors que la plupart des dirigeants n'ont pas de projet d'entreprise et/ou de vision sur 2 ans, ceux-ci n'ont aucune organisation et préparation quant à la gestion d'une situation de crise. Il en est de même pour les plans de continuité d'activité. Ils n'ont pas cette culture. En cas de problème majeur, les chefs d'entreprise ont le réflexe de nous appeler. Nous mobilisons alors des acteurs issus du réseau pour apporter leurs compétences et faire face à la situation rencontrée. L'Union Patronale du Lot organise des réunions de sensibilisation avec des illustrations concrètes d'études de cas sur le territoire avec 6 sessions thématiques. La prévention est un état d'esprit ».

La sensibilité des chefs d'entreprises a évolué dans le temps suite à des événements survenus de façon récurrente et pour lesquels ceux-ci ont échangé entre eux. Ces événements concernent essentiellement les cyberattaques et les questions de santé sécurité au travail. La culture des dirigeants a beaucoup évolué sur ce dernier point entre 1980 et 2000 ceux-ci se sentaient peu, voire pas concernés. Depuis 10 à 15 ans, une prise de conscience sur les effets directs dans le fonctionnement des organisations sur la productivité et les gains liés ont amené les chefs d'entreprises à investir dans la qualité de vie au travail et la prévention des risques professionnels et mettre en place un véritable management de la santé sécurité au travail. Ils répondent également à une évolution sociétale et l'attitude des salariés sur leurs conditions et qualité de travail. Les formations sur ce thème sont maintenant légion. Cependant du travail reste à faire ; à titre d'exemple, lors de la première réunion de la commission sécurité de la CPME de Tarn et Garonne, seul 4 adhérent à cette organisation professionnelle étaient présents dont 3 en lien direct avec la sécurité, sur 117 adhérents.

La préparation des dirigeants de TPE/PME à gérer une situation exceptionnelle et qui plus est de crise, est inexistante de la même façon qu'aucun dispositif de gestion de ces situations n'existe. Le réflexe face à ce type d'événement est de se tourner vers leurs organisations professionnelles ou consulaires pour la majorité des interlocuteurs interrogés. L'exception serait portée par le département de la Haute Garonne bien que la CCI soit dotée, à l'exception de la cybersécurité, de plusieurs bureaux dont un très actif en santé sécurité au travail. Là encore, le manque de temps, « *trop de chose à surmonter au quotidien* », et la notion de coût/bénéfice à court terme seraient les facteurs déterminant. De plus les TPE/PME ne disposeraient pas du personnel formé compétent pour cela, les actions se faisant sur le moment, « *Chacun ce le gère à sa façon* ».

Aussi, la plupart des organisations consulaires et professionnelles ont des dispositifs permettant de soutenir les entreprises avec des niveaux variés de solutions. Celles-ci résident vers l'orientation immédiate du chef d'entreprise vers la structure experte recensée dans le réseau d'adhérent, en lien direct avec la situation rencontrée : cyberattaque par exemple. Ces structures sont référencées et selon les organisations de façon formalisée ou pas et sont situées géographiquement à l'échelon départemental, régional

voir national selon le domaine d'expertise requis et recensé. Le MEDEF réalise au niveau national une sensibilisation sur la gestion de crise et propose un accompagnement si nécessaire lors de survenue d'un événement majeur. La Chambre de Commerce et d'Industrie de Montauban et de Tarn et Garonne, dispose quant à elle d'une cellule de crise en veille permanente. Activée lors d'un événement majeur à impact individuel ou collectif (tempête de 2016), elle est tenue par quatre personnes formées. Sa vocation est de diffuser de l'information auprès des chefs d'entreprises, mettre à dispositions de locaux en cas de sinistre, informer sur les procédures d'indemnisation ou encore d'organiser des réunions avec les services compétents de l'Etat.

Aussi au quotidien bien que peu sollicitées sauf événement comme il l'a été rapporté, des dispositifs de sensibilisation ou de formation sont proposés pour leurs adhérents sur les problématiques de sécurité. A deux exceptions près, toutes les organisations se sentent très concernées et priorisent ces actions. Toutefois toutes ces actions n'ont de participants que si le titre est bien « marketé » et sujets d'actualités. Des organisations proposent des actions selon des thèmes définis par leurs adhérents ou commission sécurité pour celles qui en sont dotées. La majorité de ses séances sont organisées sous forme de petit déjeuner ou en after work de courte durée et très accès information-action. Le rythme est de 1 à 5 par an. Le sujet phare est sans surprise la santé sécurité au travail (Faire face aux arrêts de travail, loi Macron et la DUP, droit social...), et les obligations des chefs d'entreprises sur leurs obligations (DUERP, Prévention des risques psycho-sociaux, prévention des troubles musculo-squelettiques, risque routier et chimique...). Des intervenants extérieurs (cabinet d'avocats spécialisé, assureur...). La CARSAT peut participer au financement de séances d'information sur les accidents du travail et maladies professionnelles. Les autres thèmes abordés et récurrents concernent la cybersécurité avec des interventions de la gendarmerie nationale, l'intelligence économique avec des sensibilisations faites par les Préfectures et dans une moindre mesure, les problématiques de sureté et malveillance avec la gendarmerie et police nationale. Le ressenti des organisations professionnelles et consulaires est mitigé sur l'impact mais ces séances de sensibilisation apportent des éléments de réflexion et génèrent des effets dans les entreprises à moyen terme.

Business School :

Prénom Nom	Organisation	Fonction
Caroline BURY	Institut LIMAYRAC (Toulouse)	Directrice adjointe ICD Toulouse
Patrice BRAS	CCI Formation de l'Aveyron	Directeur de l'Enseignement et de la Formation
Thomas FACHIN	ISG Programme Business et Management (Toulouse)	Coordinateur Pédagogique

Les trois business school avec lesquelles j'ai pu m'entretenir et qui assurent la formation de futurs dirigeants ou cadres dirigeants d'entreprises, n'ont aucun cours dans les cursus de leurs étudiants en lien avec la sécurité quel que soit son domaine. Non pas que le sujet

n'intéresse pas les équipes pédagogiques mais les curriculums, issus de l'éducation nationale ou du RNCP¹³⁵, n'inclut pas ce type d'enseignement. Celui-ci est trop spécialisé pour y être intégré et le timing des programmes ne permet pas d'intégrer de modules complémentaires. Certains domaines sont toutefois abordés mais ventilés dans des cours tel que l'Intelligence Economique dans les études de marché pour sa partie « benchmark concurrentiel » ou la cybersécurité dans les cours d'informatique ou lors des signatures des chartes informatiques (Institut LIMAYRAC). Le Centre d'Enseignement et de Formation de la CCI de l'Aveyron (CCI Formation 12) propose une sensibilisation à la Santé Sécurité au Travail à ses étudiants en Bachelor « Management et Commerce » dans son module sur les ressources humaines, à la demande de la CARSAT. Certains établissements proposent ou ont proposés des conférences optionnelles, dont l'acquisition des connaissances par les étudiants ne fait pas l'objet d'évaluation. Ces conférences se font hors temps de cours normé et leur suivi et à l'appréciation des étudiants. Elles se réalisent en « one shot » et non pas de façon systématique car trop compliqué à caler dans le temps. Leur organisation est très dépendante de la dynamique ou de la sensibilité des équipes pédagogiques. Par exemple, l'Intelligence Economique au-delà de son aspect veille concurrentielle est proposée par l'ISG car ce thème fut l'objet du mémoire de fin d'étude de son coordinateur pédagogique. Seule des formations très spécialisées telle que Licence Professionnelle en « Qualité Sécurité et Environnement » avec Santé sécurité au travail, sureté/malveillance et intelligence économique, « Ingénieur Informatique » avec cybersécurité et cryptographie et « Master 2 Qualité Environnement » avec risques industriels, disposent par leur nature même de cours dédiés. En revanche, aucune sensibilisation pour les « Ingénieurs Mécanique » en santé sécurité au travail... (CCI Formation 12). De plus, les stages réalisés par les étudiants au cours de leur cursus de formation, ne leur apporteraient aucune information ou sensibilisation sur ces problématiques. Cette donnée est à relativiser car de l'aveu des interlocuteurs, ceux-ci ne disposent que peu de matière pour avoir un avis certain.

La question de la capacité pressentie pour ces futurs professionnels à gérer une situation exceptionnelle ou de crise de sécurité pour les interlocuteurs est tranchée : Non ceux-ci n'auraient pas cette capacité car aucune connaissance et maturité dans ces champs-là de par leur formation. L'approche générationnelle serait aussi en cause avec une conception de la gestion des événements basée sur la réaction immédiate et non pas sur l'anticipation.

Enfin et ce de façon unanime « *et tellement évident* », toutes les personnes avec lesquels les entretiens se sont déroulés considèrent qu'un enseignement, « *d'une vingtaine d'heure* », sur les problématiques de sécurité globale devraient être intégré aux programmes de formation. et ce pour faire face aux défis d'aujourd'hui et répondre à ceux de demain. Le contexte économique, le contexte géopolitique, la mondialisation des échanges,

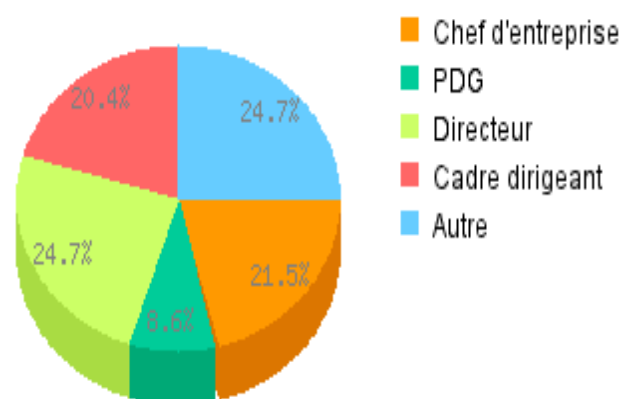
¹³⁵ Le **Répertoire National des Certifications Professionnelles** (RNCP) a pour objet de tenir à la disposition des personnes et des entreprises une information constamment à jour sur les diplômes et les titres à finalité professionnelle ainsi que sur les certificats de qualification figurant sur les listes établies par les commissions paritaires nationales de l'emploi des branches professionnelles. Il contribue à faciliter l'accès à l'emploi, la gestion des ressources humaines et la mobilité professionnelle.

l'internationalité du travail sont autant d'éléments intégrés à part entière dans les écosystèmes dans lesquels ces professionnels évolueront. « *A moins de toucher les têtes de réseau* », la difficulté réside dans la remontée, prise en compte et modification des curriculums par les instances nationales et l'inertie inhérente... Pour être totalement efficaces, toucher les cibles en profondeur de façon marquante et pérenne, pour une efficacité optimale en terme d'acquisition de connaissances, ce ou ces modules d'enseignement devraient être portés par les écoles en faisant intervenir des professionnels « *dont c'est le job* ». Cette approche serait la plus efficace pour la génération reconnaissant les compétences des individus plus que les titres ou fonctions. Une autre approche, ou approche parallèle, consisterait à intégrer de façon permanente et diluée les principes de sécurité dans tous les domaines abordés dans les cursus.

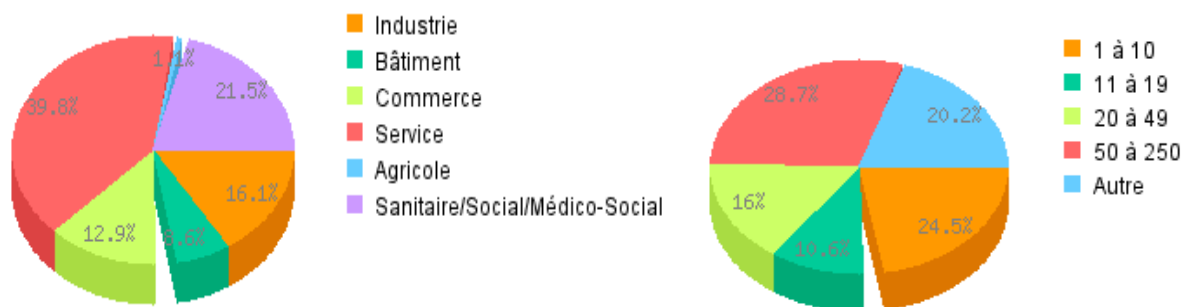
5) Axe 1 (Approche anthropologique) : L'acculturation des chefs d'entreprises de TPE et PME sur la sécurité globale

L'enquête menée sur « La culture de sécurité des chefs d'entreprises de TPE/PME » du 12/10/2017 au 11/12/2017 auprès d'entreprises de tout secteur d'activité, a permis de collecter 93 retours. Les PME/TPE ayant répondu se situent à 79,57% sur le territoire d'Occitanie Ouest, cible principale de mon échantillonnage de par l'accès aux contacts de ces structures grâce au fichier clients et prospects du centre de formation professionnelle Croix Rouge Occitanie. Toutefois, près de 20% d'entreprises issues du reste du territoire ont répondu grâce au relais des organisations professionnelles, à qui le questionnaire avait été envoyé pour diffusion. De fait, ce chiffre montre un certain intérêt pour les questions de sécurité au sein des organisations et est à considérer comme un facteur positif sur la culture des chefs d'entreprise en ce secteur.

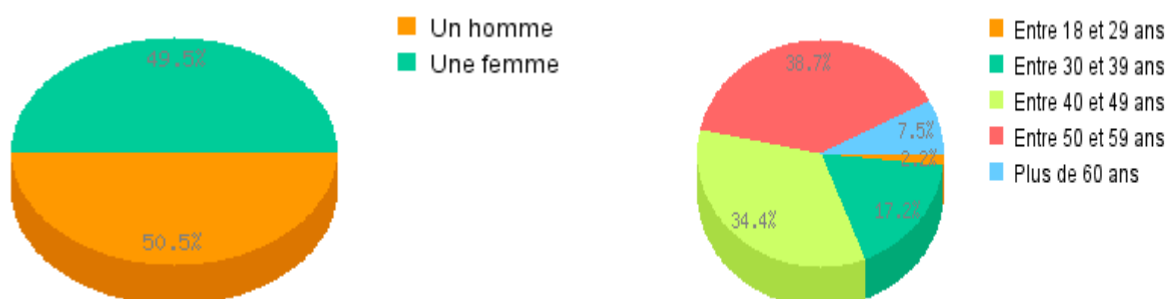
Plus de 55% des répondants sont des chefs d'entreprises, PDG ou directeurs, 20% sont des cadres dirigeants et seulement 25% exercent une fonction autre que dirigeante (formateur, chargé HSE, agent de maîtrise, responsable qualité...). Une confirmation se porte sur l'intérêt que porteraient les dirigeants sur les questions de sécurité.



Plus de la moitié des réponses sont issues d'entreprises du secteur tertiaire (52,7%) qui démontre une dynamique importante sécurité tout comme pour l'industrie et le BTP à 30,1% de par la notion historique de risques et de culture de sécurité (industrie) et la prise de conscience récente pour les travaux publics et le secteur du bâtiment. La surprise réside dans les établissements sanitaires, sociaux et médico-sociaux avec plus de 20% de réponses (21,5%) où une conscience sur la sécurité de leurs structures serait d'actualité.



Les réponses ont été apportées par près de 25% de TPE, plus de la moitié de PME (55,3%) et 20,2% d'entreprises dont la taille dépasse le cadre de la TPE/PME.



La parité homme/femme est atteinte concernant les répondants. Prêt des trois quart ont entre 40 et 60 ans (73,1%), représentant la génération X (1965-1979) et 17% dans la tranche d'âge 30-39 ans soit la génération Y (1980-2000).

Ainsi, le profil type du répondant est un homme ou une femme ayant entre 40 et 60 ans, et exerçant la fonction de dirigeant au sein d'une PME du secteur d'activité des services sur la région Occitanie Ouest (Ex Midi Pyrénées).

A la question sur comment les répondants définissent ils la sécurité globale en entreprise, 93,5% d'entre eux ont apporté une réponse (**Annexe 3**). La perception de cette notion est variée mais peut se regrouper en 4 catégories. Tout d'abord près de la moitié des réponses (49,43%) porte sur le fait que cette définition englobe tout ce qui touche à la sécurité des personnes (salariés, clients, actionnaires...), des biens matériels (bâtiments, matériels...) et immatériels (données, image...). Ensuite, dans 31% des réponses apparaissent les notions d'actions d'anticipation et de prévention de tous les risques : risques physiques, incendie, malveillance et sureté, informatique... et intègre l'ensemble des mesures d'informations et de formations. Pour 11,5% des retours considèrent que la sécurité globale est un concept intrinsèque à l'entreprise dans son fonctionnement quotidien, assurant son bon fonctionnement et de bonnes conditions de qualité de vie au travail. Enfin, obligatoire pour assurer la vie et survie de l'entreprise, la protégeant des « attaques » internes et externes, et est un levier de réussite de son fonctionnement (6,9%).

La sécurité globale en entreprise regroupe tous les domaines visant à protéger les biens matériels et immatériels ainsi que les personnes, parties prenantes de l'organisation. Ce concept intègre l'ensemble des actions de prévention des risques et, intrinsèquement lié à l'entreprise, la sécurité globale contribue à la protection, la qualité de vie et au développement de la structure de façon pérenne.

Toujours dans le registre des définitions, intéressons-nous à celle relative à la « Culture de sécurité en entreprise ». Ainsi la question posée, 95,7% des entreprises ont apporté une réponse (**Annexe 4**) chacune témoignant que la très grande majorité a une idée ou une représentation de ce concept. Quatre grandes tendances se dessinent.

La première dans 33,7% des réponses repose sur le fait que la culture de sécurité en entreprise est avant tout un **état d'esprit** responsable, permanent, individuel et collectif (quel que soit le niveau hiérarchique des acteurs) sur la sécurité, intimement lié à la culture de l'organisation. Celui-ci est un ancrage de la sécurité dans l'entreprise avec une notion de vigilance citoyenne et professionnelle où chaque collaborateur travaille en sécurité pour lui, ses collègues et les biens de l'entreprise. Ce niveau de sensibilisation général à son environnement par les salariés et les dirigeants, englobe les aspects comportementaux, managériaux, techniques et la manière de penser sur la prise de conscience et maîtrise des risques d'un groupe de travail, de l'activité de l'organisation ainsi que celle de ses partenaires (fournisseurs, clients...). Cette veille permanente et constante, vise ainsi à anticiper les risques et une capacité à réagir dès l'identification d'une situation dangereuse. Le bénéfice pour l'entreprise de cette appropriation et imprégnation au quotidien de la notion de culture de sécurité que certains ont qualifié de « safety first » est un fondement à sa protection et pérennisation. Ainsi, la culture de sécurité est l'ensemble des **habitudes et coutumes rendues automatiques**, et fait partie intégrante à la vie de l'entreprise, sur tous les points de la sécurité.

La seconde idée (22,5% des réponses) est basée sur le fait que la « culture de sécurité en entreprise » englobe la **connaissance** des acteurs de l'organisation de toutes les **pratiques professionnelles** développées au sein de l'entreprise pour assurer et promouvoir la sécurité. Pour arriver à ces fins, des actions d'information (communication interne, affichage des consignes), de sensibilisation sur les bonnes pratiques et de formation, les procédures mises en place (Comment réagir face à un danger ou risque) et obligations (règlement intérieur, Prévention des risques professionnels) auxquelles doivent se soumettre les entreprises et leurs collaborateurs. Toutes ces règles, apprises et connues de tous, sont rappelées de façon récurrente pour que chacun garde un niveau de connaissance optimal et l'acquisition de bons réflexes.

A part égale avec le développement précédent, pour 22,5% des répondants, leur définition montre que cette notion est portée et intégrée au projet d'entreprise et est l'image de la volonté du dirigeant en matière de sécurité. La culture de sécurité en entreprise est impulsée par le chef d'entreprise dont c'est le rôle et fait que, placée comme

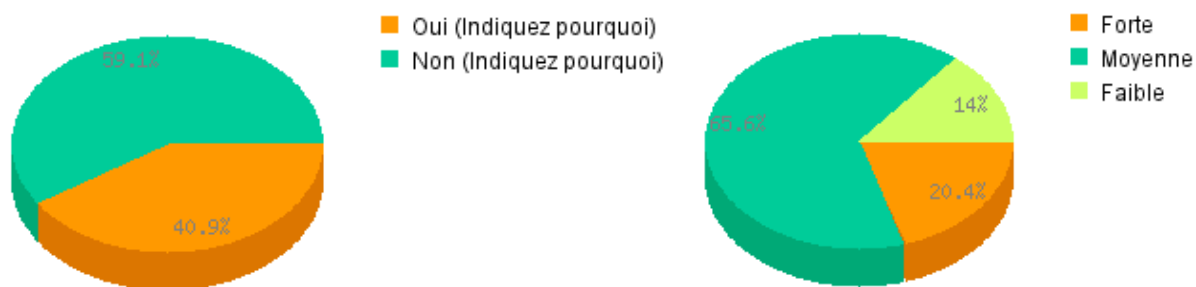
« préoccupation N°1 » et orientation stratégique, chaque salarié devient acteur de prévention pour lui-même et les autres. Intégrée dans les pratiques courantes et quotidiennes, elle vise à obtenir une vigilance et un réflexe de chaque salarié sur les différentes situations qu'ils rencontrent. Cette démarche nécessite une animation constante de la politique de sécurité de l'entreprise ; information et formation des équipes, mise à jour des documents et process sécurité, implication des personnels... et garantir la pérennité des activités de l'entreprise par la maîtrise de ses risques. Les sujets en liens avec la sécurité sont ainsi à l'ordre du jour permanent à toutes les strates de l'organisation (Management, achats, techniques, comportements...). « *La culture de sécurité c'est la **construction du projet d'établissement** qui prenne en compte tous les champs de la sécurité afin que chaque personne connaisse les risques potentiels et leur gestion. Cette culture doit être prise en compte tant au niveau des **objectifs** que de l'**organisation** ».*

Avec 10% de réponses, la culture de sécurité en entreprise se rapproche ou s'assimile à la démarche qualité. C'est l'implication des acteurs de l'organisation qui, aidés d'un cadre réglementaire ou non, participent à l'amélioration de la sécurité par la prise en compte des risques que les professionnels d'un établissement partagent et mettent en débat. Cette démarche amène la création d'un « langage commun » pour **faire de la sécurité ensemble** et **améliorer de façon constante** le niveau de sécurité globale au **sein de l'organisation**.

Enfin, le solde de réponses restant (10%) apporte que la culture de sécurité en entreprise est une « bonne-nécessité-obligatoire » pour la « gestion du risque » et la « protection des biens, des services et des hommes » pour laquelle « il y a encore du boulot ». Toutefois cette « approche obligatoire du respect individuel et collectif » fait que « l'on est passé du rien à trop de pression sur l'encadrement ».

Ainsi, la culture de sécurité d'entreprise est pour les uns, un état d'esprit des acteurs intégrant les habitudes et coutumes rendues automatiques, pour les autres la connaissance de l'ensemble des pratiques professionnelles en matière de sécurité au sein de l'entreprise ou encore l'esprit impulsé par le dirigeant à ses collaborateurs et porté par le projet d'entreprise. Enfin, la culture de sécurité est un principe d'amélioration constante de la sécurité par le chef d'entreprise et les salariés.

Sur l'ensemble des entreprises ayant répondu à l'enquête seule 41 % évalue la culture de sécurité de leurs salariés et parmi celles-ci, 2/3 la juge « moyenne ». Pour ceux réalisant cette démarche, l'évaluation est réalisée lors des CODIR, réunions de CHSCT, par la mesure du taux de participations lors de causeries, par un audit ou avec un psychologue interne à la structure. Enfin, pour les structures ne réalisant pas d'évaluation de la culture de sécurité de leurs collaborateurs, ceux-ci se justifient par le fait qu'ils n'ont pas le temps ou moyens (outils, indicateurs) pour réaliser une telle enquête, un effectif trop faible pour être pertinent ou une structure pas assez importante et une notion de « non culture » pour une telle démarche.

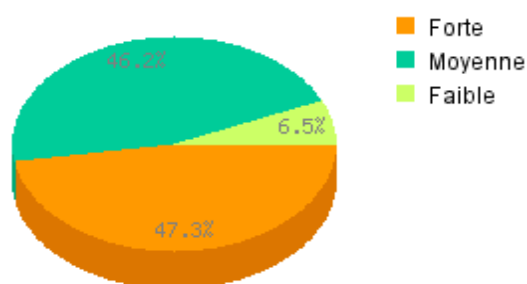


Les indicateurs utilisés pour l'évaluation de la culture de sécurité de l'entreprise (**Annexe 5**) sont soit des outils formalisés ou informels :

Outils formalisés	Evaluation informelle
Questionnaire	Visites
Nombre d'accidents du travail	Evaluation hebdomadaire
Taux de participation aux causeries	Interventions terrains des membres du CHSCT
Taux de participation aux réunions sécurité	Questionnement ciblé
Taux d'absentéisme	Proximité
Audits flash	Evaluation par responsable de secteur
Audit sécurité	Ordre du jour des réunions
Nombre de fiches anomalie	Visites sécurité
Nombre de remontée de situations dangereuses	Réactivité aux tentatives de fraude
QCM auprès des collaborateurs	Signalement des malveillances informatiques
Nombre de causeries organisées	La bonne santé de l'entreprise
Nombre de remontée de presque accidents	Constat du port des EPI
Nombres de formations sécurité réalisées	Retour sur satisfaction de la formation prévention
Nombre de personnels formés SST	Plaintes orales des salariés
Indicateurs confidentiels au groupe	
HSEPI : indicateur interne groupe	
Nombre d'actions sécurité réalisées	
Tableaux et statistiques de suivi	
Déclarations événements indésirables	
Déclaration incidents service informatique	
Déclaration intrusions	
Quizz cybersécurité	
Taux de formation des nouveaux entrants	
Nombre de consultations médecins/infirmiers ATSL	
Nombre d'arrêts de travail	
Taux de fréquence et tentative d'intrusion sur réseau informatique	
Nombre d'occurrence d'événements	

Indicateurs stratégiques, opérationnels, management	
Drills	
Exercices sur protocoles	
Nombre de pannes machine	
Nombre d'exercices gestion de crise	
Mails tests	
Taux de participation au Mur de la sécurité	
Taux d'Accidents du Travail/Maladie Professionnelle	

Enfin, les répondants déclarent à part égale que leur culture de sécurité est soit forte (47,3%) soit moyenne (46,2%) avec toutefois une perception très variée : « Faible en ce qui concerne la sécurité du système informatique, forte pour ce qui est de la protection des personnes », « (Ma culture) trop tourner sur elle-même et pas assez tourner vers une culture générale



d'amélioration continue », « C'est à rappeler sans cesse. Nous prenons des exemples réels vécus pour entretenir cette culture du "sensible" », « Pas pris beaucoup en compte dans le domaine de la formation », « Forte chez moi faible dans beaucoup de mes entreprises clientes », « Cela n'est jamais suffisant ». Les indicateurs (**Annexe 6**) mis en avant pour l'évaluation de leur culture peuvent être regroupés en 3 grandes familles :

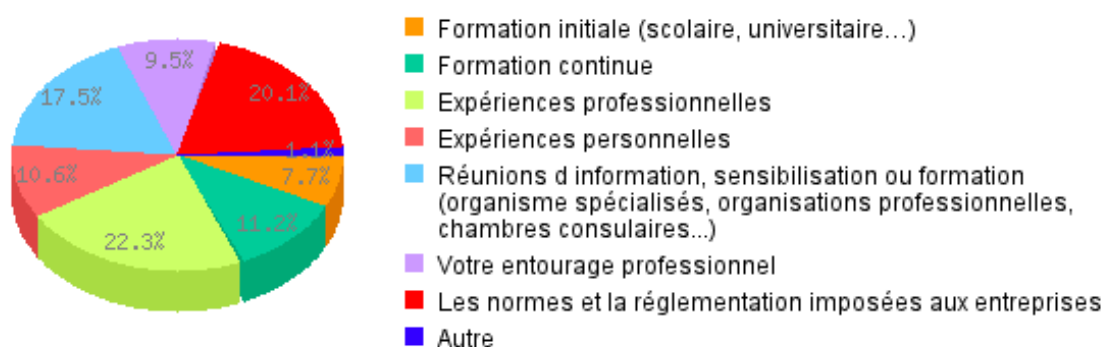
Mesures prises	Ressenti	Outils
Antivirus à jour	Actualités	Nombre d'accidents du travail
Destruction des documents confidentiels	Echanges en réunion	(Le peu) d'arrêts maladie
Fermetures des bureaux et armoires	Investissement des collaborateurs : Qualité de vie au travail	Mise en place du document unique et d'évaluation des risques professionnels
Ordinateurs avec mots de passe	Anticipation des risques possibles	Taux de fréquence, gravité
Mails d'informations aux salariés	Réflexes acquis	Remontée des incidents
Règlement intérieur	Expérience en France et étranger	Règlement intérieur
Mise en place du document unique et d'évaluation des risques professionnels	Comparaison entre obligations réglementaires et « normes » internes	Taux de sinistre

Organisation de formations annuelles	Prévention des risques au travail	Taux de litiges
A jour de la réglementation	Respect des consignes de sécurité données en formation	Taux de sinistres
Obtention de la formation SST en 2017	Prises de risque	Nombre de fiches anomalie
Communication permanente	Respect des consignes de sécurité	Nombre de remontée de situations dangereuses
Actions et planification (affichage, formations, réunions...)	Temps consacré à la sécurité et connaissances	Rapport annuel des accidents
Abonnement à des flux RSS sur la sécurité	Jugement des collaborateurs	Nombre de causeries organisées
Service QSE mis en place	Responsabilisation inter thématique	Nombre de formations externes et internes liées à la sécurité
Mise en place de SST	Expérience personnelle	HSEPI = Indicateur interne
Actions stratégiques, managériales et opérationnelles	Préoccupation constante	Tableau des objectifs annuels
Multiplication des pare-feu	Importance apportée au quotidien (dirigeant)	Nombre d'incidents critiques
Equipements adéquats	Intérêt et temps passé à lire des articles liés à la sécurité	Nombre de signalement
Cloisonnement de l'information selon niveau hiérarchique	Intuition	Taux de réponse aux quizz cybersécurité
Moyens mis en œuvre au sein de l'entreprise	Réactivité en cas de problème de sécurité	Statistiques QSE
Affichage	Penser aux conséquences d'une prise de décision	Couts opérationnels
Sauvegardes informatiques, signalement	Conscience de la plupart des risques et faire en sorte de les limiter	Taux d'absentéisme
	Démarche individuelle	Résultats des exercices
	Implication sur la mise en place des actions sécurité	Aucun accident
	Retour des collaborateurs	Aucun
	Curiosité	
	Implication personnelle	
	Comportement	
	Respect des process	
	Comparaison avec d'autres sociétés	
	Discussion avec autres responsables sécurité	

L'ensemble des verbatim est repris dans les annexes 5 et 6 pour les indicateurs exprimés.

Une évaluation de la culture ou du moins du niveau d'actions formalisées ou informelles et de leur efficacité est réalisée au sein des entreprises tant par les dirigeants vis-à-vis de leurs collaborateurs que de leur propre culture de sécurité. Le niveau exprimé de fort ou moyen de celle-ci est quasi équivalent pour les chefs d'entreprises (93,5%) que pour les collaborateurs (86%). Toutefois, force est de constater que ces notions touchent essentiellement la santé sécurité au travail (obligations de l'employeur) et la cybersécurité (récurrence des actes malveillants).

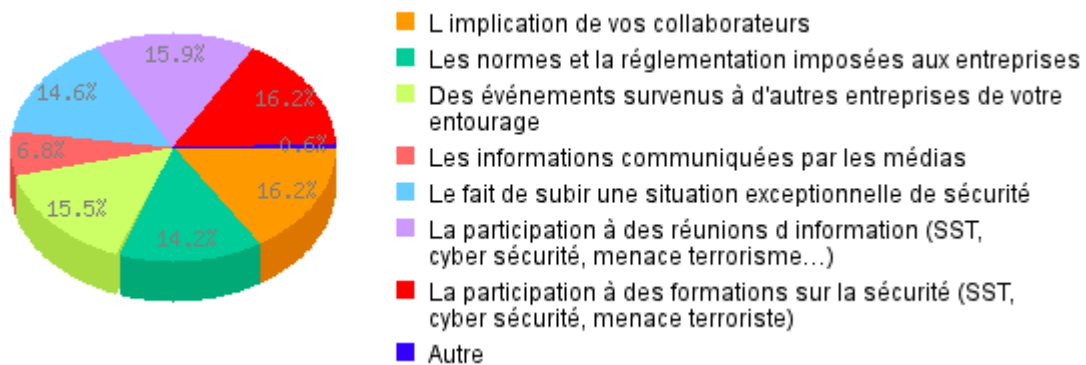
Si les répondants expriment que leur culture de sécurité est forte à moyenne, cherchons à savoir comment celle-ci s'est forgée dans leurs parcours. Ainsi, à la question « Comment votre culture de sécurité c'est elle construite ? », trois grandes tendance se démarquent regroupant à elles seules 60% des origines soit près de 2/3 de celles-ci.



Tout d'abord une origine issue de l'expérience professionnelle pour près de ¼ des cas (22,3%) dont certaine dramatique comme un début de carrière marqué par la gestion décès d'un collaborateur suite à une chute dans les escaliers, le vécu de l'explosion de l'usine AZF en 2001 ou un poste de Risk Manager, suivi des normes et de la réglementation imposées aux entreprises (20,1%) puis la participation à des réunions d'information, de sensibilisation ou formation organisées par des organismes spécialisés (exemple de collaboration avec la CPAM et la médecine du travail), organisations professionnelles ou consulaires (17,5%). Enfin, dans une autre mesure et à part égale, l'origine de cette culture de sécurité trouverait sa source dans les formations continues suivies (11,2%) puis les expériences personnelles dont le service militaire (10,6%) et l'entourage professionnel (9,5%). La formation initiale elle ne représente que 7,7% de l'origine de l'expérience acquise ce qui confirme en ce domaine la carence dans les formations initiales. Le solde restant (1,1%) a diverses origines dont une présence sur le terrain avec les membres du CHSCT et les exigences du Groupe. Un dirigeant insiste sur l'importance de la sécurité et de sa responsabilité morale « *On est responsable de chacun des hommes contribuant à l'activité et il faut être à la hauteur. On prend des engagements il faut se donner les moyens de les tenir* ».

La culture de sécurité telle que exprimée, provient de l'expérience des répondants (professionnelle, personnelle, relations de travail) pour 42,4% et de la formation (initiale, continue, actions de sensibilisation) pour 36,4% puis dans une moindre mesure des obligations auxquelles les entreprises doivent répondre.

Enfin plusieurs facteurs influencent ou influenceraient l'évolution à la hausse de la culture de sécurité. Pour cela le résultat suivant va nous aider à connaître les éléments influents :



A part égale nous retrouvons les facteurs ayant inculqué la culture initiale de sécurité tel que vue précédemment, qui nous donnent par regroupement ; « l'expérience » avec les retours sur des événements survenus à d'autres entreprises (15,5%) ou une situation exceptionnelle vécue et gérée par son organisation (14,6%) mais aussi par l'apport fait par ses collaborateurs (16,2%) soit une position à 46,3%. La participation à des formations sur le thème de la sécurité (16,2%) et à des réunions d'informations (15,9%) ainsi que de l'information véhiculée par les médias (6,8%) pour le volet « formation » avec un score de 38,9%. Finalement, les normes et réglementations imposées ne représentent que la part de 14,2% alors que la santé sécurité au travail, partie la plus réglementée dans la sécurité globale en entreprise ressort le plus significativement lors des expressions sur cette thématique par les dirigeants.

La culture de sécurité des chefs d'entreprise ne serait pas innée mais s'acquerrait comme tout apprentissage par un mélange équilibré de connaissances issues de la formation et de compétences issues de l'expérience acquise dans son écosystème professionnel et personnel.

6) Axe 2 (Approche management) : L'intégration par les TPE et PME du management d'une situation d'exception et/ou de crise

La question de recherche du présent mémoire porte sur « En quoi la culture de sécurité des chefs d'entreprises de PME contribue-t-elle à la gestion d'une situation d'exception ? ». Nous venons de voir précédemment, de part une approche anthropologique, comment la sécurité globale en entreprise est-elle perçue et qu'elles seraient les sources de l'acquisition et du développement de celle-ci par les dirigeants. Nous allons nous intéresser maintenant par le

biais des retours de l'enquête, comment les chefs d'entreprises sont-ils préparés à la gestion d'une situation d'exception, sous l'angle du management.

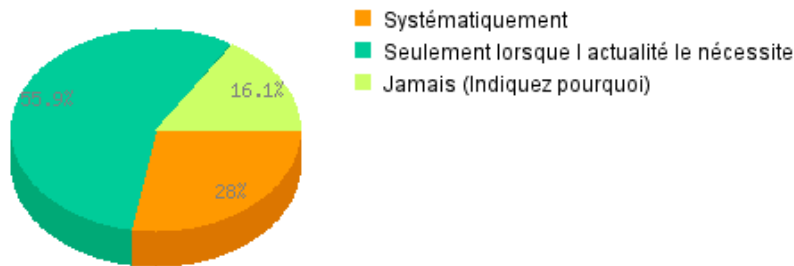
Sur l'ensemble des répondants, 42,6% des entreprises ne disposent d'aucune certification en lien avec la sécurité. Les organisations disposant de ce type de certification, soit 57,4% des répondants, l'on dans le domaine de la santé sécurité au travail (27%) et de la sécurité informatique (12,2%). Nous retrouvons ici une fois de plus les deux « parents riches » de la sécurité en entreprises. Les certifications en sûreté/malveillance (4,3%) et intelligence économique (2,6%) n'arrivent que très loin derrière montrant encore la faible prise de conscience des entreprises dans ces domaines. Enfin, 11,3% des entreprises ayant déclaré avoir une certification sécurité, disposent d'un autre modèle répondant à une norme ou une obligation tel que passage de la commission de sécurité et application des recommandations plus contrôles de l'inspection d'académie tous les 3 à 4 ans (Ets scolaire privé), norme radioprotection CEFRI E, risque infectieux, plan bleu et risque attentat. Pour un dirigeant « *Je n'ai pas les normes indiquées. Par contre étant dans le domaine, j'applique toutes les sécurités à l'échelle de ma TPE* »,



Les certifications en lien avec la sécurité commencent à être intégrées au sein des organisations. Il y a une tendance forte pour celles touchant les obligations de l'employeur en termes de santé sécurité au travail et sur la sécurité informatique. Ces domaines sont très médiatisés et font l'objet de plusieurs attaques de PME. Il y a une sensibilisation de la part des organisations professionnelles et des pouvoirs publics.

Pour les entreprises disposant d'un CODIR (COmité de DIRection) ou organe apparenté (Exemple donné : *Réunions pédagogiques*), celles-ci sont 56% à intégrer les questions de sécurité à l'ordre du jour uniquement en cas de nécessité de par l'actualité de leur organisation ; « (Nous n'avons) *Pas vraiment de CoDir formalisé mais plutôt la transmission d'information quand nous avons l'information d'un besoin particulier en vigilance* ». Plus d'un quart les inscrit systématiquement à l'ordre du jour (28%) et seulement 16% jamais dont certains jugeant comme n'étant pas « *un sujet majeur* ». Ces éléments font remonter que dans les ¼ des réunions de CODIR, la sécurité est un sujet qui est traité et traduit une certaine appétence pour ce domaine. Cependant, nous voyons qu'il faut au moins un événement de sécurité pour que cette question soit inscrite à l'ordre du jour comme en témoigne ce dirigeant « *C'est intégré chaque fois qu'on fait un investissement et à chaque*

incident de parcours ». La démarche reste d'occasion plus que d'anticipation avec des démarches volontaires « *De plus en plus, d'action en se sens vont être menées* ».



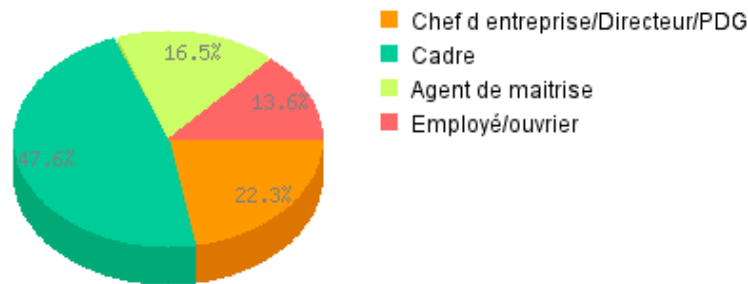
Le top management n'occulte pas les questions de sécurité, n'hésitant pas à mettre celles-ci en discussion en Comité de Direction chaque fois que nécessaire.

Les entreprises disposent pour 86,3% d'entre elles d'une personne dédiée à la sécurité (Responsable HSE ou QHSE, conseillère prévention, psychologue, membre du CHSCT, responsable ISO dans les exemples cités) et ce, majoritairement dans le domaine de la santé sécurité au travail - SST (35,6%) et la sécurité informatique - SI (20,5%). Nous retrouvons une fois de plus le duo, de tête de liste sur les aspects sécuritaires en entreprise. Arrive sur des valeurs proches, la malveillance/sureté avec 11% des répondants et la disposition d'un personnel polyvalent dans cette activité, caractéristique des fonctions support dans les TPE/PME ou sur des postes de cadres « *La sécurité fait partie intégrante des missions des cadres* » ou du dirigeant. Les 6,2% d'entreprises disposant d'une personne dédiée à la sécurité sur d'autres tâches que la SST, SI, sureté/malveillance ou intelligence économique, est orientée sur des secteurs tel la sécurité incendie, juridique ou infectieuse. Enfin, les structures ne disposant pas d'un tel profil, expliquent cette carence par une taille trop petite (activité, effectif, budget), n'en voient pas la nécessité ou n'ont pas d'obligations et pour certaines externalisent cette tâche (Ex. informatique, agent de sécurité, société de services aux entreprises, sécurité passive).

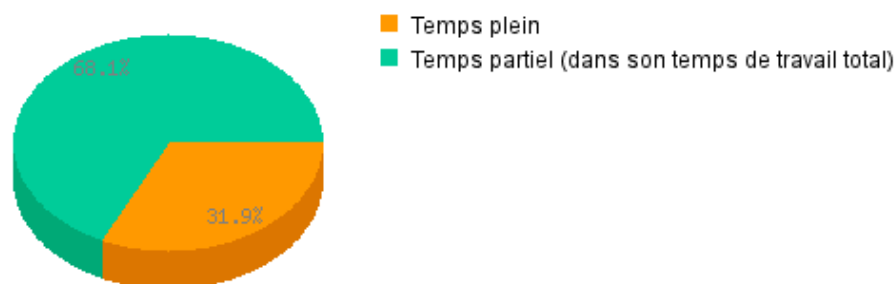


Pour les structures disposant d'une personne dédiée à la sécurité, cette fonction est majoritairement confiée à des personnes ayant un statut de cadres (70%) dont cadres dirigeant dans 22,3% des profils. Toutefois, presque 1/3 des personnes en charge des questions de sécurité ont un profil agent de maîtrise (16,5%) ou employé/ouvrier (13,6%). Les questions de sécurité sont considérées comme majeur dès que confiées à des acteurs de

l'entreprise. Toutefois, avec 1/3 des profils non cadres, il y a encore des marges de progression pour les organisations sur la place de la sécurité en leur sein.



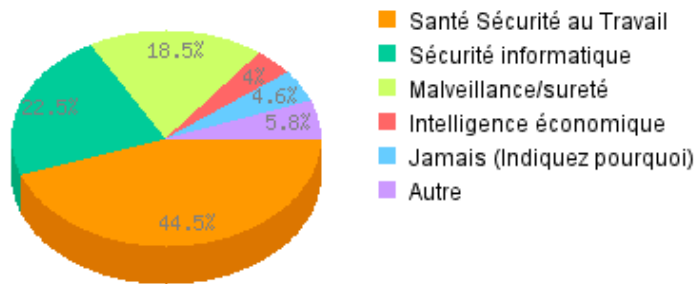
Enfin, près de 70% des personnes dédiées à la sécurité au sein de l'organisation, exercent cette tâche en temps partiel sur leur temps de travail global avec des valeurs allant de 1 à 50%. Pour des organisations « Cette responsabilité est exercée par plusieurs personnes chacune dans son domaine » ou intégré à la fiche de poste générale « La personne est chargée de la mise en œuvre du plan de formation et de la politique prévention- sécurité ».



Une majorité de TPE/PME disposent d'une personne dédiée à la sécurité, principalement axée dans la santé sécurité au travail et la sécurité informatique, ayant un profil de cadre et exerçant cette fonction à temps partiel dans un temps de travail total.

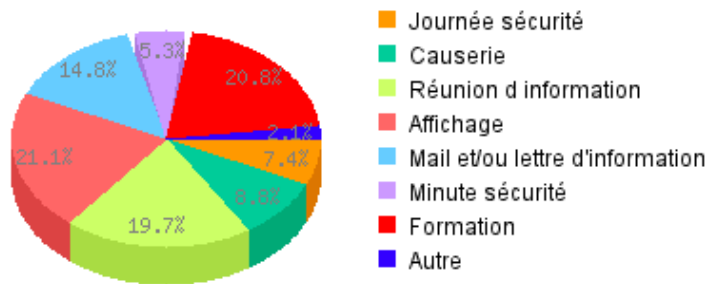
Dans les actions mises en place par les entreprises en termes de sensibilisation, information ou formation dans le champ de la sécurité globale, nous retrouvons encore le duo gagnant, santé sécurité au travail pour 44,5% des cas et sécurité informatique (22,5%) ou par exemples « Tous les nouveaux entrants sont formés à la sécurité en entreprise et règles de sécurité physiques et informatiques » et « J'applique pour ma petite entreprise des règles de sécurité informatique et veille à la prévention des risques (routier, plain-pied) ». Les réseaux Ces leaders sont suivis par le domaine de la sûreté et malveillance (18,5%) faisant lien avec l'actualité. Les actions mises en place en intelligence économiques (4%) ou autres (5,8%) restent à la marge. Les réseaux sont sollicités « Rencontre dans des réseaux professionnels avec différents acteurs : Services de Santé Au Travail, Entreprises du numérique, Services de l'Etat... » ainsi que la mobilisation d'experts externes et forces internes avec des « Journées de formation avec la Croix Rouge », « Formation systématique en interne de chaque nouveau salarié + une semaine annuelle de la prévention avec des ateliers organisés avec des

partenaires » ou en sollicitant « *FONDATION MAIF USAGER ROUTE, ANPAA ADDICTION, HOPITAL IST* ». Enfin, une organisation spécifique peut être mise en œuvre « *L'information est descendante. Les cadres y réfléchissent se mettent en conformité avec les normes ou les exigences législatives et font appliquer les consignes de sécurités* ». Seulement 5,8% des entreprises n'ont aucun dispositif. Les raisons avancées vont de la société très récente qui n'a pas pris le temps de s'en occuper, les entreprises qui n'en voient pas le besoin, le temps nécessaire pour mettre des actions en place à la vision comme n'étant pas un sujet majeur ou sont intégré « *Au fil de l'eau car notre activité de conseil et une activité "sensible"* ».



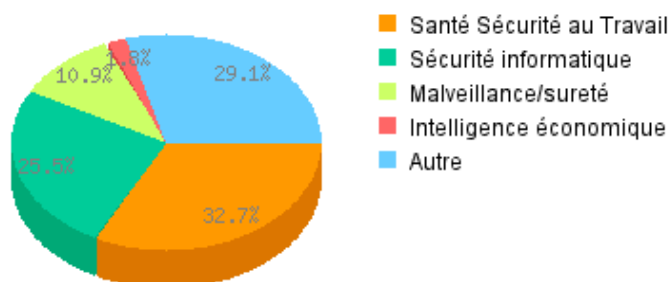
Les actions mises en place sont très polymorphes mêmes si 3 types se distinguent à part égales : l'affichage (21,1% des réponses), simple et visible de tous de façon permanente est un bon moyen pour informer et de rappeler les règles et consignes de sécurité globale. Son inconvénient est dans le fait qu'à force de voir les affiches, on ne les voit plus... Les formations (20,8%) telles que *travail en hauteur, montage échafaudage, sauveteur secouriste du travail, gestion des situations difficiles, manipulation des extincteurs, port des EPI, risque routier*, qui sont financées par le fond formation auquel cotise les entreprises. Celles-ci sont efficaces si une formation continue régulière permet de maintenir et actualiser les connaissances. Toutefois celles-ci touchent essentiellement dans les réponses exprimées, le champ de la santé sécurité au travail. Les réunions d'information (19,7%) et causeries (8,8%) dans lesquelles nous retrouvons des techniques d'animation comme le « *Quart d'heure de prévention* » ou réalisées « *dès que nous identifions un risque significatif il est abordé et traité* ». Simples et efficaces, ces actions facilitent les échanges et les partages de pratiques et touchent directement les cibles sur une courte durée donnant une certaine efficacité d'impact. Les journées sécurité (7,4%) représentent encore un faible pourcentage des actions menées, mais sont en pleine expansion dans les entreprises car simples à organiser et de faible coût, elles permettent de sensibiliser un grand nombre d'acteurs des organisations sur un laps de temps court mais à efficacité percutante.

Enfin la transmission par mail news letter reste à un bon niveau de vecteur d'informations ou permet de diffuser des quizz (maintien des connaissances) ou enquête sécurité (amélioration continue).

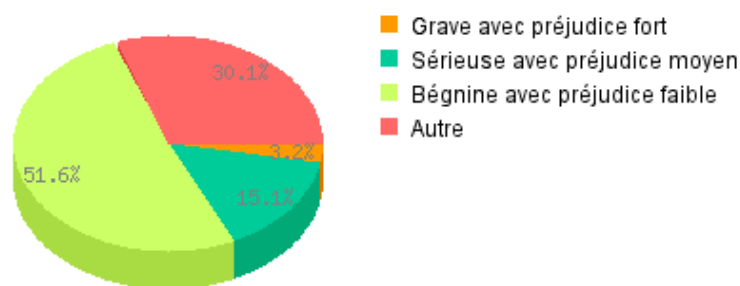


Les entreprises investissent dans la mise en place d'actions de sensibilisation (minute et journée sécurité – 7,4%), d'information (réunions, causeries, affichage, mail et news letter – 64,4%) et de formation (20,8%). Celles-ci restent principalement ciblées sur la santé sécurité au travail de par les obligations incombant au dirigeant et à la cybersécurité en raison des menaces et dommages subis par les TPE/PME dans le champ de la sécurité informatique. Encore peu sensibles sur les autres domaines de la sécurité (intelligence économique et sureté/malveillance), les actions restent timides.

Toutes les organisations ayant répondu à l'enquête déclarent avoir été confrontée au moins à une situation exceptionnelle de sécurité au cours des 3 dernières années. Pour près d'un tiers des cas (32,7%), cette situation est du domaine de la santé sécurité au travail avec des cas de feu électrique, explosion, évacuation de bâtiment suite à fuite de gaz d'une canalisation percée lors de travaux, accident du travail, risque infectieux et un cas d'harcèlement sexuel sur étudiant. Les problématiques de sécurité informatique représentent 25,5% des réponses avec attaques de virus, piratage de serveur, crypto virus en 2 ans. D'autres champs sortant des propositions du questionnaire dans 29,1% des cas intéressent par exemple un cas de maltraitance sur usager. La sureté ou malveillance avec des exemples d'agressions verbales et menaces, de dégradation de ligne téléphonique et internet, vol de carburant, des violences de la part d'utilisateurs ou arnaque aux annuaires (10,9%). L'intelligence économique ne représente que 1,8% des cas et aucun n'exemple n'a été donnée.

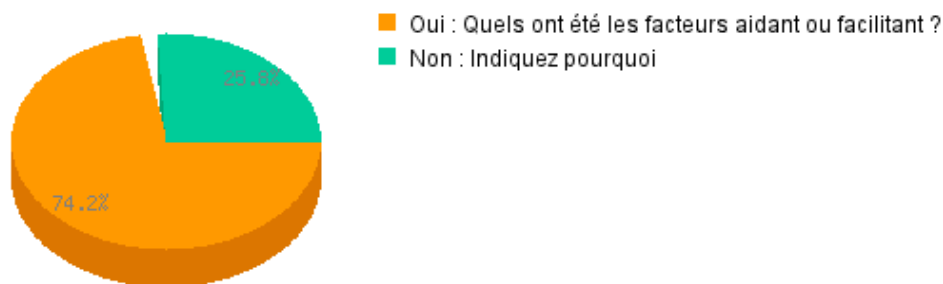


Toutes ces situations exceptionnelles survenues aux entreprises ont occasionné des préjudices très variés tant sur le plan humain, financier qu'organisationnel. Ainsi dans plus de la moitié des cas, l'incidence fut bénigne avec un faible préjudice notamment financier. Dans les cas cités, ce sont plus les infrastructures qui ont été touchées ; « *On s'en est finalement bien sorti, notre serveur avait été infecté et touchait au fur et à mesure nos documents de travail* » et « *Grosse paralysie informatique pendant 2 jours mais aucune perte de données* ». Les situations sérieuses avec préjudices moyens représentent 15,1% des situations et sont aussi très diverses pour les TPE/PME avec un impact financier ou d'organisation comme ce cas où l'entreprise a dû réaliser une « *formation obligation qui impacte le budget* » ou un préjudice humain et financier comme le rapporte cette réponse « *2 accidents de travail et perte financière* ». Enfin les situations graves avec fort préjudices restent des cas très rare avec 3,2% des situations notamment en lien avec la géographie des répondants et les structures qui furent touchées directement par *l'explosion de l'usine AZF* en 2001. Les « autres cas, bien que représentant 30,1% des réponses ne sont pas détaillés et donc non exploitables ici. Un seul témoignage relate le fait d'avoir dû « *Gérer avec les usagers, les familles et les autorités de contrôle* » sur un cas de maltraitance d'utilisateurs.



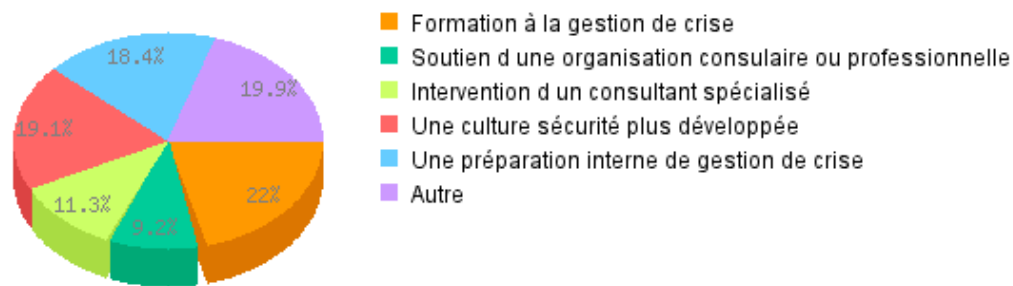
Dans $\frac{3}{4}$ des cas les ressources internes des organisations (74,2%), avec du personnel qualifié et/ou d'expérience, ont permis de faire face au(x) situation(s) exceptionnelle(s) rencontrée(s) : « *Compétences des professionnels en interne et associatifs- Plan d'action rapidement mis en œuvre et suivi* » et « *Des personnels disponibles et réactifs pour intervention et prise en compte* ». L'anticipation et la préparation à ces événements a été un atout majeur et plusieurs organisations en témoignent : « *La préparation par des procédures de gestion de situation dégradée* », « *Le respect de la stratégie mise en place pour gérer le problème (Ex. consignes d'évacuation)* », « *Anticipation sauvegarde informatique* », « *Procédure maltraitance, échanges avec la cellule nationale de l'APF sur la maltraitance* » ont contribué à la bonne gestion des situations. Les instances représentatives du personnel contribuent à la gestion de telles situations « *Travail en partenariat avec le CHSCT* » ainsi que des organisations professionnelles comme la « *Fédération du BTP* ». La possession de matériels spécifiques est aussi un atout « *la présence d'un défibrillateur dans l'entreprise qui a permis de sauver une personne d'un arrêt cardiaque* » avec la formation adéquate des professionnelles « *Mes personnels sont formés au SST* » et « *Plus de 10% de mes salariés sont formés au SST* ». Les structures n'ayant pas ce type de force confient la gestion de ces situations à des prestataires externes (25,8%) qui pour certains ont eu un rôle curatif et

formatif « *On a fait intervenir des spécialistes qui nous ont appris et formé puis on a ajusté les processus en conséquence* » ou uniquement curatif « *Aide par la médecine du travail et par un fournisseur informatique avec qui nous avons un contrat de maintenance* » ou encore « *Nous avons fait intervenir la SSII qui s'est rendue rapidement disponible et a restauré les données* ». Certaines organisations cumulent l'emploi de ressources internes et externes comme cette PME « *De bonnes connaissances informatique d'une personne en interne et la rapidité de réaction de la société d'infogérance* ». Pour des structures, des analyses d'accidents sont rapportés, aidant pour éviter ou anticiper des cas similaires « *L'analyse d'accident a été réalisée avec les services et les élus* » ou pour une autre entreprise « *Pouvoir évoquer les situations sans tabou ni affectivité pour analyser au mieux* ». Enfin, l'organisation elle-même peut être une structure naturellement résiliente « *Taux d'encadrement permettant une réactivité, petite équipe de professionnels, flexibilité et adaptation possible face à l'actualité* » et une « *Forte culture de la sécurité* ».



Enfin, lorsque les organisations sont interrogées sur ce qui pourrait être aidant ou facilitant pour améliorer la ou les situations exceptionnelles vécues, trois grandes tendances se dessinent. La première et majoritaire qui serait une priorité pour les entreprises, est d'augmenter les capacités internes à faire face à ce type de situation avec 59,5% des réponses. Ainsi, des actions de formation à la gestion de crise (22%) avec témoignage complétant les données statistiques « *les formations sur site avec un formateur spécialisé facilitent la gestion de crise ou nous permet de les anticiper...* », ainsi qu'une préparation interne à la gestion d'une telle situation (18,4%) et d'avoir une culture de sécurité plus développée (19,1%) sont les actions que les organisations privilégieraient. La seconde tendance est de faire appel à une ou des forces externes à l'entreprise pour 20,5% des répondants en mobilisant les organisations professionnelles (9,2%) notamment en amont de la situation exceptionnelle en ayant de la part de ces structures « *Plus d'informations sur les sujets* » et/ou d'un consultant spécialisé (11,3%) « *Si besoin spécifique, nous faisons intervenir un expert, interne groupe ou externe* » ou d'un « *Partenaire externe* ».

Enfin pour 19,9% des répondants, ceux-ci ne jugent pas utile d'avoir une meilleure préparation ou ne se sentent pas concernés.



Toutes les entreprises ont été confrontées à une situation exceptionnelle, principalement dans le domaine de la santé sécurité au travail et de la sécurité informatique. Même si pour la moitié des structures les conséquences furent bénignes et sans gravité, 18% ont été impactées de façon sérieuse à grave avec un préjudice moyen à fort. De par la fragilité des PME, ces événements auraient pu être déléteurs pour ces organisations. Dans les $\frac{3}{4}$ des cas les situations ont pu être gérées par des ressources internes faisant appel à une aide extérieure essentiellement dans le domaine de la cybersécurité. Toutefois près de deux tiers expriment le besoin de faire monter en compétence leurs ressources internes pour une meilleure aptitude à gérer des événements exceptionnels en leur sein.

Synthèse :

La culture des chefs d'entreprises n'est pas innée et se développe au fur et à mesure de leurs expériences et « sensibilisations ». Malgré quelques initiatives personnelles, l'absence de modules sur la sécurité globale dans les cursus de formation initiale des futurs dirigeants ne joue pas en la faveur de l'émergence d'une culture de sécurité. Les organisations professionnelles, syndicales et consulaires, jouent un rôle prépondérant pour palier à cette carence. Toutefois les thèmes abordés restent ciblés majoritairement sur les obligations légales en termes de santé sécurité au travail et d'occurrence des problèmes de sécurité informatique. Pris par la gestion courante de leurs structures, d'autres domaines tels l'intelligence économique ou le terrorisme, les chefs d'entreprises ne sont en demande que suite à un dommage subit au sein de leurs organisations. En cas de situation exceptionnelle, la plupart des organisations professionnelles ou consulaires savent apporter un soutien aux entreprises sous différentes formes : conseil, mobilisation de personnes ressource... Toutefois, sensibilisés aux problématiques de sécurité, les entreprises travaillent sur le développement de moyens permettant de prendre en compte cette dimension dans leurs organisations. L'approche pour renforcer la sécurité au quotidien afin de mieux appréhender l'exceptionnel consisterait à un changement de paradigme en amenant cette « matière » dans le cursus de de formation initiale et d'installation avec un soutien des branches, des organismes et par la mobilisation des acteurs de la sécurité et de la sureté. L'approche passant comme un levier de développement à part entière pour l'entreprise.

Conclusion

Les petites et moyennes entreprises représentent la première force économique en France. Toutefois leur structuration fait de ces organisations des entités vulnérables où un événement majeur peut rapidement mettre en faillite la pérennité de leur activité. Effet paradoxal, leur organisation les rends plus flexibles à faire face et à s'adapter au changement.

Les dirigeants de PME, plus dans un costume d'homme-orchestre que de chef d'orchestre, ont du mal à prendre le recul nécessaire et d'avoir une vision globale sur le fonctionnement de leurs structures. Accaparés par la résolution des problèmes du quotidien et à assurer la pérennité de leurs établissements face à une concurrence de plus en plus agressive et mondialisée, leur projet d'entreprise est plus une navigation à vue qu'au cap.

La priorité est donnée aux domaines névralgiques que sont la production, le marketing et la commercialisation. La partie ressources humaines et gestion arrivant en suivant. Parent pauvre des organisations, la sécurité dans l'entreprise, dont le retour sur investissement n'a pas la même visibilité que le lancement d'un nouveau produit ou d'une nouvelle machine, est dépendant des obligations réglementaires et de l'occurrence de survenue d'un danger. La santé et sécurité au travail et la cybersécurité bénéficient ainsi d'une certaine attention.

Les chefs d'entreprises se doivent pourtant d'être de plus en plus sensibles à la sécurité globale de leurs organisations de par l'écosystème dans lequel ils évoluent ; réglementation de plus en plus renforcée, ouverture vers l'international, nouvelles menaces, démocratisation du piratage informatique... Au-delà des accidents du travail, maladies professionnelles et demandent de rançons pour décrypter les données informatiques piratées, les entreprises sont sous la menaces du risque attentat et du vol de leurs données sensibles (fichier clients, secret de fabrication...). Autant de danger pour l'entreprise dont la prise en compte des dommages possible n'intervient qu'une fois « l'accident » arrivé.

Aussi les chefs d'entreprises doivent entrer la sécurité globale dans leur quotidien et la mettre au service du développement de leurs organisations. Il leur sera ainsi plus aisé d'utiliser en premier ressort leur force interne pour manager une situation exceptionnelle. Pour cela, ils doivent être aidés par les organisations professionnelles, consulaires, les acteurs de la sécurité et de la sureté et l'intégration du concept de sécurité globale dans les cursus de formation initiale. La prise en compte des savoirs faire et savoir être de leurs collaborateurs ayant pour chaque métier de vraies compétences développées en matière de sécurité. Ainsi, cet ensemble de connaissances, expériences, observations, façons de faire quotidiennes, modes de pensées, amèneront les dirigeants de TPE et de PME à la transformation d'une sensibilité à la sécurité à une véritable culture de sécurité globale. Ils seront ainsi plus à même de prendre les mesures appropriées lors de la survenue d'une situation exceptionnelle de sécurité à l'instar de ce qu'ils font face à une situation concurrentielle, économique ou de ressource humaine majeure.

Bibliographie :

PME 2016 : Rapport annuel sur l'évolution des PME. Observatoire des PME. Editeur Bpifrance – 2016.

Différence entre grand groupe et PME. In *Primastone Consultant* (En ligne), 2017. Disponible sur <http://primastoneconsultant.net/conseils-projet-professionnel/81.html>

Shridath Ramphaml consultable sur <https://www.iisd.org/biography/shridath-ramphal>, sur *International Institute for Sustainable Development*, 3 mars 2015

Strange, Susan, *The Retreat of the State, The diffusion of Power in the World Economy*, Cambridge, Cambridge University Press, 1996

Roucaute, Yves, « Une revue scientifique pour penser la sécurité globale », *Cahier de la Sécurité*, n°14, octobre-novembre 2014, p. 7-15

Roucaute, Yves, « The ongoing European shake-up », *Cahier de la Sécurité*, n° Spécial issue, mars 2010

Roucaute, Yves, « Le bouleversement inachevé européen », *Cahiers de la Sécurité*, n°14, octobre-novembre 2010

WIKIPEDIA, « Sécurité globale (concept) », modifié le 28 septembre 2016. Disponible sur [https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_globale_\(concept\)](https://fr.wikipedia.org/wiki/S%C3%A9curit%C3%A9_globale_(concept))

La fraude était tellement sophistiquée... *Le Parisien.fr* Fait du jour, 17 novembre 2013. Disponible sur <http://www.leparisien.fr/espace-premium/actu/la-fraude-etait-tellement-sophistiquee-17-11-2013-3322519.php>

BESTRON, Christian, « Interview » in : *6 minutes pour trancher*. Radio : RTL, 17 mai 2017

HOLLANDER, Alexandre. « Ce qu'une entreprise devrait faire pour assurer la sûreté de ses employés à l'étranger » (En ligne). *Huffingtonpost*. 23 février 2016, 14 :45. Disponible sur : http://www.huffingtonpost.fr/alexandre-hollander/surete-expatries-entreprise_b_9297454.html

COHADON, Jean. « Sur un chantier, un maçon se tue en tombant de 12 mètres ». *Ladepeche.fr* (en ligne) le 06 septembre 2017. Disponible sur <http://www.ladepeche.fr/article/2017/07/06/2607854-chute-mortelle-d-un-ouvrier-a-toulouse.html>

TRALET, Claude. « La sécurité globale contribue à la croissance ». In : *Lesechos.fr* (En ligne) le 12 mai 2017. Disponible sur <https://www.lesechos.fr/idees-debats/cercle/cercle-169927-la-securite-globale-contribue-a-la-croissance-2086457.php>

OCQUETEAU, Frédéric. « Chefs d'orchestre de la sûreté des entreprises à l'ère de la sécurité globale » 2001.

BEZIERS la FOSSE, Arnaud, FAGE, Sébastien, DARDON, Hubert. « Sécurité des entreprises : Construire une véritable stratégie ». LinkedIn le 23 mars 2017.

IBACH, Chrystelle. « Attaque et demande de rançon en ligne : comment y faire face ». *Cadre et Dirigeant magazine* (En ligne). 20 mars 2017.

DE COATPONT, Tanguy. « Attaque et demande de rançon en ligne : comment y faire face ». *EconomieMatin* (En ligne). 02 novembre 2014. Disponible sur <http://www.economiamatin.fr/news-attaque-informatique-piratage-pme-tpme-differnece-protection-strategie>

« Cybersécurité : 5 chiffres-clés à connaître ». *Microsoft Ideas* (En ligne). 30 août 2016. Disponible sur <http://www.economiamatin.fr/news-attaque-informatique-piratage-pme-tpme-differnece-protection-strategie>

MEDDAH, Hassan. « Les usines sont vulnérables aux cyberattaques ». L'Usine Nouvelle (En ligne). 22 octobre 2016. Disponible sur <http://www.usinenouvelle.com/article/tribune-les-usines-sont-vulnerables-aux-cyberattaques.N453387>

Etude Cabinet Deloitte, 2017 « Les grandes tendances 2017 de l'industrie et défense ».

MEDDAH, Hassan. « La cybersécurité, nouveau talon d'Achille du secteur aéronautique ? ». L'Usine Nouvelle (En ligne). 13 mars 2017. Disponible sur <http://www.usinenouvelle.com/article/la-cybersecurite-nouveau-talon-d-achille-du-secteur-aeronautique.N513924>

MEMHELD, Pierre. « Faut-il plus de cybersécurité, de cyberdéfense ou de cyberrenseignement ? » The Conversation 5 (En ligne). 09 mars 2017. Disponible sur <http://theconversation.com/faut-il-plus-de-cybersecurite-de-cyberdefense-ou-de-cyber-renseignement-73215>

BOLLET, Laurent. « Maitriser la sécurité des entreprises ». Bienpublic.com (En ligne). 05 décembre 2016. Disponible sur <https://portail-ie.fr/short/1350/la-d2ie-appelee-a-disparaitre>

LARIVET, Sophie. *Intelligence économique : Enquête dans 100 PME*. Le Harmattan, 2009, 260p.

Les PME se mettent à l'intelligence économique. L'Entreprise.com (En ligne). Publié le 23 mai 2014 et mis à jour le 19 janvier 2015. Disponible sur http://lentreprise.lexpress.fr/gestion-fiscalite/responsabilites-assurances/les-pme-se-mettent-a-l-intelligence-economique_1545939.html

La Délégation Interministérielle à l'intelligence économique a son site internet. Club des Directeurs de Sécurité et de Sûreté des Entreprises (En ligne). 15 avril 2013. Disponible sur : <https://www.cdse.fr/la-delegation-interministeriel-a-l>

La D2IE appelée à disparaître. Portail de l'IE (En ligne). 28 janvier 2016. Disponible sur <https://portail-ie.fr/short/1350/la-d2ie-appelee-a-disparaitre>

RIMONDI, Laurent. « Intelligence économique, un outil de compétitivité pour les PME ». Le Nouvel Economiste.fr (En ligne). 15 avril 2015. Disponible sur <https://www.lenouveleconomiste.fr/lesdossiers/intelligence-economique-un-outil-de-competitivite-pour-les-pme-26792/>

Intelligence économique : les PME (...) sont concernés. Entreprendre.fr (En ligne). 05 janvier 2015. Disponible sur <http://www.entreprendre.fr/intelligence-economique-des-pme-aux-grands-groupes>

Exemples concrets d'intelligence économique ». acrie.unblog.fr (En ligne). Date inconnue. Disponible sur <http://acrie.unblog.fr/performance-rentabilite-pragmatisme/demarche-de-veille-cellule-de-veille-veille-strategique/>

Enquête sur les pratiques de Veille & d'Intelligence Economique des entreprises bretonnes, 8^{ème} édition. Octobre 2015, CCI de Bretagne.

Zoom sur l'intelligence économique, 4^{ème} édition. Janvier 2015. CCI de la Drôme.

Pratiques et usages du numérique dans les PME et TPE, septembre 2015, CCI de Lyon.

MATHIE, Jérôme. « L'intelligence économique fait son apparition dans les normes ISO 9001 et 14001 ». LinkedIn. 26 octobre 2016.

LOUSSAIF, Catherine. « Risques géopolitiques : Quels enjeux systémiques pour les entreprises ? ». Actualité & Analyse et Tech & Entrepreneuriat. 06 mai 2017.

HOLLANDER, Alexandre. « Ce qu'une entreprise devrait faire pour assurer la sûreté de ses employés à l'étranger ». Huffingtonpost (En ligne). 23 février 2016. Disponible sur http://www.huffingtonpost.fr/alexandre-hollander/surete-expatries-entreprise_b_9297454.html

MEDDAH, Assan. « Sécurité des collaborateurs à l'étranger, les entreprises font encore l'autruche ». L'Usine Nouvelle (En ligne). 11 février 2016. Disponible sur <http://www.usinenouvelle.com/article/securite-des-collaborateurs-a-l-etranger-les-entreprises-font-encore-l-autruche.N378533>

Chronologie des actes terroristes en France, modifié le 12 juillet 2017. Disponible sur https://fr.wikipedia.org/wiki/Chronologie_des_actes_terroristes_en_France#Ann.C3.A9e_2015

BEZIERS la FOSSE, Arnaud, FAGE, Sébastien, DARBON, Hubert. « Sécurité des entreprises : Construire une véritable stratégie ». LinkedIn le 23 mars 2017.

Opinionway, *Le baromètre de la sécurité des collaborateurs à l'international* (En ligne). Vague 2b, Décembre 2015. https://www.cdse.fr/IMG/pdf/deuxieme_barometre_cdse_de_la_securite_des_collaborateurs_a_l_international.pdf

LEFEVRE, Richard. « Passer du management de la sûreté sous l'uniforme, à celui de la sûreté de l'entreprise expatriée : « The right man in the right place ». Carrière & Leadership. 17 janvier 2017.

HORNUS, David. « Sécurité des collaborateurs à l'international : les entreprises françaises mal placées ». Experts de l'entreprise (En ligne). 31 mai 2016. Disponible sur <http://www.expertsdelentreprise.com/Securite-des-collaborateurs-a-l-international-les-entreprises-francaises-mal>

LEBOIS, Laurent. « Les dirigeants de PME-PME face au risque terroriste en France ». Journal de l'Economie.fr (En ligne). 04 avril 2017. Disponible sur http://www.journaldeconomie.fr/Les-dirigeants-de-PME-PMI-face-au-risque-terroriste-en-France_a4595.html

INRS. « Introduction à la prévention ». Site web de l'INRS. Disponible sur <http://www.inrs.fr/demarche/principes-generaux/introduction.html>

Evolution des principales obligations réglementaires dans le domaine de la santé au travail. Malakoff Mederic (En ligne). Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/evolution-des-principales-obligations-reglementaires>

Service-Public. « Sécurité et santé au travail : obligations de l'employeur ». Service-Public.fr (En ligne). Disponible sur <https://www.service-public.fr/particuliers/vosdroits/F2210>

SOUSTRE, Coralie. « De l'intérêt de prévenir les accidents du travail et les maladies professionnelles ». Business les Echos (En ligne). 23 mars 2017. Disponible sur <https://business.lesechos.fr/entrepreneurs/ressources-humaines/9550936-de-l-interet-de-prevenir-les-accidents-du-travail-et-les-maladies-professionnelles-307711.php>

Répondre aux obligations réglementaires en santé et sécurité. Malakoff-Médéric Entreprises (En ligne). Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires>

Mettre en place une démarche de prévention. Malakoff Médéric (En ligne). Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/mettre-en-place-une-demarche-de-prevention>

La santé sécurité dans une PME. Magasine Agir Mag N°48. Parution Septembre/Octobre 2013. Disponible sur <http://www.agir-mag.com/sante-securite-sante-securite-au-travail-pme.html>

RADISSON, Laurent. « La santé sécurité au travail de moins en moins prioritaire pour les TPE-PME ». Actu-environnement.com (En ligne). 13 mars 2015. Disponible sur <https://www.actu-environnement.com/ae/news/sante-securite-travail-sst-tpe-pme-recul-inrs-24092.php4>

Directive cadre 89/391/CEE, loi n°91-1414 du 31 décembre 1991, Décret n°2001-1016 du 05 novembre 2001 et circulaire n°6 du 18 avril 2002

Obligatoire : Réaliser le document unique. Malakoff Médéric (En ligne). Disponible sur <https://entreprise-territoire-de-sante.malakoffmederic.com/obligations-reglementaires/info/le-document-unique-une-obligation>

RICHER, Martin. « Pour un euro investi en santé sécurité au travail, le retour sur investissement est de 2 à 5 euros ». Management et RSE (En ligne). 06 juin 2016. Disponible sur <http://management-rse.com/2016/06/06/euro-investi-sante-securite-travail-retour-investissement-de-2-a-5-euros/>

DONET-MARY L. DUFES E, RATINAUD C, TORMOS G « La crise : du minimum requis au minimum commun ». Dossier ENSOSP.

LIBAERT, Thierry. Crise de 1 à 150. OIC éditions, Collection 360°. 2007. Page 6.

COMBALBERT, Laurent. Management des situations de crise. ESF Editeur. Série « Entreprise » Paris. 2005. Page 23.

DUFES et RATINAUD, « Situations de crise : une réponse modélisée en 3D » Dossier ENSOSP 2013.

MERCADAL, Laurent. « Préparer ses collaborateurs à la crise, la vraie... » LinkedIn. 31 mai 2016.

LEVINE, Jehna, VRAIE, Benoit. « Gestion de Crise et continuité d'activité : la survie de l'activité entreprise suite à la survenue d'un incident ». Portail de l'Intelligence Economique - Jeudis du Risque (En ligne). 23 février

GRAINES-ROSS, Leslie. « *What CEOs Should Know About Speaking Up on Political Issues* ». Harvard Business Review (En ligne). 2017. Disponible sur <https://hbr.org/2017/02/what-ceos-should-know-about-speaking-up-on-political-issues>

Etude de Weber Shandwick et KRC Research « *The Compagny behind the Brand II : In Goodness We trust* » 2017. Disponible sur <http://www.webershandwick.com/uploads/news/files/company-behind-the-brand-in-goodness-we-trust.pdf>

NORMANDIN, François. « Communication de crise : quand le silence tue... ». Revue gestion.ca (En ligne). 20 février 2017. Disponible sur <http://www.revuegestion.ca/agir/communication-de-crise-silence-tue/>

DONET-MARY L. DUFES E, RATINAUD C, TORMOS G « La crise : du minimum requis au minimum commun ». Dossier de l'ENSOSP.

MH. Côté, *Une approche anthropologique*. Revue A Babord N°12 de déc.2005/janv.2006 « Dossiers les non lieux de la culture ». Disponible sur <https://www.ababord.org/Une-approche-anthropologique>

WIKIPEDIA, « *Edward Burnett Tylor* », modifié le 09 septembre 2017 à 13:32. Disponible sur https://fr.wikipedia.org/wiki/Edward_Tylor

S.A. Sackman, *Cultural knowledge in organization*. Sage, 1991.

L. Smircich, *Concepts of Culture and Organizational Analysis*. Administrative Science Quarterly n°28, 1983.

Frost et al. *Reframing corporate culture*. Sage, 1991.

Godelier. E, *La Culture d'entreprise, Source de pérennité ou source d'inertie ?* Revue Française de Gestion 2009/02, n°192, pages 95-111.

Moran. ET et Kwein JF, *The Cultural approach to the formation of organizational climate*. Human Relations Vol. 45, n°1, 1992, pages 19-47.

- C. Durand, JF. Fili, A. Henault, *Culture d'entreprise*. Culture d'entreprise free (en ligne), 2014. Disponible sur <http://culture.entreprise.free.fr/>
- C. Henriët, *Culture d'entreprise et motivation des salariés*. Mémoire de fin d'étude, 2007. Disponible sur http://www.uprt.fr/mesimages/fichiers-uprt/so-social/so-management/so-henriet_c.pdf
- Laurent A, *The cultural diversity of western conceptions of management*. International Studies of Management and Organization. Vol. 13, n°1-2 printemps/été 1983, p. 75-96
- Gordon, GG, Industry determinants of organizational culture. Academy of Management Review, 1991. Vol. 16, n°2, p. 396-415.
- J. Elliot, *The Changing culture of a factory*. Tavistock, 1952.
- T.J. Peters, R.H. Waterman, *Le Prix de l'excellence*, InterEditions, 1983 (rééd. Dunod, 1999), W.G. Ouchi, *Théorie Z*, InterEditions, 1982 (rééd. 1989)
- La culture d'entreprise, facteur de compétitivité ? Les Echos (en ligne), le 27 septembre 2012. Consultable sur http://archives.lesechos.fr/archives/cercle/2012/09/27/cercle_55079.htm
- Denison DR. Corporate culture and organizational effectiveness New York. Wiley, 1990.
- I. Francfort, F. Osty, R. Sainsaulieu et M. Uhalde *Les mondes sociaux de l'entreprise*, Desclée de Brouwer, 1995.
- N. Journet, *La culture, de l'universel au particulier*. Editions Presses Universitaires de France, 2002. Page 291.
- C. Handy, *L'Olympe des managers*, éditions d'Organisations, 1986. D. Graves, *Corporate Culture*, St Martin's Press, 1986.
- G. Morgan, *Images of organization*, Beverly Hills, CA, USA, Sage, 1986.
- P. d'Iribarne, *La Logique de l'honneur*, Editions du Seuil, réédition 1998.
- M. Maurice, F. Sellier et J.J. Sylvestre, *Politique d'éducation et organisation industrielle en France et en Allemagne*. Editions Puf, 1982.
- G. Ribeill, *Les Cheminots*. La découverte, 1984.
- M.Liu, *Approche sociotechnique des organisations*. Editions d'Organisations, 1982.
- M. Tripier, Culture ouvrière et culture d'entreprise. Sociologie du travail N°3, 1986.
- R. Sainsaulieu, D. Segrestin, Vers une théorie sociologique de l'entreprise. Sociologie du travail N°3, 1986.
- R. Marnette, *Qu'est-ce qu'une culture d'entreprise ?* Neocamino (en ligne). Publié le 02/12/2013. Consultable en ligne sur <http://blog.neocamino.com/quest-ce-quune-culture-dentreprise/>.
- C. Durand, JF. Fili, A. Henault, *Culture d'entreprise*. Culture d'entreprise free (en ligne), 2014. Disponible sur <http://culture.entreprise.free.fr/>
- Thevenet, M. *Culture d'entreprise : une définition*. CAIRN.INFO, 14/09/2017 p.32-54.
FRESSOZ JB, *L'apocalypse joyeuse : Une histoire du risque technologique*. Seuil, 2012
- Commission des Communautés Européennes, *Promouvoir un cadre européen pour la responsabilité sociale des entreprises*. Livre Vert, 18/07/2001, p. 7.
- MOTET Gilles, *Risque acceptable : un permis de tuer ?* Tribunes de la sécurité industrielle, 2013, n°2, p.2

Chevreau F.R et Wybo J.L, *Approche pratique de la culture de sécurité*. CAIRN.INFO 171-189 (En ligne)

TAZI, Dounia, *Avoir des ambitions de culture de sécurité cohérentes avec le contexte de son activité*. Conviction n°18, février 2016.

GILBERT, Claude, *La sécurité : une affaire de professionnels ?* Tribunes de la sécurité industrielle, 2015, n°6

DANIELLOU F, SIMARD M, BOISSIERES L, *Les facteurs humains et organisationnels de la sécurité industrielle : un état de l'art*. Les cahiers de la sécurité Industrielle, Février 2010.

BAREIL C, *Modèle diagnostique des phases de préoccupations : une approche utile dans la gestion des changements*. 1999, Ecole des Hautes Etudes Commerciales.

BRUNEL, C, *Promouvoir les comportements proactifs en sécurité est incontournable pour développer la culture de sécurité*. Nos Convictions, 2014, ICSI, Toulouse.

CRESSY Jean-Paul, *Dialogue social : Incontournable pour la culture de sécurité*. Tribunes de la sécurité industrielle, 2016, n°6.

BESNARD Denis, *Les opérateurs qui prennent des initiatives renforcent la sécurité*. Conviction n°21, mai 2016.

TAZI Dounia, *La culture locale n'est pas le facteur d'influence majeur de la culture de sécurité*. Conviction n°10, Avril 2015.

Besnard, D et al, *A worldwide meta-analysis of 21 safety culture surveys in oil, gas transport facilities & storage and services companies*. APS conference Singapour, 2013. Enquête ICSI ;

Brunel Camille, *La perception des conséquences de nos actions influence nos comportements de sécurité*. Conviction n°17, janvier 2016.

BESNARD Denis, *Les individus agissent, adhèrent et résistent en accord avec leurs perceptions*. Conviction n°5, octobre 2014.

VILLENA-LOPEZ Jesús, *Les accidents n'arrivent pas toujours aux personnes les moins expérimentées*. Conviction n°8, février 2015.

RASMUSSEN Jens. *Skills rules and knowledge ; signals, signs and symbols, and distinctions in human performance models*. 1983, IFSE Transactions on Systems. Man and Cybernetics, MC-13, 257-266.

BESNARD Denis, *Les personnes les plus expérimentées peuvent être trop sûres d'elles*. Conviction n°12, juin 2015.

AMALBERT René, *Piloter la sécurité : théories et pratiques sur les compromis et les arbitrages nécessaires*. Springer, 2012, Paris.

SIMARD Marcel, *Culture et gestion de la sécurité*. Encyclopédie de la santé et sécurité au travail, OIT Ginebra, 1989.

ICSI, *L'Essentiel de la culture de sécurité*, Avril 2017. Collection Les Essentiels de la Sécurité Industrielle.

DUFES E. « Le processus de la recherche » cours DEPRO – FORSUP de l'ENSOSP (19/02/2016) – Méthode de l'enquête et techniques du questionnement et de l'entretien.

Annexe 1

Entretien avec écoles « Business School » et organisations professionnelles

Madame, Monsieur bonjour,

Nous nous sommes rencontré... ou Je vous contact de la part de... (*Pour les personnes avec qui je ne suis pas en lien direct quotidiennement*).

Je réalise dans le cadre de mon Master 2 en Ingénierie et Management en Sécurité Globale Appliquée, un mémoire d'étude dont le thème porte sur la culture de sécurité des chefs d'entreprise et plus précisément en quoi celle-ci influencerait-elle une meilleure gestion d'une situation d'exception en sécurité (Cybersécurité, intelligence économique, santé sécurité, sûreté/malveillance...).

(Cas 1) : Aussi, je vous contacte pour savoir si vous pourriez me mettre en relation avec la ou les personne(s) les plus en liens avec la thématique au sein de (*nom de la structure*), et qui pourrait m'accorder une heure d'entretien pour répondre à quelques questions. Votre structure m'intéresse particulièrement car en lien directe avec le monde de l'entreprise et de ses dirigeants.

(Cas 2) : Aussi, je vous contacte pour savoir si vous, et/ou un membre de (*nom de la structure*), pourriez m'accorder une heure d'entretien pour répondre à quelques questions sur cette thématique. Votre structure m'intéresse particulièrement car en lien directe avec le monde de l'entreprise et de ses dirigeants.

Je vous remercie pour le temps que vous voudrez bien consacrer à cet échange.

Très cordialement,

Fabien VALENTE

Business school :

Les étudiants ont-ils dans leurs cursus de formation (cours et/ou stages), une approche sur les questions de sécurité (globale) dans les entreprises ?

Si oui, en quoi consiste(nt) t-il(s) et si non, pouvez-vous expliquer pourquoi ?

En tant que futur managers, cadres dirigeants, chefs d'entreprises... pensez-vous qu'un tel enseignement leur soit ou puisse leur être bénéfique et pourquoi ?

Comment percevez-vous la capacité de ces futurs professionnels à gérer une situation exceptionnelle de sécurité au sein d'une entreprise ?

Seriez-vous prêt à tenter l'expérience d'introduire un module de formation sur les problématiques de sécurité (globale) en entreprise ?

Organisations professionnelles :

Comment percevez-vous la culture de sécurité des chefs d'entreprises de votre organisation ?

Dans quel domaine celle-ci est-elle plutôt développée et pourquoi ?

Comment les chefs d'entreprises se préparent-ils à gérer une situation exceptionnelle ?

Quels dispositifs existe-t-il au sein de votre organisation pour les soutenir dans une telle situation ?

Votre organisation mène-t-elle des actions sur les problématiques de sécurité ? Si oui, lesquelles et si non, pourquoi ?

Annexe 2 :

Questionnaire : La culture de sécurité des chefs d'entreprises de TPE/PME

Madame, Monsieur bonjour,

Je réalise dans le cadre de ma formation professionnelle en Master 2 "Ingénierie et Management en Sécurité Globale Appliquée" option Gestion de Crise, un mémoire d'étude dont le thème porte sur la culture de sécurité des chefs d'entreprise et plus précisément en quoi celle-ci pourrait permettre une meilleure anticipation et gestion de crise.

Ce questionnaire est confidentiel et les informations récoltées ne seront pas divulguées, tout comme leur rendu dans le mémoire et la soutenance finale. Seule la compilation et l'analyse seront intégrées pour étayer mon hypothèse grâce à votre vécu de professionnels.

Les résultats vous seront envoyés sur simple demande en renseignant votre adresse mail à la fin du questionnaire.

Aussi, je vous remercie pour le temps (5 minutes) que vous voudrez bien consacrer à répondre aux 28 questions courtes qui vous sont proposées.

Pour répondre à ce questionnaire, cliquez ici :

<http://www.askabox.fr/repondre.php?s=159644&d=SPhL4dpGwDsf> ou rendez-vous sur www.askabox.fr dans la partie 'Répondre à un questionnaire' avec votre code questionnaire : 159644 et votre code réponse : SPhL4dpGwDsf

Très cordialement,

Fabien VALENTE

Questionnaire de l'enquête

1) Quel est le nom de votre entreprise (facultatif) ?

2) Dans quel département se situe votre entreprise (indiquez le N°) ?

3) Quelle est votre fonction au sein de l'entreprise :

- Chef d'entreprise
- PDG
- Directeur
- Cadre dirigeant
- Autre (Précisez)

4) Quel est le secteur d'activité de votre entreprise :

- Industrie
- Bâtiment
- Commerce
- Service
- Agricole
- Sanitaire/Social/Médico-Social

5) Quel est l'effectif de votre entreprise ?

- 1 à 10
- 11 à 19
- 20 à 49
- 50 à 250
- Autre (Précisez)

6) Votre entreprise a-t-elle une ou des certification(s) sécurité ?

- Santé sécurité au travail (ISO 45001, ISO 9001, OHSAS 18001, MASE...)
- Sécurité informatique (ISO 27001, 27002, ITIL, COBIT...)
- Malveillance/Sureté
- Intelligence économique
- Aucune
- Autre (préciser)

7) Votre entreprise dispose-t-elle de personne(s) dédiée(s) à la sécurité ?

- Santé Sécurité au Travail
- Sécurité informatique
- Malveillance/sureté

- Intelligence économique
- Polyvalente
- Aucune personne n'est dédiée à la sécurité (Indiquez pourquoi)
- Autre (Précisez)

8) Quel est le statut de la ou des personne(s) dédiée(s) à la sécurité ?

- Chef d'entreprise/Directeur/PDG
- Cadre
- Agent de maîtrise
- Employé/ouvrier

9) Si votre entreprise dispose d'au moins une personne dédiée à la sécurité, quelle est la part du temps de travail qui lui est consacrée ?

- Temps plein
- Temps partiel (Dans son temps de travail total)

10) Les questions de sécurité de l'entreprise sont-elles abordées en CODIR ?

- Systématiquement
- Seulement lorsque l'actualité le nécessite
- Jamais (Indiquez pourquoi)

11) Mettez-vous en place des actions de sensibilisation, information ou formation sur la sécurité globale au sein de votre entreprise ?

- Santé Sécurité au Travail
- Sécurité informatique
- Malveillance/sûreté
- Intelligence économique
- Jamais (Indiquez pourquoi)
- Autre (Précisez)

12) Si oui, quelles actions mettez-vous en place ? Si non, passez cette question.

- Journées sécurité
- Causerie
- Réunions d'information
- Affichage
- Mail et/ou lettre d'information
- Minute sécurité
- Formation
- Autre (Précisez)

13) Quelle définition donneriez-vous à « sécurité globale en entreprise » ?

14) Quelle définition donneriez-vous à « culture de sécurité en entreprise » ?

15) Évaluez-vous la culture de sécurité des collaborateurs de votre entreprise ?

- Oui (Indiquez pourquoi)
- Non (Indiquez pourquoi)

16) Quels sont les indicateurs qui vous permettent d'évaluer la culture de sécurité de vos collaborateurs (Santé Sécurité au Travail, malveillance, cybersécurité...)?

17) Comment évalueriez-vous la culture de sécurité de vos collaborateurs ?

- Forte
- Moyenne
- Faible

18) Comment évalueriez-vous votre culture de sécurité ?

- Forte
- Moyenne
- Faible

19) Sur quels indicateurs mesurez-vous votre culture de sécurité ?

20) Comment votre culture de sécurité c'est elle construite ?

- Formation initiale (scolaire, universitaire...)
- Formation continue
- Expériences professionnelles
- Expériences personnelles
- Réunions d'information, sensibilisation ou formation (organisme spécialisés, organisations professionnelles, chambres consulaires...)
- Votre entourage professionnel
- Les normes et la réglementation imposées aux entreprises
- Autre (Précisez)

21) Quels sont les facteurs qui influencent ou influenceraient à la hausse votre culture de sécurité ?

- L'implication de vos collaborateurs
- Les normes et la réglementation imposées aux entreprises
- Des événements survenus à d'autres entreprises
- Les informations communiquées par les médias

- Le fait de subir une situation exceptionnelle de sécurité
- La participation à des réunions d'information (SST, cyber sécurité, menace terrorisme...)
- La participation à des formations sur la sécurité (SST, cyber sécurité, menace terrorisme...)
- Autre (Précisez)

22) Avez-vous eu ces 3 dernières années une ou plusieurs situations exceptionnelles de sécurité ?

- Santé Sécurité au Travail
- Sécurité informatique
- Malveillance/sureté
- Intelligence économique
- Autre (Précisez)

23) Votre entreprise a-t-elle été impactée (organisation et/ou financier et/ou humain) de façon ?

- Grave avec préjudice fort
- Sérieuse avec préjudice moyen
- Bénigne avec préjudice faible
- Autre (Précisez)

24) Vos ressources internes (organisation, personnes qualifiées, process...) ont-elles permis de faire face à cette ou ces situation(s) exceptionnelle(s) ?

- Oui : Quels ont été les facteurs aidant ou facilitant ?
- Non : Indiquez pourquoi

25) Qu'est ce qui aurait pu être aidant et/ou facilitant pour améliorer la gestion de la ou des situation(s) vécue(s) ?

- Formation à la gestion de crise
- Soutien d'une organisation consulaire ou professionnelle
- Intervention d'un consultant spécialisé
- Une culture sécurité plus développée
- Une préparation interne de gestion de crise
- Autre (Précisez)

26) Vous êtes ?

- Un homme
- Une femme

27) Vous avez ?

- Entre 18 et 29 ans
- Entre 30 et 39 ans
- Entre 40 et 49 ans
- Entre 50 et 59 ans
- Plus de 60 ans

28) Votre adresse mail (Facultatif) ?

Annexe 3 :

Question 13. Quelle définition donneriez-vous à « sécurité globale en entreprise » ?
Prévenir vaut mieux que guérir
Pensez les risques auxquels peut être confrontée l'entreprise et les prévenir
prise en compte de tous les acteurs internes ou externes à l'entreprise pour assurer la sécurité de chacun à tous les niveaux (communication, logistique, accueil du public, etc)
Un cadre de travail sûr pour la santé et la sécurité de nos employés. un respect des règles de sécurité. une protection de nos données confidentielles
Je pense qu'il s'agit de la sécurité sous toute ses formes au sein de l'entreprise entière que ce soit physique, morale...
Une des composantes de la réussite de l'entreprise
Prise en compte des risques (incendies/malveillance/agressivité/vol et dommages/risques électriques/ terrorisme...) informatique sauvegarde des données quotidienne
C'est tout mettre en œuvre pour éviter les accidents avec les clients ou le personnel
ANTICIPER LES RISQUES
Procédures pour que tous salariés travaillent en toute sécurité dans une entreprise pérenne.
Ensemble de mesures permettant de prévenir des nuisances techniques ou humaines, d'y faire face et/ou d'y remédier dans la mesure du possible.
A mettre en place obligatoirement
Sécurité de tous et du cadre de travail, y compris en déplacements
PREVENTION DES RISQUES
Capacité de faire un diagnostic des risques potentiels en entreprise et de les anticiper
La sécurité au centre de nos préoccupations.
Survie de l'entreprise
Sécurité à tous les niveaux de l'entreprise et pour l'intégralité du personnel
Mise en place de formations, d'informations, etc. pour que chacun prenne conscience des enjeux du travail en sécurité et des moyens pour y parvenir.
Vitale c'est une vigilance quotidienne
Sécurité du personnel, du matériel et des données.
Ensemble des aspects sécuritaire dans l'entreprise
Ensemble de procédure de sécurité cohérente les uns avec les autres
Indispensable à la marche d'un établissement mais très complexe, la sécurité permet de mettre hors de danger les usagers, de prévenir les risques de quelque nature qu'ils soient.
VIGILANCE DE TOUS LES INSTANTS
Sécurité, tous concernés
Protection des salariés
PREVENIR LES MALVEILLANCES ET LES RISQUES
Cela concerne toute la sécurité en entreprise des personnes et des biens (matériel et immatériel-information, sensibilisation, réputation). Santé, sécurité physique, morale et matérielle, sûreté (malveillance, intrusion, menaces)

<p>C'est une démarche volontaire qui vise à :</p> <ul style="list-style-type: none"> - anticiper les changements, - augmenter la réactivité et la performance de l'entreprise dans la prévention des risques en SST, - limiter les dysfonctionnements en SST, - assurer une cohérence globale avec les autres démarches de management. <p>Elle participe à l'amélioration de l'image de l'entreprise.</p>
<p>1 - Actions continues de prévention 2 - Actions de prévention à jour au regard des risques et des activités 3- Impliquer toutes les strates de l'entreprise (ex : que les acheteurs soient sensibilisés quand ils ont le choix entre plusieurs matériels). la prévention se fait par l'information mais aussi par les méthodes et par les matériels mis à disposition (des téléphones peu émetteurs d'ondes...) 4 - Etre prêt en cas de...</p>
Gestion de la sécurité effectuée par tous les processus de l'organisme (humains/financiers/matières 1ère/produits/production/matériels/Infrastructures SI...)
Gestion encadrée des enfants
Une priorité, avant Qualité
Capacité d'assurer à une collectivité et à ses membres un niveau de protection suffisant contre les risques et menaces de toutes natures (médicales, sociales, sociétales, environnementales, économiques ...)
Politique de management au quotidien et d'implication de tout le personnel
Sécurité des biens (intrusion physique et virtuelle) et des personnes (physique, morale)
Attitude visant à anticiper les risques pouvant affecter les biens et ou personnes de l'entreprise
A chaque étape de travail
Protection des salariés et des produits
Cadre permettant la sécurité des biens et des personnes
Prévention, vigilance, réactivité
Assurer la préservation des biens et des personnes qui composent l'entreprise
C'est prendre soin des personnes et des biens, avec un angle large porté sur la sécurité (pas d'atteinte physique ni morale des personnes) mais également sur leur santé durablement.
Entreprise attentive à tout ce qui touche la sécurité dans tous les domaines de l'entreprise (stratégie, commerce, marketing, gestion, production, services, ...)
Sert à protéger toutes les personnes présentes dans l'entreprise
SAUVEGARDE DES INTERETS MORAUX ET ECONOMIQUES
Protection élargie de toutes les entités de l'entreprise, qu'elles soient matérielles, immatérielles ou humaines. (protection données, matériel / mobilier, et le personnel)
Dispositif formalisé permettant de limiter les risques
Respect du salarié
Mise en place de moyens et mesures permettant de protéger le patrimoine de l'entreprise contre la perte ou l'altération de ressources
L'ensemble des moyens matériels et humains visant à permettre à tous de travailler dans des conditions qui respectent la sante physique, mentale
Ensemble des dispositions prises pour prévenir les accidents matériels et humains
S'assurer que les salariés soient en sécurité + sécurité des données informatiques
Actions mises en place par l'entreprise afin de sensibiliser, former, anticiper et agir pour la sécurité des salariés en entreprise

Ensemble des actions menées par l'entreprise en vue de sensibiliser tous les salariés à la prévention et aux dangers sur tout ce qui concerne la sécurité physique et informatique de l'entreprise
Une attention quotidienne
Démarches permettant de protéger l'entreprise
Sécurité des personnes et des biens en termes d'hygiène, de déplacements, de mise à jour et conformité des appareils (incendie..), du respect de la convention collective
Se protéger pour le bien-être de tous (salariés, clients, partenaires, actionnaires....)
PROTECTION DES PERSONNES CLIENTS OU EMPLOYES
Envisager tous les risques pouvant affecter les activités de l'entreprise
PRESERVER LE PERSONNEL, LES INSTALLATIONS ET LES EQUIPEMENTS DANS UN ENVIRONNEMENT DE TRAVAIL RESPECTUEUX DU CADRE REGLEMENTAIRE
Permettre à chacun d'être en sécurité au sein de l'entreprise
La sécurité globale en entreprise comprend l'ensemble des domaines suivants : SST + malveillance/sécurité + informatique + intelligence économique
Eviter tous les risques potentiels
Elle concerne la sécurité des biens, des données et des agents
Impossible
Assurer la sécurité des biens et des personnes (personnes handicapés et personnel) tout en poursuivant les activités relevant des missions de l'établissement. L'anticipation, la prévention et la mise en place des plans d'action permettant de limiter tout stress ou angoisse dans la gestion de crise.
Sécurité des résidents et des personnels
Prise en compte des risques
Un ensemble d'actions qui permettent de réduire les risques internes et externes afin d'assurer la pérennité de l'entreprise.
La sécurité globale c'est l'équivalent de la qualité zéro défaut c'est à dire les risques mettre en place des actions correctives mesurer les écarts faire de la formation et respecter les procédures qualités ; ainsi on arrive à la sécurité total dans tous les domaines, informatique, sécurité, bien-être au travail, maintien de revenu, santé, emploi, pérennité de l'entreprise, développement techniques etc...
Sécurité sur tous les postes de travail
La sécurité fait partie intégrante de la qualité de vie au travail
Sécuriser l'espace de travail et son environnement
Garantir l'intégrité des collaborateurs et des biens
Limiter tout risque qui puisse déstabiliser l'entreprise
sécurité des personnes, sécurité environnementale, sécurité économique
Une prévention de tous les instants, une prise de conscience collective, une véritable culture d'entreprise
SECURITE DES SALARIES AINSI QUE DES CLIENTS
SECURITE TRANSVERSE
Il s'agit d'assurer des conditions de travail qui permettent au personnel de travailler dans un environnement cohérent et sur
Limiter les risques d'accidents ou de malveillances, et donc de mise en cause de l'entreprise et de son dirigeant
Prévention et culture du risque
Sécuriser tous les postes de l'entreprise et former tous les acteurs aux bonnes pratiques de sécurité. Aménager et investir dans des équipements nécessaires à la sécurité.
OBLIGATOIRE

Annexe 4 :

14. Quelle définition donneriez-vous à « culture de sécurité en entreprise » ?
Y a du boulot
Ensemble de pratiques professionnelles visant à garantir la sécurité de l'entreprise
communication interne sur la sécurité en entreprise
L'anticipation/la prévention des risques professionnels et la mise en place de solutions pré déterminées connues de tous (formation -information). Sujet à l'ordre du jour en permanence (manager et employés)
Je pense que c'est la manière et les actions mis en place pour assurer et promouvoir la sécurité dans l'entreprise.
L'image de la volonté de la direction
Prévention des risques, informations, consignes : règlement intérieur/ affichage
Les règles de sécurité sont apprises et connues et des rappels (formations) sont mis en place de manière récurrente afin que chacun soit sensibilisé.
LA PREVENTION // LA FORMATION // LA REACTIVITE AUX ANOMALIES
Procédures pour anticiper et réagir face aux risques
Etat d'esprit qui doit permettre d'ancrer la sécurité comme un prérequis dans les différentes actions menées
A suivre et à entretenir
Approche obligatoire du respect individuel et collectif
ACQUISITION DES BONS REFLEXES
La culture de sécurité au travail englobe les différents aspects de maîtrise des risques d'un groupe de travail (comportementaux, managériaux etc ... Le renforcement d'une culture de sécurité au travail vise à développer une perception du risque partagée par tous les membres de l'entreprise, avec comme résultat un ensemble de comportements et de pratiques sécuritaires réduisant significativement la fréquence et la gravité des accidents...
QUALITE SECURITE CLIENT SATISFAIT ET PDG PAS FACHE
Obligatoire
Etat d'esprit permanent autour de la sécurité
Etat d'esprit de chaque collaborateur à travailler en sécurité pour lui, ses collègues et les biens de l'entreprise.
On est passé de rien à trop de pression sur l'encadrement
Les réflexes à avoir selon le domaine d'action.
Il s'agit des fondamentaux qui sont donnés à tous comme la culture d'entreprise en fait elle en fait partie tout simplement.
Niveau de sensibilisation général des salariés et dirigeants à la sécurité
Ensemble de procédures, prises en compte des risques que les professionnels d'un établissement partagent et mettent au débat, dans un cadre législatif donné.
CULTURE PARTAGEE, PARLEE, DEBATTUE, ETAYEE PAR DES FORMATIONS
La sécurité est la préoccupation N° 1
Sensibilisation à son environnement
VIGILANCE CITOYENNE ET PROFESSIONNELLE
Manière de penser et de faire par l'entreprise sur la maîtrise des risques liée à ses activités ainsi qu'à celles de ses partenaires (transporteurs, affréteurs, par ex.)
Elle englobe les différents aspects comportementaux, managériaux et techniques de maîtrise des risques d'un groupe de travail.
Impliquer toutes les strates de l'entreprise (ex : que les acheteurs soient sensibilisés quand ils ont le choix entre plusieurs matériels). la prévention se fait par l'information mais aussi par les méthodes et par les matériels mis à disposition (des téléphones peu émetteurs d'ondes...)

Connaissance des règles de sécurité au niveau du poste de travail et participation des salariés à l'amélioration de la sécurité
Etre attentif aux besoins de chacun
"Safety first"
Intégration de cette notion de sécurité globale dans le projet d'établissement
Un état d'esprit et une capacité à réagir dès qu'on détecte une situation dangereuse
Impulsion donnée par le dirigeant sur l'importance de la sécurité dans l'entreprise
Attitude visant à anticiper les risques pouvant affecter les biens et/ou les personnes
Un état d'esprit
Prévention
Langage commun en matière de "faire la sécurité" ensemble
La sécurité est l'affaire de tous à titre individuel ou collectif
Faire en sorte que chaque salarié soit acteur de prévention pour lui-même et pour les autres
Chaque salarié doit être en veille permanente pour lui et pour les autres. Une forme de responsabilité individuelle constante.
Tout est fait pour durer, s'améliorer, se protéger quelle que soit l'action menée
Instruire les salariés et le chef d'entreprise à la sécurité en entreprise
PROTECTION DES BIENS, DES SERVICES ET DES HOMMES
Les habitudes de chacun en ce qui concerne la sécurité sur tous les points (donner le mot de passe de l'ordinateur à quelqu'un hors entreprise / le code de l'interphone ...)
Intégration dans les pratiques courantes et quotidiennes
Rôle du dirigeant
Sensibilisation des collaborateurs au fait que le patrimoine de l'entreprise est une richesse convoitée et précieuse, donc à protéger
L'appropriation par chacun de son rôle de "moyen humain" (en référence à ma définition ci-dessus)
Implication des salariés à la prévention des accidents matériels et humains
Obtenir un réflexe de chaque salarié sur les différents points de sécurité : vigilance et alerte
Politique mise en place par l'entreprise afin de sensibiliser, former, anticiper et agir pour la sécurité des salariés en entreprise
Actions de prévention (affichage, formations, information)
Une nécessité
Fondements pour bien protéger l'entreprise
C'est la nécessité de toujours animer les équipes dans le sens d'une culture d'établissement à la sécurité des personnes et des biens à travers la mise à jour des documents, de formations dédiées à la sécurité, d'informations à faire redescendre aux équipes
Donner à chacun les moyens d'agir
SENSIBILISATION A LA SECURITE
Garantir la pérennité des activités de l'entreprise et la santé de ses collaborateurs
ACTION DE PREVENTION
Faire prendre conscience que la sécurité de chacun est le rôle de tous
L'implication des tous, à tous les niveaux, de la hiérarchie de la sécurité globale
Etat d'esprit responsable
C'est la connaissance du personnel en matière de sécurité au travail (physique et mentale)
Imprégnation au quotidien de la notion de sécurité

La culture de sécurité c'est la construction du projet d'établissement qui prenne en compte tous les champs de la sécurité afin que chaque personne connaisse les risques potentiels et leur gestion. Cette culture de sécurité doit être prise en compte tant au niveau des objectifs que de l'organisation.
Mise en pratique des réglementations
Prise de conscience des risques
Si le risque est une condition de la réussite sa bonne gestion Est une garantie du succès
Que tout le monde soit formé
Pour moi elle se rapproche de la qualité en entreprise et de ses méthodes HACCP ou autres... elle passe par le respect de norme afnor ou iso par exemple et de certification afin de valider les compétences du personnel.
La sécurité est entrée dans les mœurs de tout le personnel
Un pilier de la qualité
Sensibiliser les collaborateurs a la sécurité et avoir les bonnes pratiques
Esprit de pérennisation des équipes de travail
Quand la sécurité fait partie intégrante de la vie de l'entreprise et que chacun (tous) ait conscience de l'importance de la sécurité et que le management entretienne cette conscience collective.
Moyens matériels et méthodes de travail adaptées et surtout recherche de l'implication du personnel
Nous essayons d'englober les différents aspects comportementaux, managériaux et techniques de maîtrise des risques.
INFORMATIONS RELATIVE A LA SECURITE DES INDIVIDUS
VGILANCE SECURITE ENTREPRISE
Cela se traduit par une volonté stratégique de faire de la sécurité un élément des activités professionnelles
Ensemble d'habitude et de coutumes rendues automatique relative à la sécurité des personnes
Gestion du risque
Inculquer à tous les salariés cette culture de mise en sécurité dans toutes les situations qu'ils rencontrent. Que cela devienne un réflexe.
NECESSAIRE
Bonne

Annexe 5 :

16. Quels sont les indicateurs qui vous permettent d'évaluer la culture de sécurité de vos collaborateurs (Santé Sécurité au Travail, malveillance, cybersécurité...)?
Aucun
Aucun
Questionnaires réguliers envoyés
Nombre d'accidents
Aucun
Suivi des présences aux causeries, réunions sécurités
Aucun
ALARMES // LITIGES // DYSFONCTIONNEMENTS // ACCIDENTS DU TRAVAIL OU DE LA CIRCULATION
La bonne santé de l'entreprise, l'absentéisme et le nombre d'accident du travail
Pas de mise en place d'indicateurs à ce jour
Aucun
Les discussions et gestes
AUDIT FLASCH
Nombre de fiche d'anomalie, d'amélioration. rapport 5/5. Nombre de remontées de situations dangereuses.
Qcm collaborateurs
Aucun
Audits sécurité
Taux de participation aux causeries et nombre de causeries
Taux d'AT/Nombre d'incidents
Evaluation hebdomadaire
Pas d'indicateurs
Interventions des élus du CHSCT sur le terrain, application de la réglementation, interpellations au sein de l'équipe sur des risques
TF / TG . Remonté des Presque Accidents
Incidents, alertes, remontées des informations
Questionnement ciblé
Je ne sais pas
Nombre de formations liées à la sécurité, nombre de personnels SST, respect des procédures et instructions en place
La proximité
Exemple: "HSEPI" plus d'autres indicateurs HSE spécifiques au Groupe, non communicables à l'extérieur. Absentéisme, engagement du personnel, etc...
Evaluation effectuée par responsable de secteur (RH, informatique ...)
TF1/TF/TF3, nombre d'actions sécurités réalisées
Aucun
aucun
Leur vigilance, les ordres du jour des réunions
Aucun
Des audits réguliers dans les sites une évaluation de nos actions
Aucun

Tableau établi avec le groupe auxquels nous appartenons
Déclarations d'évènements indésirables en lien avec la médecine du travail , la sécurité du SI, les intrusions
Aucune
Il n'y en a pas
Visite sécurité
Aucun
Cybersécurité : Vidéo de rappels suivis de Quiz
Taux de formation des nouveaux entrants à 100%
Statistique et suivi
Santé Sécurité au Travail, réactivité aux tentatives de fraude , ...
Les consultations médecins/infirmiers ATSL/ Suivi par notre informaticien qui nous signale si malveillance, arrêt de travail ou pas, respect de la convention collective
Quiz, tests, problèmes, audits....
PAS D'INDICATEUR CHIFFRE, VERIFICATION DE LA MISE EN PLACE DES CONSIGNES DE SECURITE, HYGIENE
SST, LES AT ET L'ABSENTEISME
Taux de fréquence, tentative d'intrusion sur réseau informatique...
Le nombre d'occurrences d'évènement
indicateurs stratégiques : indicateurs opérationnels : indicateurs de management
Aucun indicateur
Les drills, exercices cadres, exercices généraux organisés en situations en application des protocoles mis en place
Panne machine, Accident travail
Aucun
Exercice incendie, gestion de crise et mesures correctives
Accident de travail et bobologie
Accidentologie / test mails
Respect des règles et consignes
Taux de participation aux QCM mensuel Taux de participation au Mur de la Sécurité
Port des EPI, retour sur la satisfaction de la formation prévention
Taux d'AT AM. Plaintes (orales) des salariés.

Annexe 6 :

19. Sur quels indicateurs mesurez-vous votre culture de sécurité ?
Aucun
Présence d'antivirus à jour, sollicitation des équipes sur les virus, destruction des documents confidentiels, bureaux et armoires fermés ou non, ordinateur avec Mot de Passe...
Echanges en réunion ou autre, mails d'information, actualités
Nombre d'accidents
Sur le peu d'arrêts maladies, l'investissement personnel des collaborateurs qui montre un bon esprit mais aussi grâce au document unique qui a mis en avant des problématiques à régler.
Les taux de fréquence, gravité mais aussi la fréquence de remontées des incidents
Anticipation des risques possibles et mesures à mettre en place règlement intérieur
TAUX D'A.T. // TAUX DE LITIGES // TAUX DE SINISTRES //
Réflexes acquis
Aucun indicateur
25 ans d'exercice en France et à l'étranger, sur site ou en laboratoire
Par comparaison avec les obligations réglementaires et ce que l'on s'impose
Prévention des risques au travail
Nbre de fiche d'anomalie, d'amélioration. Nombre de rapport 5/5. Nombre de remontées de situations dangereuses.
Réponse au Qcm et rapports annuel des accidents
Aucune
Sur le respect de chaque consigne de sécurité donnée lors des formations
Nombre de causeries
Prise de risques
Respect des consignes de sécurités
Le temps que j'y consacre, la connaissance que j'en ai.
A jour sur la réglementation, organisation de formations chaque année sur ce thème
Je m'en remet au jugement de mes collaborateurs
Responsabilisation inter thématiques
Mon expérience. Seule pas besoin d'indicateurs tels qu'on l'entend.
SST obtenu en Septembre 2017
Préoccupation constante
Nombre d'AT, Nbre de SST, nbre de formations externes et internes liées à la sécurité
Sur notre communication permanente
HSEPI = Indicateur interne groupe
L'importance que j'y apporte au quotidien
A l'intérêt et au temps passé à lire des articles liés au sujet
Tableau des objectifs annuel
Sur les actions et les plans mis en place
aucun
Actuellement je n'en connais pas
intuitif (!)
Le bilan des accidents de travail

Incidents critiques
Penser aux conséquences d'une prise de décision (ouverture d'une pièce jointe d'un mail douteux...) / Réactivité en cas de problème de sécurité / abonnements aux organismes qui promulguent des notes d'informations
Nombre de signalement
Aucun
Il n'y en a pas
Dans ma fonction je suis conscient de la plupart des risques et fais en sorte de le limiter
Aucun
Assez indifférent, donc pas d'indicateurs...
Cybersécurité : Taux de réponses aux quizz
Actions réalisées au sujet de la sécurité en entreprise (formation, réunions, affichages, ...)
J'assiste à toutes les formations, campagnes d'affichage, etc....
la QSE mis en place et ses statistiques rendues
SST, Coûts opérationnels
C'est à ce jour une démarche individuelle mais que nous devrions travailler au sein de l'association gestionnaire. les indicateurs seraient la tenue d'un tableau de bord GRH (en cours), le respect strict de la réglementation (temps de travail, de pause, de congés...)
IMPLICATION LES MISES EN PLACE D' ACTIONS LIEES A LA SECURITE
Taux absentéisme AT
AT
Obligations EDF / code du travail, etc.
Le nombre d'accident/incidents et les retours collaborateurs
Aucuns
Lors des formations
Stratégiques, managériales et opérationnels
Aucun indicateur
Par rapport aux résultats des différents exercices impulsés, aux indicateurs légaux existants
Malveillance / sûreté : temps de réaction / cyber sécurité : multiplication des pare feu / sécurité au travail : utilisation des équipements adéquates - information : cloisonnement par niveau hiérarchique
Je viens de la qualité je dirais donc que je reste ouvert et que ma curiosité n'est jamais assez assouvi
Taux AT
Aucun
Nombre d'incidents?
Retour collaborateur et AT
Pas d'indicateurs
Moyens mis en œuvre, implication totale
Préoccupation permanente
Je ne sais pas
PAS UN SUJET MAJEUR
Je ne sais pas
Comportement de chacun
Respect des process, sauvegardes, signalement.
Comparaison avec d'autres sociétés, discussions avec d'autres responsables sécurité.
L'affichage
Pas d'accident

Quelques citations...

L'histoire nous enseigne qu'une civilisation, pour garder la maîtrise de son destin, doit se donner les moyens de sa sécurité. (Jacques Chirac)

Un ordinateur en sécurité est un ordinateur éteint. Et encore... (Bill Gates)

Dans l'entreprise, dans une équipe, donnez de l'importance à tous et du respect à chacun. (Didier Court)

La véritable culture, celle qui est utile, est toujours une synthèse entre le savoir accumulé et l'inlassable observation de la vie. (Francesco Alberoni)

La culture c'est la réponse à la crise. (Nicolas Sarkozy)

La qualité n'est pas une action, c'est une habitude. (Aristote)