

La formation continue des salariés en veille stratégique et cybersécurité

Mis à jour le 29 Mai 2019



© Adobe Stock

Les cyber attaques et les guerres concurrentielles demandent aux entreprises un effort d'adaptation accru qui implique une mise en place interne de dispositifs de veille ciblée pour orienter l'innovation et les choix stratégiques du chef d'entreprise.

Le contexte actuel d'évolution permanente et de « guerre » économique

Les multiples **attaques cyber des systèmes d'information**, et les guerres concurrentielles actuelles/à venir, demandent aux entreprises un effort d'adaptation accru. Cela implique une mise en place interne de **dispositifs de cyber sécurité** et **une veille ciblée** pour orienter l'innovation et les choix stratégiques du chef d'entreprise.

En situation de méconnaissance, ou de connaissance insuffisante, de leur l'environnement économique, nombre d'entreprises, en particulier les PME-TPE, sont en défaut d'anticipation et d'adaptation, voire en difficulté : elles ne sont pas en capacité de cerner et d'apprécier à leur juste mesure les risques, et les opportunités de leur marché. Face à cette menace, il est nécessaire qu'elles structurent des veilles professionnelles à l'aide des outils de la digitalisation. Ces **démarches** de veille, encore mal connues des PME, sont **de plus en plus performantes** même lorsqu'il s'agit d'une démarches simple de traitement de l'information - thème de l'intelligence Economique : détection, collecte, analyse, et diffusion interne.

Les veilles s'effectuent sur des sujets tels que l'activité des concurrents, les changements d'orientation des marchés, l'évolution réglementaire, l'innovation technologique, les normes écologiques, ou encore l'évolution du comportement des consommateurs, et de façon générale les nouvelles tendances sociétales sur un secteur précis.

La mise en place de cette fonction de **veille stratégique et sécurité** est l'affaire de tous, chef d'entreprise et salariés, et implique l'organisation du partage de l'information en interne, sur l'ensemble des thèmes convenus. Elle permet d'identifier de nouvelles sources de croissance, ou de voir venir de nouvelles menaces.

Cette démarche est devenue essentielle. Le parcours de l'entreprise Kodak en est un exemple. Leader dans la photographie argentique, l'entreprise n'a pas, semble-t-il, su prendre le virage du numérique. Sa survie, comme celle de toute entreprise, technologique ou non, est liée à cette capacité.

Former et sensibiliser

Les **compétences additionnelles** nécessaires pour mettre en place de telles démarches impliquent de former des collaborateurs de l'entreprise, qui interviendront en complément de prestations occasionnelles de consultants, experts du renseignement à haute valeur ajoutée. Parallèlement, il est nécessaire de **sensibiliser les salariés et partenaires** à la dimension de cyber sécurité pour assurer la protection des biens immatériels et parer aux différentes attaques qui impactent l'activité : par exemple, le piratage de compte, la demande de rançon ou les virus informatiques et, au-delà, les attaques concurrentielles et réputationnelles qui peuvent être beaucoup plus graves.

Former un salarié en première approche sur ces thèmes permettra d'introduire dans la structure une culture et une pratique minimum, en structurant les fonctions de veille et de sécurité économique. Les offres de formation doivent donc suivre, et même anticiper ce mouvement de fond.

L'offre de formation continue en veille et cyber sécurité

- **Formation à la veille régulière en interne** sur des thèmes très ciblés, ou des renseignements précis.

Les recherches se font en lien étroit avec la demande des équipes et du chef d'entreprise, sur des thèmes liés à la stratégie de développement de l'entreprise.

Cette formation permettra au salarié déjà en poste sur une fonction support, et formé en complément, d'appréhender les outils, le raisonnement, pour mettre en place une veille concertée et opérationnelle. La veille pourra porter sur le dépôt des brevets, l'évolution d'un marché (mécanique de précision, appareil de laboratoire, etc.), les clients potentiels d'un secteur, etc. Elle permettra de répondre ainsi aux besoins de l'entreprise qui lui seront formulés clairement.

- **Formation à la cybersécurité, et aux multiples risques**, liés au Cloud (importance des contrats de prestation), à la mise en place du règlement général sur la protection des données (RGPD), aux contrats de sous-traitance, au respect des réglementations, à la mise en conformité aux règles anticorruption (Compliance) sur lesquelles les amendes américaines sont particulièrement élevées – cas d'Alstom par exemple.

Tous les risques qui menacent l'entreprise pourront être évoqués pour une prise de conscience des risques élémentaires dans un premier temps, et une prise en main spécifique impliquant l'ensemble des salariés dans un second temps. Selon l'entreprise, le niveau des risques sera plus ou moins élevé.

Il s'agit d'une **formation de premier niveau qui accompagne la numérisation des entreprises**.

Faire appel aux salariés de niveau bac ou bac +2 permet d'introduire en entreprise la culture et les outils de veille et de protection, sans coût supplémentaire pour la structure, en apportant aux salariés une connaissance et pratique complémentaire à leur fonction principale.

Le chef d'entreprise et ses collaborateurs, convaincus par la production d'informations clés qui leur seront apportées à la demande, pourront alors choisir de monter en compétence en interne au fil du temps, et de créer un vrai poste à plein temps si nécessaire, enfin, de faire appel ponctuellement à des professionnels consultants externes.

La démarche sera la même pour la veille ou la protection des données et des sites.

Les offres de formation à développer et multiplier

Ces fonctions nouvelles sont insuffisamment préparées et maîtrisées au sein des PME, alors que l'activité de celles-ci est la cible de nombre de concurrents internationaux ou nationaux, ou d'acteurs malveillants qui pratiquent des attaques sous de multiples formes. Le but est donc d'acculturer le milieu des petites et moyennes entreprises françaises par la formation continue.

La Disse (Déléguée à l'information stratégique et à la sécurité économique) en Ile-de-France, qui est rattachée à la Direccte Ile-de-France, a constaté que pour installer une veille de qualité en interne, les entreprises ne disposant généralement pas de compétences spécifiques donnent la préférence à la solution la moins coûteuse en faisant le plus souvent appel à un stagiaire d'école d'Intelligence Economique, plutôt que de faire appel à un professionnel plus expérimenté, même de façon ponctuelle.

Aujourd'hui, des offres de formation initiales spécialisées de niveau bac +4 et 5 sont présentes sur le marché, comme celles portées par divers établissements d'enseignement supérieur - [Institut des hautes études de défense nationale](#) ^[1] (IHEDN), [Institut national des hautes études de la Sécurité et de la Justice](#) ^[2] (INHESJ), [Ecole de guerre économique](#) ^[3] (EGE), [Ecole Européenne d'Intelligence Economique](#) ^[4] (EEIE), [Conservatoire des arts et métiers](#) ^[5] (Cnam) -, ou encore des universités. Mais elles s'adressent à des professionnels de haut niveau pour en faire des experts, dont les rémunérations sont souvent inaccessibles pour les TPE/PME. De plus, ces formations, si elles ne sont pas complémentaires à une formation métiers, intéressent peu les entreprises : il est entendu aujourd'hui, que ces compétences ne sont opérationnelles qu'en complément des métiers de l'entreprise.

A l'opposé, **les offres de formation professionnelle continue visant des niveaux bac ou bac + 2** sont peu nombreuses. La Disse en Ile-de-France pense prioritaire de développer une offre de formation pour ce public : le salarié de la TPE/PME gagnera ainsi en compétence, pour enrichir sa mission principale (et le coût de formation continue sera réduit pour le chef d'entreprise). Ce dernier en retirera un bénéfice immédiat : apporter de la cohérence à des données brutes, partielles et éparpillées, et transformer collectivement les informations en connaissance marché. Cela lui permettra en outre de nouer des coopérations, des partenariats, et d'actionner les meilleurs leviers.

Si les formations de haut niveau déjà proposées constituent une étape décisive, elles ne sont pas suffisantes pour toucher l'ensemble du tissu économique. Dès lors la nécessité de sensibiliser les entreprises et de leur proposer simultanément une offre de formation professionnelle continue paraît indispensable.

Les profils des salariés à former pourraient être : assistants de direction, commerciaux, comptables, personnes en contact direct avec le chef d'entreprise pour dialoguer sur ses besoins en renseignements précis, ou informations plus larges. Ainsi, peut être concerné tout type

de poste en fonction de la configuration de l'entreprise, et de l'appétence et l'ouverture des personnes candidates. Ces métiers demandent aptitude à l'écoute et facilités numériques, sans diplôme particulier.

En qualité de « référents » dans leur fonction de management de l'information, tant auprès de leurs collègues que des experts externes, ils seront des relais pour la mise en place de bonnes pratiques dans la structure. Ils veilleront donc à maintenir un dialogue permanent avec le chef d'entreprise sur les sujets à suivre et les risques, et pourront lui recommander des contacts sérieux, ou des dispositifs sécurisés, labellisés, dans les domaines repérés.

Elargir la palette des communications et initiatives existantes

- Des **présentations** ou formations ont été réalisées, par la Disse et bien d'autres acteurs économiques, à destination de professionnels accompagnant les entreprises, institutionnels, et réseaux d'entreprises. Il s'agit d'actions de sensibilisation ayant pour but de **créer un intérêt** pour une prise en main de ces démarches, en lien avec la numérisation des TPE-PME.
- Des **ateliers** de formation sont proposés, portés en Ile-de-France par la Chambre du commerce et de l'industrie (CCI), la Confédération des petites et moyennes entreprises (CPME), le Mouvement des entreprises de France (Medef), et d'autres organismes, sur une journée, ou quelques journées, avec des résultats très positifs.
- Des **publications** ^[6] dédiées à l'Intelligence économique sont diffusées.
- Des **conférences, débats, colloques** se tiennent régulièrement : voir les sites [Le portail de l'IE](#) ^[7], [Veille Mag](#) ^[8], [l'Agence nationale de la sécurité des systèmes d'information](#) ^[9] (ANSSI), le [Cybercercle](#) ^[10], [CCI France](#) ^[11], les CCEF, Conseillers du Commerce extérieur de la France, la [Banque publique d'Investissement](#) ^[12] (BPI France).

Il est donc proposé, à plus long terme, de **multiplier les offres de formation** de jeunes de niveau bac/bac pro/bac +2, déjà en entreprise ou arrivant sur le marché du travail ; ce projet est à construire avec l'appui des partenaires régionaux. **Une formation de 50 ou 70 heures**, par exemple, pourrait donner accès à un certificat portant sur l'élaboration d'une veille, la recherche d'informations clés, la protection des informations de l'entreprise, la construction d'un site Internet pour l'entreprise, son e-réputation, la communication sur les réseaux sociaux, les activités sur le Web, etc.

Des référentiels de formation déjà proposés, d'autres en cours d'élaboration

- Un **référentiel de formation à la cyber sécurité** : le Service de l'information stratégique et de la sécurité économiques (Sisse) a mis en ligne sur son site ce référentiel de formation réalisé avec l'ANSSI, à disposition de tous les organismes de formation, et notamment les CCI. On pourra aussi consulter, sur le site de Défi métiers, [le référentiel de formation](#) ^[13].
- Un **référentiel de formation à la veille** est en cours de rédaction par l'Afpa, sous l'impulsion de la Direccte Ile-de-France. Il sera mis en ligne dans les prochains mois, après consultation de professionnels qui apportent leur expertise.

On pourra se reporter à la plaquette de la Direccte Ile-de-France sur les métiers de l'Intelligence Economique, et sur ses écoles, dont les références sont à retrouver dans la partie Ressources de ce dossier réalisé par Diane De Souza, Déléguée à l'information stratégique et à la sécurité économique (Disse), Direccte Ile-de-France.

Ressources

- Les **guides et MOOC** Sécurité et Intelligence Economique des organismes cités plus haut, que l'on retrouve sur les divers sites et dans la plaquette de la Direccte intitulée **Les acteurs de l'Intelligence économique en Ile-de-France** ^[14] ;
- Le **film Primadiag** ^[15] de la Direccte (Disse) : témoignage d'un chef d'entreprise, sur Youtube ;
- Les **fiches et autodiagnostic** ^[16] sur le site du Sisse ;
- Les **Films sur la sécurité en entreprise** ^[17] présentés lors du [festival Security System Valley](#) ^[18] ;
- Le **Guide du Routard de l'IE** ^[19] sur le site du Sisse.

Ce dossier a été réalisé par Diane De Souza, Déléguée à l'information stratégique et à la sécurité économique (Disse), Direccte Ile-de-France.

Contacts

Coordonnées des Délégués à l'information stratégique et la sécurité économique (Disse) :

- Diane de Souza, diane.de-souza@direccte.gouv.fr ^[20] 01 70 96 16 94
- Antoine Clermond, antoine.clermond@direccte.gouv.fr ^[21] 01 70 96 15 04
- Frédérique Lebon, frederique.lebon@direccte.gouv.fr ^[22] 01 70 96 16 94 à compter du 01/06/2019.

Service de l'information stratégique et sécurité économique (Sisse), Direction générale des entreprises, Direccte Ile-de-France

Tags

Tags : [Veille stratégique](#) ^[23] | [cyber sécurité](#) ^[24] | [intelligence économique](#) ^[25] | [Direccte](#) ^[26] | [Ile-de-France](#) ^[27]