MARCHÉ DE L'EMPLOI

ANALYSE MARS 2014

AU SOMMAIRE

MÉTIERS D'AVENIR

LE GESTIONNAIRE DE RISQUES LIES A LA SECURITE DE L'INFORMATION

(RISK MANAGER)

La sécurité de l'information devient un enjeu majeur pour les petites et grandes entreprises, quel que soit le secteur d'activité. Pour y faire face, de quels types de professionnels le marché aurait-il besoin dans trois à cinq ans ? Quelles sont les prestations à mettre en place sur le marché de l'emploi pour accompagner les évolutions ? Quelles réponses apporter dès aujourd'hui, aux défis de demain ? Autant de questions auxquelles l'analyse prospective ici proposée tentera de répondre.

Le présent document comprend deux parties. La première inscrit la démarche dans son contexte et présente brièvement les résultats de l'étude prospective. La seconde reprend dans le détail l'ensemble du processus d'analyse et ses résultats.

PARTIE 1 : CONTEXTE ET SYNTHESE DES RESULTATS

Anticiper les évolutions, la transformation et l'émergence des métiers constitue un axe majeur de la mission d'analyse et d'information sur le marché du travail du Forem. Une première approche à caractère exploratoire, a été réalisée en 2013 dans le cadre de l'étude publiée sous le titre « Métiers d'avenir pour la Wallonie »[1]. Cet ouvrage reprend les grandes tendances d'évolution des secteurs de l'économie identifiées sur base d'une large revue bibliographique et de la consultation de 300 experts. L'impact de ces évolutions sur les métiers y a été brièvement abordé. Mais il nécessitait d'être complété par un travail plus approfondi afin de dégager les implications concrètes et les mesures à mettre en place pour y faire face. C'est pourquoi, le Forem a entamé une série d'analyses détaillées et en profondeur de l'évolution de certains métiers identifiés comme d'avenir pour la Wallonie sur base de la méthode *Abilitic2Perform.*

Abilitic2Perfom est une méthode d'anticipation des compétences basée sur l'animation de groupes d'experts lors d'ateliers successifs et éprouvée sur une quinzaine de métiers lors de son développement dans le cadre de projets européens « Interreg IV »[2]. Cette méthode est inspirée des études relatives à la prospective stratégique, dont certains outils sont mobilisés comme l'analyse structurelle ou morphologique[3].

La démarche qui se base sur la participation d'un panel d'expert a rassemblé une dizaine de personnes issues de milieux divers, tels que la finance, l'administration publique, des fournisseurs de solutions informatiques spécialisés dans la sécurité ou encore des centres de recherche et de formation.

Le présent rapport s'intéresse à l'évolution des métiers de la sécurité de l'information. Ces métiers peuvent s'avérer très variés selon que l'on se situe au niveau technique (installation, développement, configuration,…), conceptuelle (algorithmie, mathématique,…) ou stratégique (risk manager, chief informatic security officer,…).

[1] Le Forem, Métiers d'avenir pour la Wallonie, septembre 2013, téléchargeable sur www.leforem.be .

[2] Voir www.abilitic2perform.eu

[3] Voir notamment, Godet, M., *Manuel de Prospective stratégique - Tome 1 : Une indiscipline intellectuelle*, Paris, Dunod, 2007 et Godet, M., *Manuel de Prospective stratégique - Tome 2 : L'art et la méthode*, Paris, Dunod, 2007.

Parmi ces différents niveaux d'intervention dans la sécurité de l'information, celui lié à la stratégie a particulièrement émergé durant les débats. En effet, c'est la conscience du caractère stratégique de la gestion de l'information qui semble manquer dans les entreprises ou autres organisations. Le profil recherché serait alors celui de gestionnaire de risques (risk manager) liés à la sécurité de l'information. Le rôle de ce dernier serait d'établir une stratégie en vue de réduire l'exposition de l'entreprise aux risques en matière de sécurité de l'information, tant au niveau technique (IT), qu'organisationnel (analyse des processus) ou encore juridique (analyse des contrats par exemple).

Aussi, s'agit-il bien ici de sécurité de l'information plutôt que de sécurité informatique. Certes, la sécurité de l'information est fortement liée à sa gestion informatisée, mais elle ne s'y limite pas. Non seulement l'information circule aussi via des canaux non informatisés, mais même lorsque le canal informatique est utilisé, les failles peuvent trouver leurs origines dans le comportement des individus ou des organisations. Si les évolutions technologiques tendent à accroître la capacité de nuisance des hackers, c'est aussi via l'ingénérie sociale qu'ils peuvent s'introduire dans le système quelles que soient les protections « techniques » installées. La sécurité de l'information est donc bien un enjeu stratégique pour l'entreprise, pour laquelle il s'agit de mettre en œuvre des mesures en lien avec les technologies de l'informatique, mais aussi des mesures organisationnelles, réglementaires, etc.

Enfin, bien qu'ayant gardé le vocable de « risque » en raison notamment du succès de la terminologie « risk manager », il semble que l'enjeu de la sécurité de l'information soit aujourd'hui et encore davantage demain, non pas de se prémunir de risques bien définis mais plutôt de se mettre en état de réagir à des attaques ou événements incertains. Il est finalement bien plus question de gestion de l'incertitude que des risques.

La sécurité de l'information constitue un enjeu tant pour les petites entreprises que les grandes. Si dans les grandes entreprises, chaque strate de professionnels de la sécurité de l'information peut être présente, les petites entreprises ne peuvent s'offrir ce type d'organisation, et recourent le plus souvent à des sous-traitants pour leur sécurité de l'information. L'analyse des tâches relatives à la gestion des risques liés à la sécurité de l'information, a été réalisée en distinguant l'exercice de la profession « en interne » au sein d'une entreprise ou en tant que sous-traitant. Il s'agit d'une réalité de travail différente, où dans la première, le professionnel sera davantage focalisé sur les aspects stratégiques, tandis que dans le second cas, le sous-traitant assurera également les tâches plus techniques.

Dans les deux cas, le professionnel devra conscientiser et convaincre son donneur d'ordre, soit sa hiérarchie ou son client.

La méthode utilisée, qui combine des phases d'expression libre des membres du groupe (du type d'un brainstorming) avec des phases objectivantes plus « cadrées », a permis de faire apparaître dix facteurs reconnus par les experts comme « importants »[4] et identifiés sur base d'une analyse structurelle comme « dominant »[5] le système des facteurs de changement. A chacun de ces facteurs, ont été associés des scenarios d'évolution qui permettent d'appréhender la situation à laquelle il faudra se préparer dans trois à cinq ans.

La **disponibilité de très larges bandes passantes** (+ 4G) devrait permettre une rapidité de transfert et de calcul de plus en plus importante d'ici 2017. Cela augmentera par conséquent la capacité de nuisance des hackers, qui bénéficient de moyens importants via le financement du cyber terrorisme, ou de l'industrie du hacking, ou encore en utilisant le matériel et la puissance d'autrui (le botnet[6]). A l'inverse, les départements de sécurité se retrouvent affaiblis, notamment parce que l'augmentation de la rapidité et la puissance de calcul des hackers rend difficile le monitoring des systèmes. Il en résulte un décalage entre les capacités des hackers et celles des organes de sécurité. En corollaire de cette évolution technologique, les experts ont déploré le manque de réglementation, en particulier internationale, dans le domaine.

La **technologie web** est aujourd'hui, et davantage encore demain, **omniprésente** et de plus en plus diversifiée. Cette croissance s'opère de manière plus ou moins anarchique et à plusieurs échelles : services, logiciels / appli, hardware / périphérique (GPS, camera,…). Les dispositifs de sécurité continuent à être « bricolés » sur une technologie davantage stimulée par des besoins de confort, d'individualisme, de rapidité, et de polyvalence que par les impératifs de sécurité.

Dans la foulée, les **équipements connectés**, au web mais aussi entre eux, devraient être de plus en plus nombreux : caméra, GPS, sur des téléphones mobiles mais aussi des voitures, des frigos, des pacemakers,… Le développement de ces équipements s'opère dans un climat de relative confiance des consommateurs peu conscients des conséquences en termes de sécurité de l'information. En effet, ces appareils collectent de plus en plus d'informations et communiquent entre eux.

Le mode de connexion « sans fil », qui répond davantage à des impératifs de confort, continuera à se généraliser. Cette **explosion du « sans fil »** n'est pas sans conséquence sur la sécurité de l'information. L'accès des bornes wi-fi ou « hotspot » ouverts « à tous » rend les systèmes d'information peu contrôlables. Toutefois les technologies devraient à l'avenir gagner en qualité en matière de sécurisation.

Les **innovations technologiques** devraient continuer à progresser en s'accélérant d'ici 2017. Le principal impact de cette rapidité et de cette diversité d'évolution est une difficulté de développer des normes de sécurisation des systèmes : leur développement est coûteux et tombe vite en obsolescence.

Plus en lien avec l'organisation des entreprises, les experts ont pointé le **caractère éclaté de l'informatique** dans les entreprises. Aujourd'hui déjà et encore davantage demain, l'informatique, sur laquelle repose essentiellement la gestion de l'information, n'est plus centralisée. Les différents départements disposent d'autonomie en matière d'achats de logiciels, des petits programmes sont facilement accessibles sur le net, sans compter la frontière de plus en plus floue entre les espaces professionnels et privés (cf. infra). D'ici à 2017, les organisations, les entreprises auront pris conscience de l'importance de la sécurité de l'information et lui accorderont une place centrale, sous la responsabilité du gestionnaire de risques liés à la sécurité de l'information. Celui-ci devra alors disposer d'une vue globale et d'une capacité d'agir auprès des différents départements et de l'ensemble des utilisateurs.

Sous la pression des usages privés, et la recherche d'efficacité et de confort, la **frontière entre les mondes professionnel et privé** tend à disparaître. La « consumérisation », soit l'importation des usages privés dans le monde professionnel en est une illustration. Ainsi en 2017, plus encore qu'aujourd'hui, les équipements servent aussi bien pour la vie privée que pour la vie professionnelle, mais les technologies de sécurité devront s'adapter. Des applications professionnelles avec des niveaux de sécurité élevés pourront être installées sur du matériel privé, du matériel privé pourrait être configuré pour répondre aux exigences de sécurité de l'entreprise, etc.

La **location de services standard** (ex : stockage de données sur le cloud, Office 360,…) est de plus en plus courante dans les entreprises (quelle que soit leur taille). En recourant à ces services les entreprises s'exposent à des risques qu'ils ne mesurent pas toujours, d'autant plus que le cadre réglementaire s'avère insuffisant. Les prestataires de ces services sont souvent situés à l'étranger, relevant donc de juridictions diffé-

[4] Voir partie 2, 1. Recensement des facteurs de changement les plus importants.
[5] Voir partie 2, 2. Sélection des facteurs les plus influents
[6] Le botnet (contraction de robot et réseau, network en anglais), appelé également "zombie", consiste pour le hacker à infecter un grand nombre d'ordinateurs et d'en constituer un réseau à l'insu des propriétaires afin d'utiliser ce réseau à des fins malveillantes comme saturer un serveur par exemple.

rentes en cas de conflit commercial. D'ici à 2017, ce recours à des services standard devrait être intégré dans une logique de co-responsabilité entre le client et le prestataire. Cette co-responsabilité doit être formalisée au travers de contrats ou de « Service Level Agreement », pour lesquels une expertise technique, en sus de celle juridique, sera nécessaire.

Enfin, l'importance de la **quantité de données et leur dissémination** constitue un dernier facteur de changement qui se divise en deux dimensions. La première concerne **les données de l'organisation**, qui sont disséminées en interne et en externe de l'organisation pour les raisons citées ci-avant (location de services « cloud », informatique éclatée, consumérisation,…). La gestion des données (gérer la duplication, la fin de vie,…) ainsi que leur sécurisation en sont devenues difficiles. Une autre dimension liée aux données est **leur échange et leur transformation sur le marché**. La communication de ces données est réalisée le plus souvent au travers de flux automatiques, dynamiques, et dans des volumes importants. Le contrôle de la qualité de ces données en devient difficile. Il est nécessaire de développer des méthodes qui permettent le contrôle de données venant de sous-traitants, comme l'analyse de comportements hors normes par exemple.

Pour accompagner ces évolutions, différentes actions nécessitent d'être mises en œuvre. Parmi la soixantaine identifiée, certaines relèvent plus du domaine des interpellations politiques (notamment en matière de financement de la recherche) d'autres de la sensibilisation des utilisateurs (sensibiliser les dirigeants de PME aux risques liés à la location de services standard, par exemple). De l'ensemble de ce plan d'action, il semble utile de faire ressortir en particulier trois types d'actions, indépendamment des scenarios qui les ont suscités : les actions d'orientation et de sensibilisation des (futurs) candidats, les actions de recrutement et les actions de formation.

Les **actions d'orientation et de sensibilisation** des (futurs) candidats aux métiers de la sécurité de l'information visent essentiellement à pointer l'importance d'apprendre en continu et de se former tout au long de la vie. Il s'agit déjà d'une nécessité dans de nombreux métiers sur le marché, en particulier pour les professionnels de l'informatique. Mais celle-ci devrait aller croissante dans les années à venir. Outre les candidats à ces métiers, cette exigence d'apprentissage en continu au niveau informatique devrait également concerner les enseignants et les formateurs. Les experts plaident d'ailleurs pour que davantage de professionnels de l'informatique s'orientent vers l'enseignement.

Concernant **les recrutements** ou la gestion des ressources humaines, plusieurs niveaux de métiers semblent impactés.

Au niveau « stratégique », les experts identifient le besoin de recruter des gestionnaires de risques (risk manager) liés à la sécurité de l'information, soit directement au sein de grandes structures, soit en recourant à la consultance pour les petites entreprises. Leur rôle serait d'établir une stratégie en vue de réduire l'exposition de l'entreprise aux risques en matière de sécurité de l'information, tant au niveau technique (IT), qu'organisationnel (analyse des processus) ou encore juridique (analyse des contrats par exemple).

En matière d'organisation des ressources humaines dans l'entreprise, le gestionnaire de risques (risk manager) liés à la sécurité de l'information, ou à défaut le responsable de la sécurité des systèmes d'information (RSSI), devra avoir une vue systémique de l'organisation, tant au niveau interne qu'au niveau de ses relations avec l'extérieur. Dans les organisations où les équipements informatiques sont « dispersés » et où les différentes entités bénéficient d'autonomie en la matière, ce professionnel devra être impliqué dans les choix des outils informatiques ou plus généralement de gestion de l'information.

Au niveau des profils plus techniques, il apparaît qu'à l'avenir le besoin en professionnels des infrastructures informatiques devrait diminuer avec l'intensification de l'usage des services standard et du cloud computing. A l'inverse, les professionnels de l'intégration seront davantage recherchés.

Enfin, plusieurs actions de **formation** ont été suggérées. Certaines s'adressent à l'ensemble des professionnels de la sécurité de l'information. Elles consistent essentiellement en des adaptations de formations existantes. Il faudrait, selon les experts, dès le début du cursus des futurs informaticiens (dans l'enseignement secondaire ou au début du baccalauréat), introduire les notions techniques et outils de sécurité de l'information. L'apprentissage des règlementations liées à la sécurité de l'information devrait être intégré dans la formation de base des informaticiens. Au niveau de la formation de base toujours, il s'agira d' « apprendre à apprendre », et d'habituer les futurs professionnels à se former en continu. Ils devront intégrer en permanence les nouveaux outils pour sécuriser le web. Ils devraient également apprendre à adopter une vision systémique, et être ainsi capables d'appréhender un phénomène dans sa globalité.

De manière plus spécifique aux fonctions stratégiques comme celle de risk manager, il s'agira de former à la gestion de l'incertitude. Leur rôle sera, en effet, dans l'entreprise, de passer de la gestion des changements à la gestion des incertitudes.

Quant aux personnes en charge de la sécurité informatique de manière spécifique, il semble nécessaire d'intégrer dans leur formation, les aspects organisationnels des entreprises (sociologie des organisations par exemple).

Les architectes réseaux devraient être formés à créer des architectures souples qui peuvent s'adapter aux évolutions technologiques. Cela nécessite notamment de ne plus donner la priorité à l'optimisation des systèmes mais à leur adaptabilité.

Enfin, au-delà de la formation des professionnels de la sécurité de l'information, d'autres formations nécessiteraient d'être adaptées en intégrant des éléments de sécurité de l'information dans les formations dédiées aux « informaticiens industriels » et automaticiens, et à des profils tels que les juristes, les professionnels des ressources humaines, les membres de la direction et du management, et le personnel des départements achats.

Sur base des éléments issus des débats, il a été possible d'identifier différentes tâches qui seront accomplies par les professionnels de la sécurité de l'information. Celles-ci ont notamment permis d'alimenter une liste d'une vingtaine de compétences / aptitudes attendues du futur gestionnaire de risques liés à la sécurité de l'information. Cette liste qui regroupe des compétences managériales, techniques ou encore des aptitudes ne constitue toutefois pas un référentiel de compétence formel.

Globalement, les compétences ont été jugées pertinentes par les experts. Toutefois l'importance de certaines de celles-ci tend à être considérée comme faible selon les conditions d'exercice. Ainsi lorsque le métier est exercé en interne d'une grande entreprise, les compétences « être capable de développer des applications mobiles répondant aux exigences de sécurité » et « être capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate" », s'avèrent moins pertinentes. Tandis que lorsque le professionnel intervient en sous-traitance, c'est la compétence « maîtriser le déploiement d'architecture du système d'information ouverte et souple (adaptable) » qui est considérée comme moins importante. Cela dénote d'une vision différente des métiers selon leurs conditions d'exercice. Le consultant est perçu comme apportant davantage une plus-value technique tandis que le professionnel « interne » aura la possibilité d'être au plus près de la stratégie.

Une première procédure objectivante a permis de mettre en lumière les impacts spécifiques qu'auront les scenarii d'évolution sur chacune des tâches.

A titre d'exemple, la **« connaissance des règlementations en matière de contrat commercial et de « Service Level Agreement »** sera particulièrement sensible à la location de services standard de la part des entreprises et à l'explosion de la quantité de données et leur dissémination. Les professionnels de la sécurité devront en effet être familiarisés avec ce type de contrats afin de pouvoir y apporter une lecture « technique ».

« Etre capable de développer des applications mobiles répondant aux exigences de sécurité » sera d'autant plus important que les technologies web seront omniprésentes et que de plus en plus d'appareils seront connectés. Le développement de ces applications devra, en outre, prendre en compte la mobilité des usagers connectés via des réseaux sans fil et le potentiel en matière de rapidité et de puissance de calcul généré par les technologies « large bande passante » ou 4G.

La **« maîtrise des méthodes d'analyse des (flux de) données afin d'identifier les "comportements anormaux" »**, sera d'autant plus pertinente que les flux gagneront en rapidité (large bande passante, 4G,…), et que ces données seront dispersées, dans l'organisation, et à l'extérieur, notamment sur des appareils privés.

« Etablir une politique de connexion différenciée en fonction des équipements, des applications, des réseaux utilisés et des utilisateurs », sera particulièrement nécessaire, alors que de plus en plus d'équipements de nature différente seront connectés, via des réseaux divers. Cette tâche devrait se complexifier sous l'influence du caractère éclaté des systèmes informatiques et la fusion des mondes privé et public.

Le professionnel de la sécurité de l'information devra également **« être capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate" ».** En effet, dès lors que les équipements connectés sont de plus en plus diversifiés, qu'ils sont tantôt professionnels, tantôt privés, et que les équipements informatiques de l'entreprise sont « éclatés », cela nécessite des configurations spécifiques.

« Développer des processus d'alerte et de réactions aux événements perturbateurs » deviendra plus complexe dès lors qu'il faudra intégrer dans le système « à contrôler », des appareils privés en raison de la fusion des mondes privé et professionnel.

Enfin, les compétences et aptitudes liées à **« l'apprentissage en continu »** et la **« capacité de suivre les évolutions technologiques »** en particulier sont rendues essentielles par l'accélération de l'innovation technologique, notamment en matière d'équipements connectés. Mais les pratiques des utilisateurs et les organisations des entreprises évoluent aussi et impliquent des mises à jour des connaissances de la part du professionnel. Ainsi l'organisation éclatée des systèmes informatiques, la location de services standard, ou encore la fusion des mondes privé et professionnel, nécessitent des adaptations de la part du professionnel de la sécurité de l'information.

Au terme de cet exercice prospectif, il apparaît que la sécurité de l'information constitue un enjeu pour les organisations. Sans exclure le besoin en techniciens en la matière, il ressort assez clairement que les besoins se font sentir sur le marché au niveau stratégique. Pour y répondre, un premier profil de gestionnaire de risques liés à la sécurité de l'information a pu être établi sur base d'une liste de compétences et aptitudes.

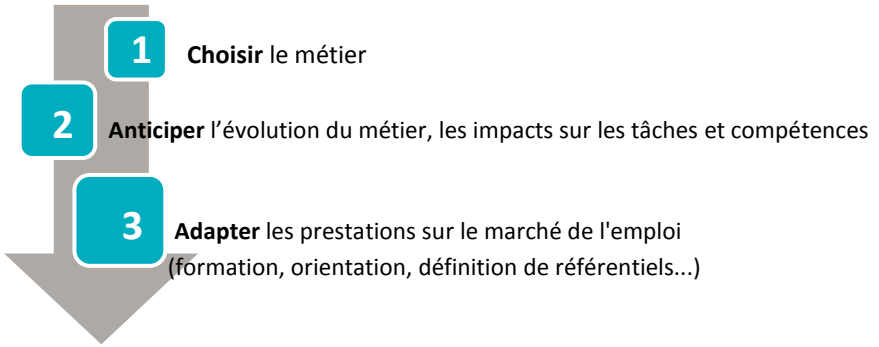
Au-delà de la nécessité pour les entreprises de disposer en son sein d'un tel professionnel ou d'y avoir recours via la sous-traitance, différentes pistes d'action ont pu être formulées afin d'accompagner l'importance stratégique que revêt aujourd'hui, et encore davantage demain, la sécurité de l'information.

PARTIE 2 : LA DEMARCHE ET LES RESULTATS PAS A PAS

Cette partie du document décrit l'ensemble du processus suivi dans le cadre du déploiement de la méthode *Abilitic2Perform* appliquée aux métiers de la sécurité de l'information.

Cette méthode repose sur une succession d'ateliers ; elle alterne d'une part des phases de réflexions créatives et collectives de type brainstorming et, d'autre part, des phases individuelles destinées à coter la pertinence ou l'impact des idées précédemment émises. Le traitement de ces cotes permet d'objectiver les éléments récoltés. Les résultats obtenus au terme de chaque phase servent de matière première à la phase suivante.

Trois grandes étapes doivent être parcourues : choisir un métier, anticiper les évolutions et leur impact sur le métier, puis adapter les prestations.



Le choix du métier a été réalisé sur base des conclusions du chapitre consacré au secteur des technologies de l'information et de la communication de la publication *Métiers d'avenir pour la Wallonie*[7]. Ces conclusions ont alimenté un premier état de l'art de la question et, moyennant un travail complémentaire, a permis d'aboutir à une première définition de ce qui avait été initialement dénommé « expert en sécurité informatique ».

Le choix du métier opéré et un premier périmètre de l'objet d'analyse tracé, il reste à identifier les membres du panel d'experts qui participeront aux ateliers d'anticipation.

Le choix des experts s'opère sur base de leur connaissance du métier. La méthode prévoit également de sélectionner des professionnels de la formation qui assureront l'appropriation des résultats dans les référentiels de formation.

Les rôles se sont répartis de la manière suivante :

- Le commanditaire est à la base de la demande et le premier bénéficiaire des résultats. Il s'agit ici du comité de direction du Forem.
- L'équipe en charge du déploiement de la méthode est composée d'un animateur, et de deux « back officers » en charge de la prise de notes et des traitements des votes. Ces rôles ont été remplis par trois personnes du Forem.
- Le rôle de formateur expert a été assumé par le responsable de ligne de produits de formation en informatique auprès du Forem.
- Les experts « métiers » sont des professionnels de la sécurité de l'information issus de milieux divers, tels que la finance, l'administration publique, de fournisseurs de solutions informatiques spécialisés dans la sécurité ou encore des centres de recherche et de formation

La suite du document reprend, étape par étape, le déroulé de la procédure d'analyse. Les étapes sont les suivantes :

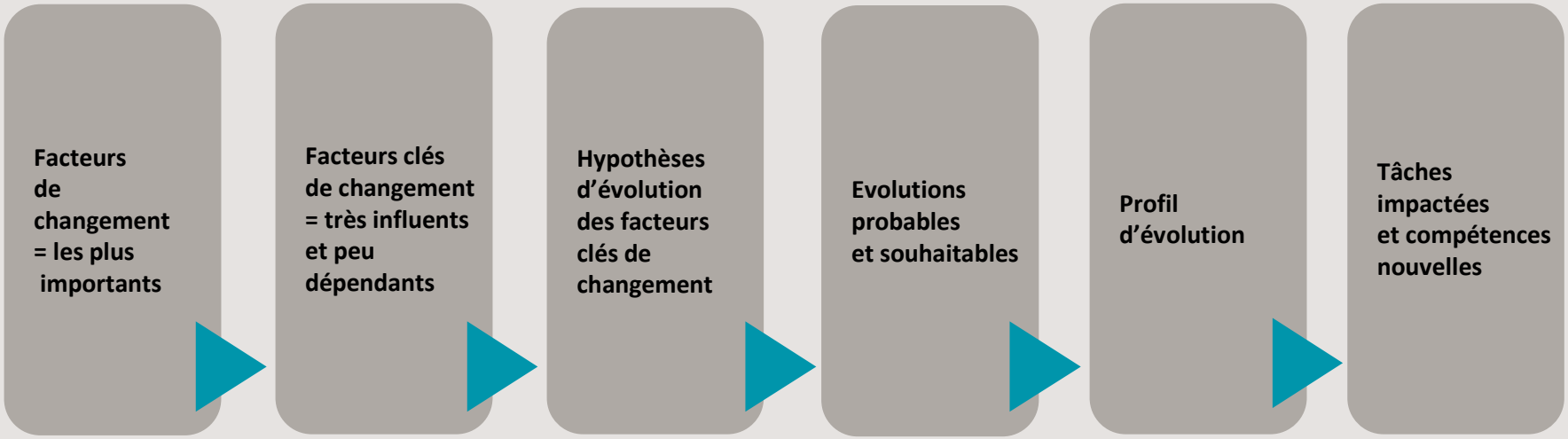
0. Le choix du métier
1. Le recensement des facteurs de changement les plus importants
2. La sélection des facteurs les plus influents
3. Les hypothèses d'évolution des facteurs clés de changement
4. Les évolutions probables et souhaitables
5. Le profil d'évolution
6. Les tâches impactées et nouvelles compétences.

Ces différentes étapes ont été réparties en 3 ateliers réunissant les experts avec des phases de consultations à distance entre les ateliers.

[7] Le Forem, Métiers d'avenir pour la Wallonie, septembre 2013, téléchargeable sur www.leforem.be

ETAPES D'ANTICIPATION

Déroulement



Relevé via brainstorming	Sélection via pondération et matrice d'influence	Projection des possibles via brainstorming	Sélection via pondération	Compromis via arbitrage (existence ou non d'actions proactives)	Définition via matrice d'impact

0. Le choix du métier[8]

Lors du premier atelier réunissant les experts, l'intitulé initial du métier, « expert en sécurité informatique » et le périmètre qui en était tracé (une première proposition de référentiel de tâches) ont suscité plusieurs questions et réactions.

Par rapport à l'intitulé, « expert en sécurité informatique », il est apparu que le terme pouvait recouvrir **des métiers très différents**, selon que l'on place l'expertise au niveau technique (installation, développement, configuration…), conceptuelle (algorithmie, mathématique…) ou stratégique (Risk manager, Chief informatic security officer…).

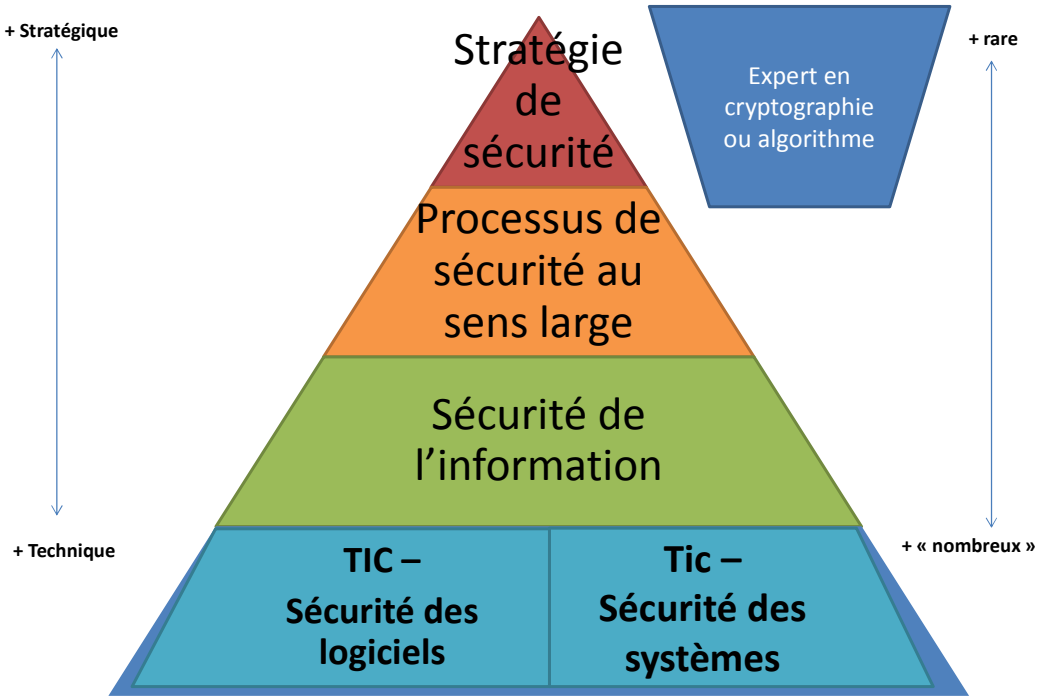
En ce qui concerne les tâches listées, les experts ont souhaité ajouter une **dimension stratégique** au profil, en raison de l'importance pour les entreprises que peut représenter la sécurité de l'information.

Enfin, à la sécurité informatique, les experts ont préféré la notion de sécurité de l'information. Certes l'ampleur de l'enjeu lié à la sécurité de l'information est fortement liée à la gestion informatisée de l'information, mais ne s'y limite pas. Non seulement l'information circule aussi via des canaux non informatisés, mais même lorsque le canal informatique est utilisé, les failles peuvent trouver leurs origines dans le comportement des individus. **L'enjeu est alors plutôt « social » que « technique »**. Aborder l'information par le seul prisme des technologies informatiques ne permet d'appréhender que partiellement le phénomène.

Les enjeux de la sécurité de l'information peuvent toucher plusieurs métiers en fonction des types d'interventions nécessaires, ou selon le type d'entreprise. Certaines grandes structures comptent différents professionnels couvrant la palette d'interventions allant du niveau stratégique à l'acte technique. Tandis que dans certaines structures plus petites, ou encore dans le cadre d'un intervenant externe (sous-traitant), le professionnel doit agir sur l'ensemble des niveaux de la sécurité informatique.

Faute de pouvoir s'arrêter sur un seul métier, il a été décidé de soumettre à l'analyse prospective l'ensemble de la gamme d'intervention en matière de sécurité de l'information, modélisée en différentes strates.

Expert / gestionnaire de la sécurité de l'information : pyramide des profils



[8] Cette phase s'est déroulée lors du premier atelier, dit « atelier 0 », en compagnie des experts, le 13 janvier2014.

1. Le recensement des facteurs de changement les plus importants[9]

L'anticipation des facteurs de changement, c'est-à-dire la détermination des facteurs clés de l'évolution des métiers de la sécurité de l'information s'effectue, selon la méthodologie *Abilitic2Perform*, en deux étapes : le recensement des facteurs de changement puis la sélection des plus importants parmi ceux-ci.

L'objectif de la première étape est d'établir une liste la plus exhaustive possible, de facteurs de changement. Ces facteurs correspondent soit à des variables, qui avaient, ont et auront encore de l'influence sur le métier demain, soit encore à des variables qui n'ont pas d'effet en 2014 mais qui en auront demain. Ces facteurs-clés sont recensés lors d'un brainstorming durant lequel les experts donnent des éléments de réponse à la question : « *Quels sont les facteurs qui vont, selon vous, influencer le métier de gestionnaire de risques d'ici 3 à 5 ans ?* »

Au total, 47 facteurs ont pu être listés[10]. Afin de poursuivre la démarche sur un nombre plus restreint, et relativement aux facteurs jugés les plus importants, il a été demandé aux experts de procéder à un vote pondéré selon les modalités de la méthode *Abilitic2Perform*.

Après consolidation et traitement des votes, en retenant notamment les éléments ayant reçus le plus de points et le plus de suffrages, 20 facteurs déterminants ont pu être identifiés :

1. Industrialisation du hacking.
2. Fusion des mondes professionnel/privé.
3. Usage trop confiant des nouveaux outils informatiques par les nouvelles générations.
4. Réglementations UE et national sur l'usage de l'information.
5. Explosion de la quantité de données et leur dissémination.
6. Accroissement du cyber activisme (hacktivisme)/cyber terrorisme.
7. Prendre en compte le rôle accru de l'utilisateur dans la sécurité.
8. Consumérisation : importation des usages personnels dans le monde professionnel.
9. Explosion du sans fil.
10. Accélération des innovations technologiques.
11. Analyse des déviances par rapport aux comportements normaux.
12. Location de services standard.
13. Disponibilité de très larges bandes passantes avec une puissance de calcul élevée.
14. Accroissement de la complexité des menaces impliquant le développement de la sécurité analytique.
15. Informatique « éclatée ».
16. Manque de régulation imposée aux fournisseurs.
17. Omniprésence de la technologie web.
18. Essoufflement de la cryptographie et des normes de sécurité.
19. Hausse des équipements mobiles connectés.
20. Garantir l'identité de son interlocuteur.

[9] « Atelier 1 », 13 janvier 2014.

[10] 28 cités en séance, 19 ajoutés dans un second temps via un prolongement du brainstorm à distance par courrier électronique.

2. La sélection des facteurs les plus influents[11]

Après avoir choisi les 20 facteurs les plus importants, il a été demandé aux experts de se prononcer sur l'impact qu'ont chacun de ces facteurs sur les autres (analyse structurelle). Les experts ont rempli une matrice en cotant l'influence des facteurs en lignes sur ceux en colonnes.

Chaque facteur se voit ainsi attribuer une cote de dépendance et d'influence. La sélection des facteurs dominants a été réalisée sur base de trois critères :

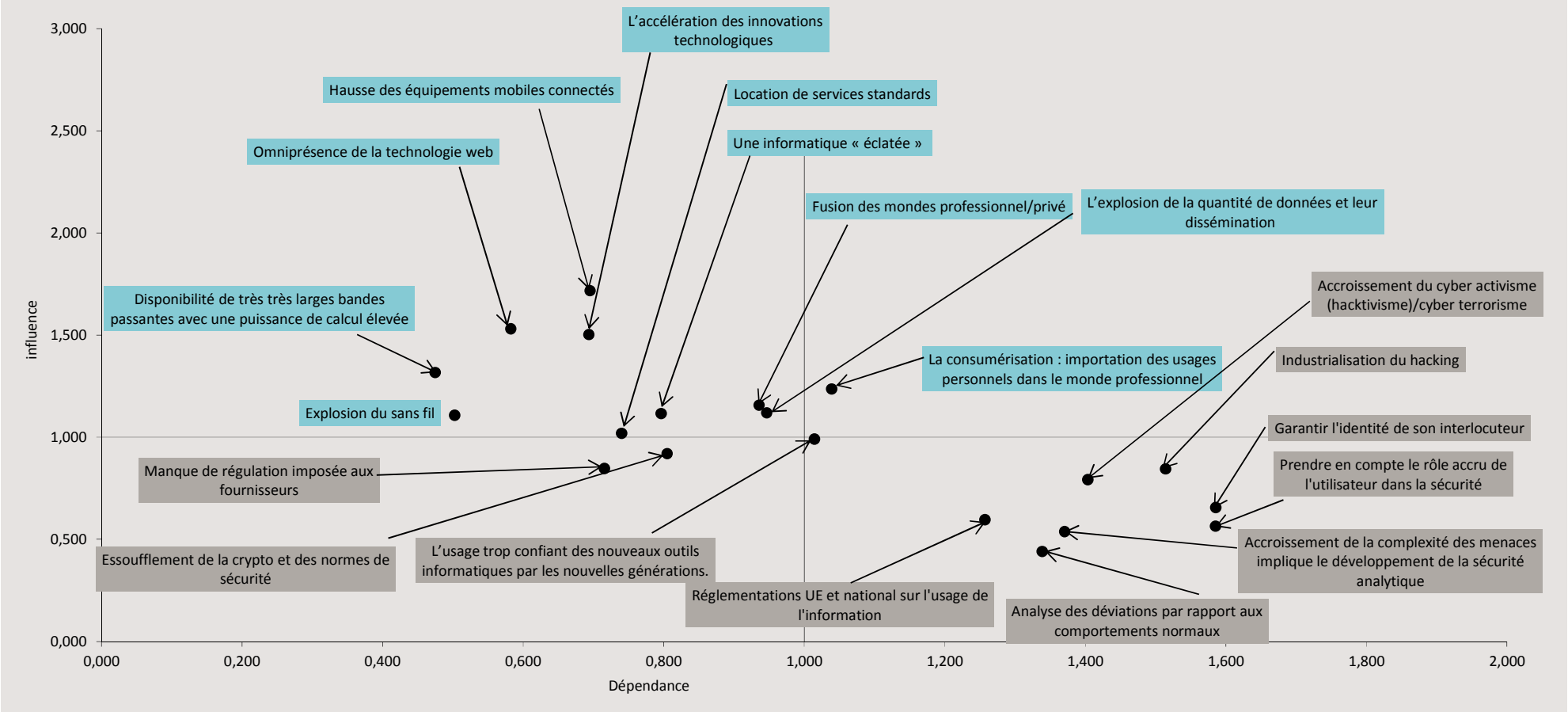
A. D'abord les facteurs simultanément très influents et peu dépendants,
B. Ensuite les facteurs les moins dépendants et à influence moyenne,
C. Ensuite les facteurs les plus influents et à dépendance moyenne.

Les dix facteurs les plus influents recensés sont :

1. Disponibilité de « très larges » bandes passantes avec une puissance de calcul élevée.
2. Omniprésence de la technologie « web ».
3. Hausse des équipements mobiles connectés.
4. Explosion du « sans fil ».
5. Accélération des innovations technologiques.
6. Informatique « éclatée ».
7. Location de services standard.
8. Fusion des mondes professionnel/privé.
9. Consumérisation : importation des usages personnels dans le monde professionnel.
10. Explosion de la quantité de données et leur dissémination.

[11] Réalisée à distance par courrier électronique.

Représentation graphique des facteurs de changement en fonction de leur influence et dépendance sur le système de facteurs



Note de lecture : En bleu, les facteurs retenus lors de l'analyse structurelle permettant la sélection des facteurs influents.

Le quadrant supérieur gauche reprend les facteurs dominants, soit ceux très influents et peu dépendants. En bas à droite, il s'agit des « variables résultats », soient les facteurs avec une forte dépendance et peu d'influence. Ces facteurs sont écartés de la suite des travaux car ils sont déterminés par d'autres facteurs dont leur évolution dépend. Le quadrant supérieur droit reprend les facteurs à la fois dépendants et influents, appelés en analyse structurelle, les facteurs relais.

Ils sont sujets à des boucles de rétroaction lorsqu'on agit dessus (leur évolution modifie un autre facteur qui lui-même directement ou indirectement vient modifier le facteur sur lequel on tente d'agir). Ce type de facteur n'est pas rejeté automatiquement. Certains dont les valeurs sont proches des moyennes peuvent être réintégrés après arbitrage avec le groupe d'experts, cela a été ici le cas pour le facteur « consumérisation ». Enfin le dernier quadrant, celui en bas à gauche reprend les facteurs qualifiés d'exogènes, soit des facteurs peu reliés aux autres, tant en termes d'influence que de dépendance. Ce type de facteur est habituellement rejeté en analyse structurelle.

3. Les hypothèses d'évolution des facteurs clés de changement[12]

Une fois que les 10 facteurs les plus influents ont été sélectionnés, il s'agit de préciser leur évolution. Pour ce faire, il a été demandé aux experts de décrire la situation actuelle et future (dans 3 à 5 ans) de chaque facteur. L'exercice s'effectue sous la forme d'un brainstorming.

En filigrane des réponses à ces questionnements apparaissent des phénomènes transversaux aux facteurs : un rythme d'évolution technologique effréné, stimulé par la recherche de confort et de rapidité pour l'utilisateur, tant au niveau de l'individu qu'au niveau des organisations et des entreprises, le tout dans un contexte règlementaire marqué par un manque de (volonté de) coordination internationale et une incapacité à suivre la rapidité des évolutions. La sécurité de l'information apparaît comme un enjeu stratégique des états et des organisations, dans un climat de risque dont l'émergence, la nature, l'origine ou l'ampleur sont difficiles à appréhender tant l'environnement semble dominé par l'incertitude.

Par rapport à l'articulation présent-futur, il est ressorti, la plupart du temps, que les tendances identifiées aujourd'hui étaient amenées à s'amplifier à l'avenir, même si quelques ruptures radicales ne peuvent être exclues, comme l'effondrement de l'internet. L'étape suivante a pour objectif de formaliser différents scenarios d'évolution.

4. Les évolutions probables et souhaitables[13]

Sur base des éléments recueillis lors de l'étape précédente, l'animateur et les back officers ont formulé, pour chaque facteur, plusieurs scenarios d'évolution. Il est assez vite ressorti de l'analyse du précédent brainstorming que nombre de facteurs étaient traversés d'axes d'évolutions différentes. Les différents scenarios ont donc été construits de manière à prendre en compte, autant que possible, ces différents axes. Enfin, le relevé des situations présentes et à venir (étape précédente) et leur scénarisation, ont permis de repréciser le contour de certains facteurs. Ainsi est-il apparu nécessaire de fusionner le facteur « consumérisation » avec celui « fusion des mondes privés et professionnels », et de dupliquer le facteur « explosion de quantité de données et dissémination » selon que l'on aborde les données au sein de l'organisation ou celles échangées entre organisations, notamment comme valeur sur le marché.

[12] « Atelier 2 », le 10 février 2014

[13] Réalisées à distance par courrier électronique

Ces scenarios ont ensuite été soumis au vote des experts qui étaient invités à attribuer une première fois une cote afin de qualifier le caractère probable du scenario (1 signifiant que le scenario est très peu probable ; 4 signifiant que le scenario est très probable), et une seconde fois pour qualifier le caractère souhaitable du scenario (1 = très peu souhaitable ; 4 = très souhaitable).

Les différents scenarios d'évolution sont repris dans la section suivante.

5. Le profil d'évolution[14]

5.1. Scenario probable et souhaitable

Après avoir compilé les résultats des différents experts, les hypothèses d'évolution qui ont obtenu le score le plus élevé distinctement en matière de probabilité (en rose dans l'illustration ci-dessous) ou de souhaitabilité (en bleu dans l'illustration ci-dessous) ont été retenues.

[14] « Atelier 3 », le 26 février 2014

Facteurs de changement	Hypothèses d'évolution des variables clés à l'horizon 2017			
	A	B	C	D
Disponibilité de très larges bandes passantes (+ 4G) avec une puissance de calcul élevée	Retour vers des modes de **connexions plus lents** et des puissances de **calculs plus faibles.**	La puissance de calcul et la rapidité de surf (via 4 G ou larges bandes passantes) **continuent à progresser**. Cette évolution augmente la capacité de nuisance des hackers (renforcée par ailleurs grâce au botnet ou à l'anonymisation sur le net) tandis que les départements de sécurité se retrouvent affaiblis (notamment en matière de monitoring). Il en résulte un décalage entre les capacités des hackers et celles des organes de sécurité.	La puissance de calcul et la vitesse de surf continuent à progresser faisant de l'internet un enjeu d'état. Les règlementations sont renforcées, les data centers sont relocalisés (également pour des raisons techniques vu que les connexions de « proche en proche » sont meilleures que celles intercontinentales). **L'internet devient à ce point stratégique**, notamment pour les états, que l'on parle de cyber-guerre.	**Internet s'effondre !** Plus de connexions plus de services web. Le système a atteint ses limites.
Omniprésence de la technologie web	Les technologies web continuent à accroitre leur présence et leur diversité de manière plus ou moins anarchique. Les évolutions de la technologie web se font à plusieurs échelles : services, logiciels / appli, hardware/périphérique (GPS, camera,…). **Les dispositifs de sécurités continuent à être « bricolés »** sur une technologie davantage stimulée par des besoins de confort, d'individualisme, de rapidité et de polyvalence que par les impératifs de sécurité. Il existe des protocoles de sécurité mais ceux-ci sont peu compris, ils délivrent, par exemple, des messages d'erreurs incompréhensibles.	Les technologies web continuent à accroitre leur présence et leur diversité de manière plus ou moins anarchique. Les technologies de sécurité continuent à accuser un retard (excepté peut-être dans des secteurs de pointe comme l'armée ou les banques). **Toutefois les développeurs et les utilisateurs auront une meilleure maîtrise de la sécurité sur le web.**	Les technologies web continuent à accroitre leur présence et leur diversité de manière plus ou moins anarchique. Les technologies de sécurité continuent à accuser un retard (excepté peut-être dans des secteurs de pointe comme l'armée ou les banques). **Toutefois la règlementation évolue, dotant le marché de certifications reconnues et fiables.**	**Les technologies de sécurité du web des secteurs de pointe sont généralisées** au reste des domaines malgré leur diversité.
Hausse des équipements mobiles connectés	**Marche arrière technologique** face aux risques liés aux objets connectés. Les appareils mobiles, et autres équipements, à présents connectés, le sont de moins en moins.	Applications/équipements (camera, GPS sur mobiles, mais aussi pacemaker, frigo …) **connectés continuent à se développer librement, dans un climat de confiance** des consommateurs au détriment de la sécurité. Ces équipements / appareils collectent de plus en plus de données de nature diverses et communiquent entre eux .	Applications/équipements (camera, GPS sur mobiles, mais aussi pacemaker, frigo …) connectés continuent à se développer. **Développeurs et utilisateurs sont sensibilisés à la sécurité et adaptent leurs pratiques en adoptant une attitude moins « confiante ».**	Applications/équipements (camera, GPS sur mobiles, mais aussi pacemaker, frigo …) connectés continuent à se développer. **Mais les législations et protocoles évoluent pour cadrer davantage les applis et fonctionnalités.** Des applis / fonctionnalités hyper sécurisées apparaissent sur le marché.

Facteurs de changement	Hypothèses d'évolution des variables clés à l'horizon 2017			
	A	B	C	D
Explosion du sans fil	**Les connexions sans fil ne sont plus du tout sécurisées** (crypto essoufflée), mais les **utilisateurs continuent à l'utiliser** sans être conscients des dangers.	L'utilisateur continue à utiliser les connexions sans fil en toute confiance grâce aux **nouvelles technologies qui s'avèrent plus sécurisées.**	Les usagers prennent conscience des enjeux liés à la sécurisation **et optent pour des connexions « câblées »,** plus sécurisées que les connexions sans fils.	
Accélération des innovations technologiques	La technologie évolue de manière rapide et diversifiée. Dans ce contexte, **le coût des normes de sécurisation et l'obsolescence rapide empêchent leur développement.**	L'évolution technologique est bridée/contenue, **la sortie d'une nouvelle technologie est conditionnée au développement de standards de sécurité.**	Les normes de sécurité/certifications suivent le rythme de l'évolution technologique	
Une informatique « éclatée »	**Retour vers un réseau contrôlé** : les services extérieurs au réseau de l'entreprise sont limités, tandis que les services internes sont soumis à un contrôle centralisé.	L'informatique est de plus en plus éclatée entre différents services. Le **security manager n'a plus de vue d'ensemble.**	L'informatique est toujours aussi éclatée. Dans ce contexte**, les organisations prennent conscience de l'importance de la sécurité et lui accorde une place centrale/stratégique**.	L'informatique est toujours aussi éclatée, les membres des organisations, les individus sont de plus en plus conscientisés aux risques liés aux services extérieurs. **Les bonnes pratiques sont adoptées au niveau individuel.**
Location de services standards	**Les entreprises /organisations / individus n'ont plus recours à des services standardisés** externes afin de maîtriser leur sécurité.	Les organisations / particuliers continuent à avoir **recours à des services standardisés externes, les organisations perdent le contrôle de la sécurité de leurs données**. Le cadre juridique est insuffisant pour garantir la confiance et la sécurité et le plus souvent établit à n niveau « national » rendant difficile toute procédure de règlement de conflit a posteriori.	Les organisations / particuliers continuent à avoir recours à des services standardisés externes, mais ces recours se font dans le cadre d'une coresponsabilité entre le sous-traitant et le client créant un **chaîne de confiance.**	Les organisations / particuliers continuent à avoir recours à des services standardisés externes, dans un **cadre juridique international** garantissant un niveau de sécurité a priori, et une facilité de règlement de conflit a posteriori.
Fusion des mondes professionnel/privé / La consumérisation : importation des usages personnels dans le monde professionnel	Pour des raisons de sécurité et / ou de meilleur équilibre entre la vie privée et professionnelle des travailleurs, **la frontière entre outils de travail** (appareil mobile, messagerie, extranet,…) **et outils privés** est réaffirmée. Les outils de travail sont utilisés sur le lieu de travail pendant le temps de travail, les outils privés sont utilisés hors du lieu et du temps de travail.	Les **outils privés ne sont plus autorisés sur le lieu de travail** (la fin du BYOD BYOA), tandis que les **outils de travail utilisés à l'extérieur sont davantage « bridés ».**	Les équipements mobiles servent aussi bien pour la vie professionnelle que pour la vie privée dans un **fragile équilibre entre sécurité et efficacité.**	Les équipements mobiles servent aussi bien pour la vie professionnelle que pour la vie privée **dans un contexte de technologie de la sécurité optimal écartant tous danger.**

Facteurs de changement	Hypothèses d'évolution des variables clés à l'horizon 2017			
	A	B	C	D
L'explosion de la quantité de données et leur dissémination (données dans l'organisation)	Les données d'une organisation sont disséminées en interne et en externe de l'organisation. Rendant leur gestion (duplication, durée de vie de l'information, ..) et sécurisation difficiles.	La gestion et la sécurisation des données est **(re)centralisée** au sein de l'organisation.		
L'explosion de la quantité de données et leur dissémination (données comme valeur transformée et échangée sur le marché)	La profusion et la diversité de données tend à rendre ces données peu fiables. **Les organisations se recentrent sur des données plus ciblées, plus contrôlables.**	Les données sont de plus en plus diversifiées et sont des biens qui se transforment et s'échangent. La communication de ces données est réalisée le plus souvent au travers de flux automatiques. C'est d'autant plus vrai que ces données sont échangées dans des volumes importants et sont dynamiques. Le contrôle de la qualité de ces données en devient difficile. Il est nécessaire de **développer des méthodes qui permettent le contrôle de données venant de sous-traitant** (analyse des comportements hors norme par exemple).	Les données sont de plus en plus diversifiées et sont des biens qui se transforment et s'échangent. La communication de ces données est réalisée le plus souvent au travers de flux automatiques. C'est d'autant plus vrai que ces données sont échangées dans des volumes importants et sont dynamiques. Le contrôle de la qualité de ces données en devient impossible. **La sécurité et la fiabilité sont alors seulement garanties par la chaîne de confiance entre le sous-traitant et le client via des dispositifs contractuels ou règlementaires.**	

Note de lecture : Les scenarios surlignés en rose sont ceux ayant obtenu le score le plus élevé quant au caractère probable, tandis que ceux surlignés en bleu, sont ceux ayant obtenus le score le plus élevé quant à leur caractère souhaitable. Sont encadrés en rouge les scenarios choisis par les experts.

L'étape suivante pour la rédaction du profil d'évolution est de procéder à un arbitrage entre le scenario probable et le souhaitable. Le scenario souhaitable sera maintenu s'il est possible de mettre en œuvre des actions permettant de l'atteindre. Dans le cas inverse, ce sera le scenario probable qui sera choisi. Les scenarios sélectionnés sont ceux encadrés en rouge ci-dessus.

Face à ces scenarios d'évolution, il a été demandé aux experts de proposer des actions à mener afin de se préparer au changement ou d'en faciliter l'émergence.

Afin de stimuler les interventions, il a été suggéré aux experts de proposer des actions de formation (formation de base ou continue), d'orientation (ou sensibilisation des futurs candidats), de recrutement, de communication (information et sensibilisation des utilisateurs), ou encore d'interpellation politique.

Il était demandé aux experts d'identifier, quand cela était possible, le type de professionnel de la sécurité de l'information concerné par l'action, voire les tâches ou compétences qui pourraient évoluer ou émerger.

5.2. Le plan d'action

Ci-après, est repris l'ensemble des actions proposées par facteur d'évolution et type d'actions.

Disponibilité de très larges bandes passantes (+ 4G) avec une puissance de calcul élevée

■ SCENARIO :

En 2017, la puissance de calcul et la rapidité de surf (via 4G ou larges bandes passantes) continuent à progresser. Cette évolution augmente la capacité de nuisance des hackers (renforcée par ailleurs grâce aux botnet ou à l'anonymisation sur le net) tandis que les départements de sécurité se retrouvent affaiblis (notamment en matière de monitoring). Il en résulte un décalage entre les capacités des hackers et celles des organes de sécurité.

⇨ **Scenario probable**

Il faut ici noter que le scenario souhaitable rejeté, mentionnait un renforcement des règlementations et une prise de conscience du caractère stratégique de la sécurité de l'information pour les états et les organisations. Bien qu'il n'ait pas été sélectionné, ce scenario n'est pas apparu improbable, les experts s'attendant en effet à un renforcement des règlementations en matière de sécurité. Au-delà de l'évolution essentiellement technologique reprise dans le scenario, les débats qui ont alimenté les actions ci-dessous ont pris en compte les enjeux connexes que sont les règlementations en la matière et le contexte de quasi « cyber-guerre » qui nécessitent une mobilisation au-delà des seuls professionnels de la sécurité de l'information.

■ ACTIONS :

Formation de base ou continue

- **Intégrer dès le début du cursus** des futurs informaticiens, les notions, techniques et outils de **sécurité de l'information** (durant l'enseignement secondaire ou au début du baccalauréat).
- Intégrer dans la formation des futurs informaticiens, l'apprentissage des **règlementations liées à la sécurité** de l'information.
- Intégrer dans la formation des futurs informaticiens les **aspects organisationnels des entreprises** (sociologie des organisations par exemple).
- Assurer la **formation continue des enseignants** aux techniques de sécurité de l'information et les sensibiliser aux risques actuels.
- Former à la **gestion de l'incertitude** des professionnels de la gestion des risques. Leur rôle sera dans l'entreprise de passer de la gestion des changements à la gestion des incertitudes.
- Intégrer des éléments de **sécurité de l'information** dans les formations dédiées aux profils autres qu'informatiques, soit **les juristes, les professionnels des ressources humaines, les membres de la direction et du management, et le personnel des départements achats** (qui doivent notamment en tenir compte dans les appels d'offres).

Orientation / sensibilisation des futurs candidats

- Orienter davantage de **professionnels de l'informatique vers les métiers de l'enseignement**.
- Inciter les professionnels à se former **tout au long de la vie**, de sorte qu'ils puissent mettre à jour leurs connaissances en matière de sécurité de l'information.

Recrutement et gestion des ressources humaines

- Recruter dans les entreprises, ou recourir à via la consultance, des **risk managers** dont le rôle est d'établir une stratégie en vue de réduire l'exposition de l'entreprise aux risques en matière de sécurité de l'information, tant au niveau technique (IT), qu'organisationnel (analyse des processus) ou encore juridique (analyse des contrats par exemple).

Communication : Information / sensibilisation des utilisateurs (clients, particuliers, organisations,…)

- Sensibiliser à la sécurité de l'information les profils autres qu'informatiques, soit les **juristes, les professionnels des ressources humaines, les membres de la direction et du management, et le personnel des départements achats.**

Interpellation politique

- Interpeller le monde politique et faire pression pour **obtenir davantage de réglementation**, même s'il est peu probable que celle-ci soit homogène au niveau international.

Tâches / compétences

- Formaliser un profil de compétences du risk management qui intègre la **gestion de l'incertitude** (méthodes d'intelligence stratégique).

Omniprésence de la technologie web

SCENARIO :

En 2017, les technologies web continuent à accroitre leur présence et leur diversité de manière plus ou moins anarchique. Les évolutions de la technologie web se font à plusieurs échelles : services, logiciels/applications, hardware/périphérique (GPS, caméra…). Les dispositifs de sécurité continuent à être « bricolés » sur une technologie davantage stimulée par des besoins de confort, d'individualisme, de rapidité et de polyvalence que par les impératifs de sécurité. Il existe bien des protocoles de sécurité mais ceux-ci sont peu compris, ils délivrent, par exemple, des messages d'erreurs incompréhensibles.

⇨ **Scenario probable**

ACTIONS :

Formation de base ou continue

- Former les futurs « techniciens », durant leur formation de base, à « apprendre à apprendre », à se former en continu. Ils devront intégrer en permanence les nouveaux outils pour sécuriser le web. Il s'agit donc d'inculquer à ces professionnels des compétences à l'apprentissage en continu. En même temps les formations de base doivent être adaptées de manière plus réactive.

Orientation / sensibilisation des futurs candidats

- Sensibiliser les (futurs) professionnels, notamment les techniciens, à la nécessité d'être capable d'apprendre en continu et donc de se former tout au long de la vie.

Recrutement et gestion des ressources humaines

- Recruter dans les centres de recherches, des experts en développement de dispositifs de sécurité de l'information (mathématiciens, cryptographes…).

Interpellation politique

- Soutenir la recherche dans les techniques de sécurité de l'information, financer des centres de recherche et lancer des appels à projets de programmes de recherche.
- Etablir des ponts entre le monde de la recherche et les entreprises via, par exemple, la création d'un cluster « TIC » avec un sous-ensemble « sécurité ». Ce cluster permettrait de faire émerger des solutions plus transversales.

Hausse des équipements connectés

SCENARIO :

En 2017, applications/équipements connectés (caméra, GPS sur mobiles, mais aussi pacemaker, frigo…) continuent à se développer librement, dans un climat de confiance des consommateurs au détriment de la sécurité. Ces équipements / appareils collectent de plus en plus de données de nature diverses et communiquent entre eux.

⇨ **Scenario probable**

ACTIONS :

Formation de base ou continue

- Intégrer dans la formation des « informaticiens industriels » et automaticiens, des notions de sécurité des systèmes d'information.

Communication : Information / sensibilisation des utilisateurs (clients, particuliers, organisations,…)

- Sensibiliser les entreprises aux risques liés aux appareils mobiles et aux connections ouvertes.
- Sensibiliser les utilisateurs à la gestion des mots de passe et à l'utilisation de leur « identité électronique ».
- Sensibiliser les informaticiens « industriels », automaticiens… aux enjeux de la sécurité de l'information.

Interpellation politique

- Légiférer sur les identités électroniques, les connections et les protocoles.
- Financer la recherche en lien avec l'industrie, sur le modèle de clusters ou de pôle de compétitivité afin de mieux faire le lien entre sécurité de l'information et développement industriel d'objets connectés.

Tâches / compétences

- Sensibiliser l'entreprise (par le risk manager) à la nécessité de règlementer les connections et utilisations des équipements mobiles privés sur le lieu de travail.

Explosion du « sans fil »

SCENARIO :

En 2017, l'utilisateur continue à utiliser les connexions sans fil en toute confiance grâce aux nouvelles technologies qui s'avèrent plus sécurisées.

⇨ **Scenario probable**

Ce scenario est qualifié de plus probable. Toutefois un surprenant retournement de l'évolution technologique pourrait se produire, par exemple si une « étude objective » démontrait des effets néfastes sur la santé humaine des ondes wi-fi.

ACTIONS :

Formation de base ou continue

- Inculquer pendant la formation de base de l'ensemble des professionnels de la sécurité de l'information, une réflexion systémique qui appréhende un phénomène dans sa globalité, la connectivité sans fil tendant à ouvrir les environnements.
- Intégrer la gestion de l'incertitude dans la formation des risk manager.

Tâches / compétences

- Sensibiliser les utilisateurs, (par le risk manager) à l'usage des connexions sans fil, particulièrement en-dehors des murs de l'organisation, tout en tenant compte des besoins des utilisateurs.
- Inciter le management à réglementer l'usage des connexions sans fil par les utilisateurs de l'organisation. Par exemple admettre certaines connexions et pas d'autres. (risk manager).
- Implémenter (par le risk manager) d'une politique de connexion applicable aux membres de l'entreprise.

Accélération des innovations technologiques

SCENARIO :

En 2017, la technologie évolue de manière rapide et diversifiée. Dans ce contexte, le coût des normes de sécurisation et l'obsolescence rapide empêchent leur développement.

⇨ **Scenario probable**

ACTIONS :

Formation de base ou continue

- Former les professionnels de l'IT à créer des architectures souples qui peuvent s'adapter aux évolutions technologiques. Cela nécessite notamment de ne plus donner la priorité à l'optimisation des systèmes mais à leur adaptabilité.

Communication : Information/sensibilisation des utilisateurs (clients, particuliers, organisations…)

- Sensibiliser les utilisateurs aux risques que peuvent recouvrir certaines nouvelles technologies.
- Sensibiliser les pouvoirs publics aux risques que peuvent recouvrir certaines nouvelles technologies, afin, notamment, qu'ils ne mettent pas en place des systèmes dont l'architecture est incontrôlable comme les réseaux wi-fi publics.

Tâches / compétences

- Veiller les nouvelles technologies et intégrer (choix d'accepter ou refuser une technologie) les plus pertinentes en fonction de la stratégie de sécurité (rôle du risk manager).
- Analyser l'impact des évolutions technologiques sur la sécurité de l'information.

Une informatique « éclatée »

- **SCENARIO :**

En 2017, l'informatique est toujours aussi éclatée. Dans ce contexte, les organisations prennent conscience de l'importance de la sécurité et lui accordent une place centrale/stratégique.

⇨ **Scenario probable**

- **ACTIONS :**

Recrutement et gestion des ressources humaines

- Assurer une vision systémique de l'organisation au risk manager ou au responsable en sécurité des systèmes d'information.
- Impliquer le risk manager ou le RSSI dans le choix des outils IT / de gestion de l'information, dans chacune des entités d'une organisation.

Location de services standard

- **SCENARIO :**

En 2017, les organisations / particuliers continuent à avoir recours à des services standardisés externes, mais ces recours se font dans le cadre d'une co-responsabilité entre le sous-traitant et le client créant un chaîne de confiance.

⇨ **Scenario probable**

- **ACTIONS :**

Formation de base ou continue

- Former les juristes d'entreprises/responsables achats au volet sécurité IT.

Information / sensibilisation des utilisateurs (clients, particuliers, organisations,…)

- Sensibiliser les juristes d'entreprises/responsables des achats au volet sécurité IT.
- Sensibiliser les dirigeants de PME aux risques liés à la location de services standard.

Recrutement et gestion des ressources humaines

- Faire analyser les contrats de location de services par un responsable expert en sécurité IT.

Tâches et compétences

- Analyser les contrats de location de services par un responsable expert en sécurité IT.
- Intégrer des clauses sécurité propres à l'organisation dans les contrats de location de services standard.
- Intégrer les nouveaux risques impliqués par la location de services standard.
- Réévaluer les effets sur la sécurité lors des mises à jour des contrats.
- Analyser le degré d'acceptabilité des risques.

Fusion des mondes professionnel/privé - La consumérisation : importation des usages personnels dans le monde professionnel

- **SCENARIO :**

En 2017, les équipements mobiles servent aussi bien pour la vie professionnelle que pour la vie privée dans un contexte de technologie de la sécurité optimale écartant tout danger.

⇨ **Scenario souhaitable**

- **ACTIONS :**

Tâches / compétences

- Identifier les applications professionnelles supportées sur le matériel privé (et inversement).
- Adapter la configuration des appareils privés à l'univers professionnel et ses exigences en termes de sécurité (et inversement).
- Identifier le type de matériel privé autorisé au travail (et inversement).
- Penser le système d'information de manière élargie (domicile du travailleurs, wi-fi public…) notamment en intégrant des appareils mobiles dans l'architecture.
- Développer des applications mobiles entreprises avec un niveau de sécurité adapté aux usages professionnels (développeurs).
- Centraliser les données et ne permette leur lecture qu'en streaming (les appareils mobiles comme des terminaux).
- Contribuer à établir la politique d'organisation du travail.

L'explosion de la quantité de données et leur dissémination (données dans l'organisation)

■ **SCENARIO :**

En 2017, les données d'une organisation sont disséminées en interne et en externe, rendant leur gestion (duplication, durée de vie de l'information...) et sécurisation difficiles.

⇨ **Scenario probable**

■ **ACTIONS :**

Recrutement et gestion des ressources humaines

- Recruter moins de personnel pour travailler sur « l'infrastructure ».
- Recruter davantage de personnel dont le profil est axé sur l'intégration.

Information / sensibilisation des utilisateurs (clients, particuliers, organisations,…)

- Sensibiliser la hiérarchie ou le client aux risques liés à l'externalisation du stockage de données, notamment en estimant le coût du risque lié à la dépendance à la connexion, ou en comparant le coût selon que l'on externalise ou internalise les données.

Tâches/ compétences

- Pouvoir convenir d'un « Service Level Agreement » avec le prestataire, ce qui nécessite des connaissances techniques et juridiques ainsi qu'une capacité de négociation.
- Adapter l'architecture du système d'information en y intégrant le stockage et/ou le traitement externalisé(s).

L'explosion de la quantité de données et leur dissémination (données comme valeur transformée et échangée sur le marché)

■ **SCENARIO :**

En 2017, les données sont de plus en plus diversifiées et sont des biens qui se transforment et s'échangent. La communication de ces données est réalisée le plus souvent au travers de flux automatiques. C'est d'autant plus vrai que ces données sont échangées dans des volumes importants et sont dynamiques. Le contrôle de la qualité de ces données en devient difficile. Il est nécessaire de développer des méthodes qui permettent le contrôle de données venant de sous-traitants (analyse des comportements hors norme par exemple).

■ **ACTIONS :**

Information / sensibilisation des utilisateurs (clients, particuliers, organisations…)

- Sensibiliser les responsables des risques encourus.

Tâches et compétences

- Développer des dispositifs d'alerte et des processus de réaction (développeur).
- Maîtriser l'analyse et la gestion des données (méthodes statistiques) en combinaison avec une connaissance du métier de l'organisation/du client.

Lorsque cela était possible, les experts ont été invités à situer à quel niveau de la pyramide des métiers de la sécurité de l'information pouvait se situer l'action à mener ou la tâche impactée.

6. Tâche impactées et nouvelles compétences

Au cours des ateliers, il n'a pas a été possible de déterminer un référentiel de compétences qui fasse consensus au sein du groupe d'experts.

C'est pourquoi, faute de pouvoir reposer l'analyse sur un référentiel préexistant, une approche plus intuitive a été adoptée.

Sur base du contenu des échanges entre les experts durant les ateliers, en particulier le troisième, une liste de 20 tâches a pu être dressée par l'équipe d'animation. Ces tâches sont uniquement celles qui ont émergé des discussions et ne peuvent être considérées comme un référentiel complet et précis.

Ces tâches ont été pour la plupart associées au métier de « gestionnaire de risques » (risk manager) liées à la sécurité de l'information. Afin de s'assurer de sa pertinence, la liste a été soumise au vote des experts. Ceux-ci étaient invités à coter de 0 à 3 l'importance (0= pas importante, 1=un peu importante, 2=importante, 3 =très importante) de la compétence pour le métier de gestionnaire de risques liés à la sécurité de l'information, selon que le métier soit exercé « en interne » dans une grande organisation ou en consultance auprès de PME.

Seules trois compétences obtiennent un score moyen inférieur à 2 :

- Lorsque le métier est exercé en interne d'une grande entreprise :
  - Etre capable de développer des applications mobiles répondant aux exigences de sécurité.
  - Etre capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate".

- Lorsque le métier est exercé en consultance :
  - Maîtriser le déploiement d'architectures du système d'information ouvertes et souples (adaptables).

Cela dénote d'une vision différente des métiers selon leurs conditions d'exercice. Le consultant est perçu comme apportant davantage une plus-value technique tandis que le professionnel « interne » aura la possibilité d'être au plus près de la stratégie.

D'autres compétences s'avèrent importantes quelles que soient les conditions d'exercice avec toutefois des différences relativement importantes dans les scores attribués. Ainsi *Maîtriser les méthodes d'analyse des (flux de) données afin d'identifier les « comportements anormaux »* semble davantage importante lorsque le métier est exercé en consultance, tandis que *connaître les aspects organisationnels des entreprises* et *être capable de convaincre et fédérer les membres de l'organisation et sa direction* semblent davantage important pour le professionnel « interne » à l'entreprise.

Cote moyenne à la question : S'agira-t-il, en 2017, d'une compétence importante pour le gestionnaire de risques liés à la sécurité de l'information ? (0= Pas du tout / 1= Un peu importante 2= Importante / 3=très importante)		Gestionnaire de risque lié à la sécurité de l'information…	
		… occupé en interne dans une entreprise?	… intervenant en sous traitance auprès de PME?
Compétences managériales	Connaître les aspects organisationnels des entreprises	2,8	2,2
	Maîtriser les méthodes de gestion des incertitudes	2,4	2,4
	Maîtriser les méthodes d'évaluation des risques	2,8	2,6
	Maîtriser les méthodes d'analyse prospective	2	2,4
Compétences juridiques	Connaître et comprendre les règlementations en matière de sécurité de l'information	2,6	2,4
	Connaître les règlementations juridiques en matière de contrat commercial et de Service Level Agreement	2,4	2,4
	Connaître les méthodes de calcul des coûts / bénéfices de la sécurisation des systèmes d'information	2,4	2,2
Compétences techniques	Etre capable de développer des applications mobiles répondant aux exigences de sécurité.	1,2	2
	Etre compétent en matière d'intégration informatique	2	2,4
	Maîtriser les méthodes d'analyse des (flux de) données afin d'identifier les "comportements anormaux"	2,2	2,8
	Etre capable d'établir une politique de connexion, en fonction des équipements, des applications, des réseaux utilisés et des utilisateurs	2,8	2,6
	Maîtriser le déploiement d'architecture du système d'information ouverte et souple (adaptable)	2,2	1,8
	Etre capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate".	1,6	2
	Pouvoir développer des processus d'alerte et de réaction aux événements perturbateur.	2,8	2,4
Aptitudes	Etre capable d'apprendre en continu	3	3
	Développer une réflexion systémique	2,6	2,4
	Etre capable de suivre les évolutions technologiques	2,8	3
	Etre capable de convaincre et fédérer les membres de l'organisation et sa direction	2,8	2,2
	Etre capable de mettre à jour ses compétences règlementaires	2,4	2,4
	Etre capable de s'adapter au métier de l'entreprise	2,6	2,4

Enfin, conformément à la méthodologie *Abilitic2Perform*, cette liste de compétences a été confrontée aux différents facteurs de changement. Les experts ont été ainsi invités à qualifier l'impact qu'a chacun des facteurs d'évolution sur chacune des compétences. Cette mesure de l'impact est réalisée au travers d'un processus de vote à distance. A la demande des experts, les cotations relatives à l'impact des facteurs sur les tâches ont été réalisées séparément selon que le métier de gestionnaire de risques liés à la sécurité de l'information est exercé en interne à l'organisation ou en consultance.

Une première analyse globale de l'impact des facteurs sur les tâches permet d'identifier celles qui subiront le plus d'effets. Ce sont les tâches suivantes qui devraient globalement être les plus impactées :

- Pouvoir développer des processus d'alerte et de réaction aux événements perturbateurs.
- Etre capable de suivre les évolutions technologiques.
- Maîtriser les méthodes d'analyse des (flux de) données afin d'identifier les "comportements anormaux".
- Etre capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate".

L'intérêt principal de l'exercice réside toutefois dans l'analyse individuelle de chaque tâche. Huit tâches semblent particulièrement touchées par un ou plusieurs facteurs d'évolution, c'est-à-dire que le score moyen d'impact d'un facteur sur la tâche est maximal.

- « Connaître les règlementations juridiques en matière de contrat commercial et de Service Level Agreement ».

La « connaissance des règlementations en matière de contrat commercial et de Service Level Agreement » sera particulièrement sensible à la location de services standard de la part des entreprises et à l'explosion de la quantité de données et leur dissémination. Les professionnels de la sécurité devront en effet être familiarisés avec ce type de contrats afin de pouvoir y apporter une lecture « technique ».

- « Etre capable de développer des applications mobiles répondant aux exigences de sécurité ».

Cette compétence sera d'autant plus importante que les technologies web seront omniprésentes, que de plus en plus d'appareils seront connectés. Le développement de ces applications devra de plus prendre en compte la mobilité des usagers connectés via des réseaux sans fil et le potentiel en matière de rapidité et de puissance de calcul générés par les technologies « large bande passante » ou 4G.

- « Maîtriser les méthodes d'analyse des (flux de) données afin d'identifier les comportements anormaux ».

- La « maîtrise des méthodes d'analyse des (flux de) données afin d'identifier les comportements anormaux », seront d'autant plus pertinents que les flux gagneront en rapidité (lare bande passante, 4G,…), et que ces données seront dispersées, dans l'organisation, et à l'extérieur, notamment sur des appareils privés.

- « Etre capable d'établir une politique de connexion, en fonction des équipements, des applications, des réseaux utilisés et des utilisateurs ».

Cette compétence sera particulièrement nécessaire, alors que de plus en plus d'équipements de nature différente seront connectés, via des réseaux divers. Cette tâche devrait gagner en complexité sous l'influence du caractère éclaté des systèmes informatiques et la fusion des mondes privés et publics.

- « Etre capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate" ».

Dès lors que les équipements connectés sont de plus en plus diversifiés, qu'ils sont tantôt professionnels, tantôt privés, et que les équipements informatiques de l'entreprises sont « éclatés », cela nécessite des configurations spécifiques.

- « Pouvoir développer des processus d'alerte et de réaction aux événements perturbateur ».

Un tel développement deviendra plus complexe dès lors qu'il faudra intégrer dans le système « à contrôler », des appareils privés en raison de la fusion des mondes privés et professionnels.

- « Etre capable d'apprendre en continu » et « être capable de suivre les évolutions technologiques »

Enfin, les compétences et aptitudes liées à l'apprentissage en continu et la capacité de suivre les évolutions technologiques en particulier sont rendues essentielles par l'accélération de l'innovation technologique, notamment en matière d'équipements connectés. Mais les pratiques des utilisateurs et les organisations des entreprises évoluent aussi et impliquent des mises à jour des connaissances de la part du professionnel. Ainsi l'organisation éclatée des systèmes informatiques, la location de services standards, ou encore la fusion des mondes privés et professionnels, nécessitent des adaptations de la part du professionnel de la sécurité de l'information.

	Disponibilité de très larges bandes passantes (+ 4G) avec une puissance de calcul élevée	Omniprésence de la technologie web	Hausse des équipements connectés	Explosion du sans fil	Accélération des innovations technologiques	Une informatique « éclatée »	Location de services standard	Fusion des mondes professionnel/privé - La consumérisation	L'explosion de la quantité de données et leur dissémination (données dans l'organisation)	L'explosion de la quantité de données et leur dissémination (données comme valeur transformée et échangée sur le marché)
Connaître les aspects organisationnels des entreprises	0,75	0,75	1,25	2,5	2,25	2,75	2,75	3,25	3,25	3,25
Maîtriser les méthodes de gestion des incertitudes	2,5	3	3,25	2,5	2,5	3,5	2	3,5	3,5	3,5
Maîtriser les méthodes d'évaluation des risques	3,25	3,25	3,25	3,25	2,25	3,25	2,5	3,25	3,25	3,25
Maîtriser les méthodes d'analyse prospective	2,5	3	3,25	2,25	3,25	3	1,5	3,25	3,25	3,25
Connaître et comprendre les règlementations en matière de sécurité de l'information	0,5	2	2	1,5	1,5	3,5	3,5	3,5	3,5	3,5
Connaître les règlementations juridiques en matière de contrat commercial et de Service Level Agreement	2,5	2,75	2,25	2,25	1,5	3,25	3,75	2,75	3,75	3,75
Connaître les méthodes de calcul des coûts / bénéfices de la sécurisation des systèmes d'information	1,75	3	3	3	1,75	3	3,5	3,5	3	3
Etre capable de développer des applications mobiles répondant aux exigences de sécurité.	3,75	3,75	3,75	3,75	1,5	2,75	1,5	1,5	1,25	1,25
Etre compétent en matière d'intégration informatique	2,25	3,5	3,5	2,25	2,5	3,5	2,5	3,5	2,5	2,5
Maîtriser les méthodes d'analyse des (flux de) données afin d'identifier les "comportements anormaux"	3,75	3,25	3,5	3,5	1,5	3,75	3,5	3,75	3,75	3,75
Etre capable d'établir une politique de connexion, en fonction des équipements, des applications, des réseaux utilisés et des utilisateurs	2,5	3,5	3,75	3,25	1,75	3,75	3,25	3,75	3,25	2,5
Maîtriser le déploiement d'architecture du système d'information ouverte et souple (adaptable)	3	3,5	3,25	2,5	3,25	3,5	3,5	3,5	2,75	2,5
Etre capable de configurer les équipements informatiques en fonction des types de connexions, des applications, des réseaux utilisés et des utilisateurs, y compris les équipements "non corporate".	3,5	3,5	3,75	3,5	2,5	3,75	3,25	3,75	2,75	2,75
Pouvoir développer des processus d'alerte et de réaction aux événements perturbateur.	3,25	3,5	3,5	3,5	3,25	3,5	3,5	3,75	3,5	3,5
Etre capable d'apprendre en continu	2,25	3	3,75	2,25	3,75	3,5	3,5	3,75	3	2,75
Développer une réflexion systémique	2,75	3,25	3,5	2,25	3,5	3,5	3	2,75	3	3
Etre capable de suivre les évolutions technologiques	3,25	3,5	3,75	3,25	3,75	3,75	3,75	3,75	3	3
Etre capable de convaincre et fédérer les membres de l'organisation et sa direction	2,25	2,25	2,75	2,75	3,25	3,5	3,5	3,5	3,25	3,25
Etre capable de mettre à jour ses compétences règlementaires	1,75	2,75	3	2	3,5	3,5	3,5	3,5	3,25	3,25
Etre capable de s'adapter au métier de l'entreprise	2	2,5	2,75	2,5	2,75	2,75	3,5	3,5	3,25	3,25

Grâce à l'aimable participation de :

- Adarssi, Mohamed (Analyste Amef, Le Forem)
- Dallons, Gautier (CETIC, responsable adjoint du département software and system engineering)
- Deherve, Eric (Formateur, Technocité)
- Desausoi Alain (CSO Head of Enterprise Security & Architecture, SWIFT)
- Fuks, Pascal (Network and Security consultant / CEO, Fiancial Art S.A., mandaté par Technofutur TIC et Technifutur)
- Grégoire, Dominique (Conseiller en sécurité de l'information et gestion de risque, Le Forem)
- Hubaux, Damien (Directeur, CETIC)
- Iwaschko, Michel (Network Research Belgium)
- Lejeune, Benoit (Director, TDO/TL Middleware Security, Euroclear)
- Roucour, Richard (Directeur adjoint, Technocité)
- Verstrepen, Michel (Responsable de ligne de produit de formation, Le Forem)

Encadrement méthodologique de la démarche et rédaction du rapport final :

- Choteau, Géry (Le Forem)
- Sobieski, Jacques (Le Forem)
- Watelet, William (Le Forem)