–CYBERSÉCURITÉ EN BRETAGNE : L'ENJEU DES COMPÉTENCES–

LES ÉTUDES DE L'EMPLOI CADRE

N° 2017-25

JUIN 2017

– Étude-action sur l'emploi formation financée dans le cadre du contrat de plan État-Région.

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BRETAGNE

Région BRETAGNE

BRETAGNE DÉVELOPPEMENT INNOVATION

PÔLE D'EXCELLENCE CYBER

APEC

– LES ÉTUDES DE L'EMPLOI CADRE DE L'APEC –

Observatoire du marché de l'emploi cadre, l'Apec analyse et anticipe les évolutions dans un programme annuel d'études et de veille : grandes enquêtes annuelles (recrutements, salaires, métiers et mobilité professionnelle des cadres, insertion professionnelle des jeunes diplômés...) et études spécifiques sur des thématiques clés auprès des jeunes de l'enseignement supérieur, des cadres et des entreprises.
Le département Études et Recherche de l'Apec et sa quarantaine de collaborateurs animent cet observatoire.

Toutes les études de l'Apec sont disponibles gratuitement sur le site **www.cadres.apec.fr rubrique observatoire de l'emploi**

SOMMAIRE

SOMMAIRE

–PRINCIPAUX ENSEIGNEMENTS–

Cette étude a été réalisée par le département études et recherche de l'Apec et cofinancée par la Région Bretagne et l'État dans le cadre d'un appel à projets pour des études-actions sur l'emploi-formation prévu dans le contrat de plan État-Région. Le Pôle d'excellence cyber et Bretagne Développement Innovation ont été associés à cette démarche et ont participé au comité de pilotage.
L'étude a été réalisée en 2 phases. D'abord, une enquête qualitative par entretiens individuels et groupes de travail a été menée auprès d'une trentaine d'entreprises, essentiellement bretonnes, recherchant des compétences en cybersécurité. Ensuite, 1 200 informaticiens issus d'un fichier Apec, dont 44 % résidant en Bretagne, ont été interrogés via un questionnaire par Internet. Elle débouche sur un plan d'actions concret qui sera mis en oeuvre par la délégation Apec Bretagne, en collaboration avec les partenaires de l'étude.

– LA CYBERSÉCURITÉ : ENJEU ET DÉFI –

Différentes menaces planent sur les systèmes d'information : vol de données, espionnage industriel, prise de contrôle à distance de machines ou de chaînes de production, arnaques ou usurpation d'identité, pratiques de rançonnage... La probabilité pour les entreprises d'être attaquées, quelle que soit leur taille, devient une éventualité de plus en plus concrète. Aussi, elle les oblige à prendre des mesures nécessaires pour se protéger. Il y a une responsabilité générale (et pénale) des entreprises de sécuriser leurs systèmes d'information, notamment pour protéger les données personnelles dont elles sont dépositaires. De surcroît, les évolutions technologiques (objets connectés, systèmes embarqués, intelligence artificielle, informatique en nuage...) et les pratiques informatiques (nomadisme, réseaux sociaux...) comportent à chaque fois des risques forts en matière de sécurité informatique. La cybersécurité constitue donc pour les entreprises à la fois un enjeu vital, une obligation réglementaire et un positionnement stratégique.

– LA CYBERSÉCURITÉ : UNE OPPORTUNITÉ POUR L'EMPLOI –

Dans un contexte de préoccupation forte des entreprises sur le sujet de la sécurité informatique, l'ensemble des études disponibles font état d'une forte progression de l'emploi pour les métiers dédiés à la cybersécurité[1]. L'évolution du nombre d'offres d'emploi diffusées par l'Apec pour des postes de cadres en cybersécurité témoigne également de cette tendance. Le nombre d'offres d'emploi diffusées par l'Apec pour des postes en cybersécurité a été multiplié par 4 entre 2014 et 2016, passant de 315 offres à 1 133 offres.
La cybersécurité constitue ainsi un domaine porteur pour l'emploi informatique et devrait continuer à se développer dans les années à venir. Les informaticiens en sont convaincus. Invités à juger sur une échelle de 0 à 10 si la cybersécurité constitue aujourd'hui un secteur porteur pour l'emploi, 29 % d'entre eux attribuent une note de 8, 9 ou 10. Mais si on leur demande d'attribuer une même note en se projetant dans 3 à 5 ans, la proportion grimpe à 69 %.

– LA CYBERSÉCURITÉ EN BRETAGNE : UN LEADERSHIP RECONNU –

Il existe un véritable écosystème breton favorable à la montée en puissance de la filière cybersécurité. La Bretagne bénéficie à la fois de l'implantation ancienne de centres étatiques (DGA-MI : Direction générale de l'Armement – Maîtrise de l'information, École des transmissions, École navale, Écoles de Saint-Cyr Coëtquidan...), de la présence d'acteurs privés majeurs sur ce domaine et d'un tissu dense de centres de formation et de recherche civils et militaires. Ainsi, initié par le ministère de la Défense et la Région Bretagne en 2014, le Pôle d'excellence cyber, qui a pris naissance en Bretagne, a pour mission d'accompagner au niveau national le développement de la filière de cybersécurité et de cyberdéfense sur les trois piliers indissociables que sont la formation, la recherche et le développement industriel.

1. Cf. par exemple Pipame, *Le secteur industriel français de cybersécurité*, janvier 2016.

L'excellence bretonne en matière de cybersécurité est reconnue. Ainsi, les informaticiens bretons interrogés par l'Apec citent la Bretagne en 2e position des régions françaises qu'ils jugent particulièrement à la pointe en matière de cybersécurité, juste derrière l'Île-de-France. Les actions entreprises par la Région Bretagne en matière de cybersécurité trouvent donc un écho au sein de la population des informaticiens résidant sur le territoire. Cette réputation dépasse les frontières de la région : les informaticiens français placent la Bretagne au 4e rang des régions les plus à la pointe sur la cybersécurité, devant des régions comme l'Occitanie ou les Hauts-de-France.

LE BESOIN EN COMPÉTENCES EN CYBERSÉCURITÉ EN BRETAGNE

Dans tous les métiers de la cybersécurité, des compétences techniques très pointues sont demandées : évaluation de composants ou de logiciels, conception d'architectures sécurisées, détection d'intrusion, modélisation des menaces et attaques, conception d'antivirus, cryptographie... Au-delà de leurs compétences techniques, les candidats sont aussi attendus sur des compétences dites comportementales. La curiosité, l'agilité, le relationnel, l'éthique et le sens du service sont posés par les recruteurs comme autant d'aptitudes personnelles à mobiliser dans l'univers professionnel d'un futur spécialiste de la cybersécurité et donc fondamentales dans l'exercice des métiers de la cybersécurité.

La tension sur le marché de l'emploi informatique en cybersécurité existe en Bretagne mais elle reste limitée par rapport à la région parisienne. L'attachement des cadres bretons à leur région est important, ce qui limite les souhaits de mobilité géographique vers d'autres régions et le turn-over. La qualité de vie en région contribue aussi à attirer des cadres venus d'ailleurs, notamment du Bassin parisien. Ainsi, parmi les informaticiens prêts à changer de région lors d'un changement de poste, 24 % indiquent la Bretagne comme une destination possible, soit la région la plus attractive avec les régions Nouvelle-Aquitaine et Provence-Alpes-Côte d'Azur.

UNE FORTE ATTRACTIVITÉ DE LA FILIÈRE POUR LES INFORMATICIENS

Les entreprises peuvent aussi bénéficier de l'attrait exercé par le domaine de la cybersécurité sur les informaticiens. En effet, 74 % des informaticiens seraient dans l'absolu intéressés pour travailler dans le domaine de la cybersécurité. Cette proportion monte à 81 % pour les informaticiens bretons. Et 82 % d'entre eux souhaitent d'une manière générale développer leurs compétences en cybersécurité (87 % en Bretagne). On peut noter que les femmes interrogées sont moins intéressées que les hommes pour travailler dans la cybersécurité (54 % contre 79 %) et pour monter en compétences sur le sujet (67 % contre 85 %).

De surcroît, le processus de montée en compétences peut potentiellement être lourd puisque seulement 40 % des informaticiens interrogés indiquent posséder des compétences techniques en cybersécurité. Et même pour ceux-là, lorsqu'on leur demande de s'autoévaluer de 0 à 10 sur différents sujets techniques (conception d'architectures sécurisées, détection d'intrusion, tests de sécurité, cryptographie...), une faible proportion considère avoir un bon niveau de connaissance.

La question de la montée en compétences sur le sujet de la cybersécurité pour les informaticiens actuellement sur le marché est donc très clairement posée.

D'IMPORTANTES ATTENTES EN MATIÈRE DE FORMATION CONTINUE

Le tissu de formation initiale en cybersécurité est relativement bien fourni, notamment à l'échelle de la Bretagne. Les enseignements spécifiques continuent de se développer que ce soit dans les universités ou les grandes écoles. On remarquera toutefois que les entreprises ne cherchent pas que des juniors. Bon nombre de métiers de la cybersécurité nécessitent de l'expérience. L'étude des offres d'emploi en cybersécurité publiées sur le site Internet de l'Apec montre qu'une grande majorité des offres ne sont pas accessibles aux débutants et jeunes diplômés.

Un réel effort est donc attendu en matière de formation continue, non seulement pour permettre d'ajuster les compétences des spécialistes sur des techniques et pratiques en constante évolution, mais aussi pour assurer la montée en compétences des cadres déjà en poste qui n'ont pas eu de formation initiale en cybersécurité. Le recours à la formation continue permettrait aussi d'améliorer l'employabilité de cadres sans emploi, et de les repositionner au sein d'entreprises qui cherchent à recruter. Et ce d'autant plus que la demande de la part des informaticiens présents sur le marché est très forte. Parmi les informaticiens déclarant vouloir développer leurs compétences en cybersécurité, 9 sur 10 auraient besoin d'une formation, que ce soit sous la forme d'une formation continue (y compris en reprise d'études) ou d'une formation interne à leur entreprise.

UN PLAN D'ACTIONS POUR FAVORISER LE DÉVELOPPEMENT DES COMPÉTENCES EN CYBERSÉCURITÉ EN BRETAGNE

Cette étude a débouché sur un plan d'actions qui sera mis en œuvre dès cette année par la délégation Apec de Bretagne, en collaboration avec les partenaires de l'étude. L'Apec s'engage ainsi dans différentes actions concrètes sur trois volets : développer la connaissance des métiers de la cybersécurité et promouvoir les métiers, travailler avec les entreprises bretonnes de la cybersécurité pour répondre à leurs besoins (recrutement, fidélisation...), accompagner les cadres et les jeunes diplômés bretons en recherche d'opportunité ou de mobilité dans la filière de la cybersécurité. Certaines actions seront pérennisées au-delà de 2017.

–1–

–LA CYBERSÉCURITÉ : UNE PRISE DE CONSCIENCE–

À l'ère où la transformation digitale est au cœur de la stratégie des entreprises et où les objets connectés et la portabilité des données ont fait apparaitre de nouvelles manières de produire et de consommer, la cybersécurité est devenue une préoccupation forte pour les particuliers comme pour les entreprises.
La cybersécurité peut être définie comme « *un état recherché pour un système d'information lui permettant de résister à des évènements issus du cyberespace susceptibles de compromettre la disponibilité, l'intégrité ou la confidentialité des données stockées, traitées ou transmises et des services connexes que ces systèmes offrent ou qu'ils rendent accessibles* »[2]. Aussi, elle vise tout à la fois à sécuriser les systèmes d'information en amont (cyberprotection), à réagir à des attaques (cyberdéfense), et à réviser les systèmes de protection en fonction des failles trouvées ou révélées (cyber-résilience).

2. Définition de l'Anssi (Agence nationale de la sécurité des systèmes d'information) citée dans le Référentiel technique (version 4.1.1) édité par le Pôle d'excellence cyber.

–DES MENACES PROTÉIFORMES QUI SONT CONNUES–

Différentes menaces planent sur les systèmes d'information : vol de données, espionnage industriel, prise de contrôle à distance de machines ou de chaînes de production industrielle[3], usurpation d'identité, interruption de services, pratiques de rançonnage... De très grands groupes internationaux comme Yahoo!, Twitter, Spotify, Paypal, Sony Pictures Entertainment ont récemment été visés par de telles attaques. À l'échelle hexagonale, de grands groupes ont également fait les frais de pirates informatiques comme TV5 Monde en 2015. De nombreuses PME sont également concernées **(encadré 1)**.

3. Industrial control system (ICS).

– Encadré 1–
Exemples d'attaques informatiques envers des entreprises

UNE ATTAQUE PARALYSANT TV5 MONDE

Le 8 avril 2015, TV5 Monde, chaîne de télévision francophone internationale, est victime d'une importante attaque informatique. L'ensemble du réseau informatique est coupé et la chaîne doit interrompre sa diffusion. La chaîne n'a pu reprendre le contrôle de son réseau qu'après plusieurs heures et la diffusion télévisée n'a pu reprendre normalement que le 9 avril au soir. L'enquête a démontré que les pirates avaient réussi à infiltrer le réseau depuis des semaines afin de préparer l'attaque. Ils auraient utilisé une technique de « phishing » en envoyant un e-mail à l'ensemble des journalistes avec un fichier joint. Ce fichier, contenant un cheval de Troie, a été ouvert, ce qui leur aurait permis de s'immiscer dans le système informatique.

UN VOL DE DONNÉES VISANT YAHOO!

En décembre 2016, le groupe Yahoo! a annoncé avoir été victime d'une cyberattaque d'ampleur en 2013. Les données de plus d'un milliard d'utilisateurs (noms, numéros de téléphone, dates de naissance) ont été dérobées. Il apparaîtrait que la méthode utilisée par l'entreprise pour protéger les mots de passe était largement obsolète[4].

4. *Le piratage de Yahoo! révèle de graves défaillances*, Le Monde, 15/12/2016.

UNE ARNAQUE FINANCIÈRE VISANT UNE PME FRANCILIENNE

En 2014, la comptable de la PME Etna Industrie, un fabricant de composants hydrauliques, reçoit une série de mails signés du nom de la dirigeante du groupe. Il lui est demandé de procéder à une opération financière. Un interlocuteur d'un bureau régional de l'expertise comptable la contacte également pour ce même dossier, renforçant le bien-fondé de cette demande. Il s'agit d'une supercherie mais la comptable s'exécute, effectuant au nom de l'entreprise un virement de 500 000 euros sur un compte d'emprunt.

UN CHIFFRAGE DE DONNÉES AVEC DEMANDE DE RANÇON VISANT UNE PME DE LA RÉGION BRETAGNE

En octobre 2015, des hackers s'introduisent dans le système d'information de la PME Sabella, une entreprise quimpéroise qui conçoit et développe des hydroliennes. L'interface de communication permettant au site quimpérois de piloter une hydrolienne devant alimenter l'île d'Ouessant est interrompue suite au chiffrage des données. S'ensuit une demande faite à l'entreprise de verser 4 000 € pour récupérer ses données. L'entreprise a réussi à restaurer elle-même son serveur et n'a donc pas payé la rançon exigée par les pirates. L'attaque a tout de même entraîné 15 jours d'arrêt de production.

La diversité de ces attaques témoigne de l'évolution des ambitions des cyberattaquants, ces derniers n'étant plus uniquement motivés par l'envie de relever un défi (celui de craquer un système) comme auparavant. Aujourd'hui, l'attrait d'un gain financier dérivé de ces attaques constitue un moteur important dans leurs démarches. De fait, on parle de plus en plus de cybercriminalité pour qualifier ces attaques. Les attaques peuvent aussi avoir un objectif d'influence ou de déstabilisation d'un pays et revêtir une dimension politique voire militaire[5].

Au-delà de la responsabilité des hackers, ces exemples montrent aussi que des salariés mal informés des pratiques élémentaires en matière d'hygiène informatique peuvent être le vecteur de telles attaques. L'ouverture de mails ou de pièces jointes indésirables et frauduleuses peut ainsi avoir des conséquences dramatiques pour les entreprises, entraînant des pertes financières et la mise à mal de leur réputation. •

5. Délégation ministérielle aux industries de sécurité et à la lutte contre les cybermenaces, *État de la menace liée au numérique en 2017 rapport n°1*, janvier 2017.

–LA CYBERSÉCURITÉ : UN ENJEU VITAL POUR LES ENTREPRISES–

Pour la première fois en 2016, les incidents sur les systèmes d'information ont été identifiés par les experts en sécurité comme l'un des principaux risques auxquels les entreprises pourraient être confrontées. Selon le Baromètre des risques d'Allianz[6], il se situe en effet en 3e position des menaces identifiables (en très forte progression en un an), derrière des interruptions de service ou de production et des phénomènes micro-économiques tels que l'augmentation de la concurrence sur leurs marchés.

Aujourd'hui en France, les conséquences financières des attaques informatiques sont rudes pour les entreprises : 1,5 milliard d'euros de pertes financières sur la seule année 2016 (enquête annuelle de PwC[7]). La probabilité pour les entreprises d'être attaquées devient de plus en plus forte. Aussi, elle les oblige à prendre des mesures nécessaires pour se protéger. Le renforcement des mesures réglementaires en matière de sécurisation des systèmes d'information est un autre élément expliquant la considération portée dans les entreprises à la cybersécurité **(encadré 2)**. En effet, les entreprises se doivent de sécuriser leurs systèmes d'information pour protéger les données dont elles sont dépositaires. Mise en place d'une politique de sécurité avec élaboration d'une charte associée, respect de normes et bonnes pratiques associées, qualification des données et de leur usage (publiques / privées), réalisation d'audits de sécurité... sont autant de moyens pour les entreprises de se protéger juridiquement en cas d'attaque. Pour les entreprises relevant des OIV (opérateurs d'importance vitale), des obligations complémentaires sont apportées en matière de déclaration d'incidents. Il s'agit d'entreprises ou de services étatiques dépendant de secteurs (défense, finance, énergie, transports, santé...) qui, s'ils étaient attaqués ou endommagés volontairement (sabotage, terrorisme...), pourraient atteindre gravement le potentiel économique du pays, sa capacité de survie ainsi que la sécurité de la population. ●

6. Allianz, *Allianz Risk Barometer – Top Business Risks* 2016.
7. PwC, The Global State of Information Security® Survey 2017.

– Encadré 2–
Principales règles de droit concernant la sécurité des systèmes d'information

Article 1383 du Code civil : « Chacun est responsable du dommage qu'il a causé non seulement par son fait, mais encore par sa négligence ou par son imprudence. »

Article 323-1 du Code civil : « Le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est puni de deux ans d'emprisonnement et de 60 000 € d'amende. »

Article 226-13 du Code pénal : « La révélation d'une information à caractère secret par une personne qui en est dépositaire soit par état ou par profession, soit en raison d'une fonction ou d'une mission temporaire, est punie d'un an d'emprisonnement et de 15 000 € d'amende. »

Article 226-17 du Code pénal : « Le fait de procéder à un traitement de données à caractère personnel sans mettre en œuvre les mesures prescrites de l'article 34 de la loi n° 78-17 du 6 janvier 1978 est puni de 5 ans d'emprisonnement et de 300 000 € d'amende. »

Article 34 de la Loi relative à l'informatique, aux fichiers et aux libertés (1978) : « Le responsable de traitement est tenu de prendre toutes précautions utiles, au regard de la nature des données et des risques présentés par le traitement, pour préserver la sécurité des données et, notamment, pour empêcher qu'elles soient déformées, endommagées, ou que des tiers non autorisés y aient accès. »

L'article 1332-6-1 du Code de la défense oblige aussi les OIV (opérateurs d'importance vitale) à informer « sans délai le Premier ministre des incidents affectant le fonctionnement ou la sécurité des systèmes d'information » qui risqueraient « de diminuer d'une façon importante le potentiel de guerre ou économique, la sécurité ou la capacité de survie de la Nation ou pourrait présenter un danger grave pour la population. »

Le Règlement général sur la protection des données (RGPD) 2016/679 (application à partir du 25 mai 2018) est le texte de référence européen en matière de protection des données à caractère personnel. Il vise à renforcer les droits des personnes, responsabiliser les acteurs traitant des données (responsables de traitement et sous-traitants), crédibiliser la régulation grâce notamment à des sanctions renforcées pour les entreprises en cas de manquement.

–DES ACTIONS CONCRÈTES POUR SE PROTÉGER DES CYBER-RISQUES–

DANS LES ENTREPRISES DE 200 SALARIÉS ET PLUS

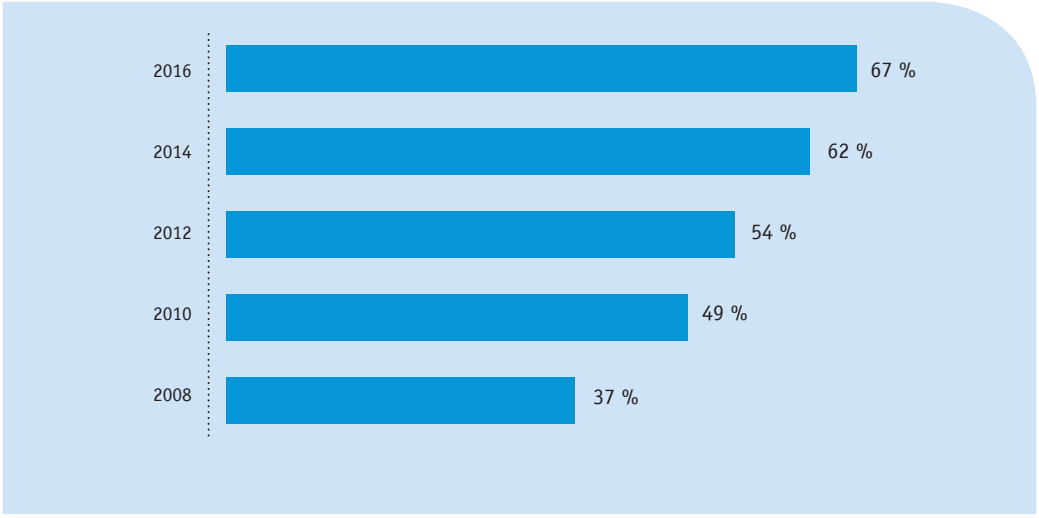
Dans son enquête menée auprès des RSSI (responsables de la sécurité des systèmes d'information) et DSI (directeurs des systèmes d'information) issus de 334 entreprises représentatives des entreprises françaises de 200 salariés et plus, le Club de la sécurité de l'information français (Clusif) identifie les principales actions mises en place pour répondre aux enjeux en matière de cybersécurité[8]. Parmi elles, la désignation d'un garant de la sécurité et de l'intégrité d'un système d'information, en l'occurrence d'un RSSI, concerne désormais 67 % de ces structures, ce qui correspond à une hausse de 30 points comparativement à 2008 **(figure 1)**.

Des solutions de sécurisation ont quasiment été généralisées dans bon nombre de grandes entreprises. Dans 9 cas sur 10, elles ont mis en place des systèmes d'antivirus et d'antimalware sur les postes de travail y compris les portables, empêchant l'activation de tous types d'attaque connue. Elles ont aussi, dans les mêmes proportions, déployé des antispams pour contrer les attaques introduites via l'usage des messageries. Par ailleurs, 6 entreprises sur 10 réalisent de la veille technologique en matière de vulnérabilité et de solutions associées.

Pour autant, certaines grandes entreprises sont en retard sur certains éléments de sécurité. Elles ne sont que la moitié à avoir procédé à une classification de leurs informations sensibles et à réaliser des analyses de risques. Aussi, seules 34 % de ces grandes entreprises chiffrent leurs données et à peine un quart d'entre elles ont souscrit des politiques d'assurances en matière de cyber-risques. Les contraintes organisationnelles et le manque de ressources financières sont identifiés par les RSSI comme les principaux freins à ces développements.

8. Clusif, *Menaces informatiques et pratiques de la sécurité en France*, 2016.

– Figure 1 –
Part des entreprises de plus de 200 salariés ayant clairement identifié et attribué la fonction de responsable de la sécurité des systèmes d'information (RSSI)



Clusif, Menaces informatiques et pratiques de la sécurité en France, 2016.

DANS LES PME

En raison de leur structure, les PME ne possèdent pas toutes un service dédié à l'informatique. Selon une enquête de la CPME[9], c'est le dirigeant même de ces structures qui prend en charge dans quasiment la moitié des cas la gestion des ressources informatiques (48 %). À défaut, c'est une personne externe à l'entreprise qui est le plus souvent mobilisée (27 %). L'enquête montre également que si 93 % des PME interrogées réalisent des sauvegardes de données, elles sont moins de 75 % à le faire au moins une fois par semaine.

Le manque de moyens et de ressources explique en partie ces résultats. À cela s'ajoute la difficile prise de conscience des PME quant aux menaces susceptibles de les atteindre. En effet, ces dernières n'imaginent pas toujours – à tort – représenter une cible potentielle pour les cyberattaquants. •

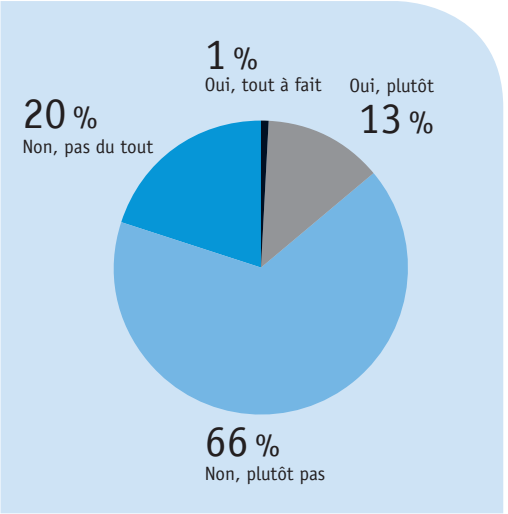
9. Confédération des Petites et Moyennes Entreprises, *Cybersécurité : Enquête CGPME*, Juin 2015.

–DES ACTIONS PAS TOUJOURS À LA HAUTEUR DES ENJEUX–

Si une certaine prise de conscience est apparue ces dernières années dans les entreprises sur l'enjeu de la cybersécurité, les entreprises ne sont pas matures sur le sujet. Elles le reconnaissent elles-mêmes : par exemple seuls 53 % des dirigeants d'entreprises industrielles jugent que leur entreprise est bien préparée sur les questions de cybersécurité[10]. Les informaticiens interrogés par l'Apec sont encore plus sévères. 86 % d'entre eux jugent que les entreprises en général ne sont pas bien préparées sur le sujet de la cybersécurité **(figure 2)**. Ils sont également presque unanimes (83 %) à penser que les salariés ne sont pas bien sensibilisés aux bonnes pratiques en matière d'hygiène informatique et de sécurité **(figure 3)**. Le travail à accomplir pour implanter une culture de la cybersécurité dans les entreprises apparaît donc encore très important. •

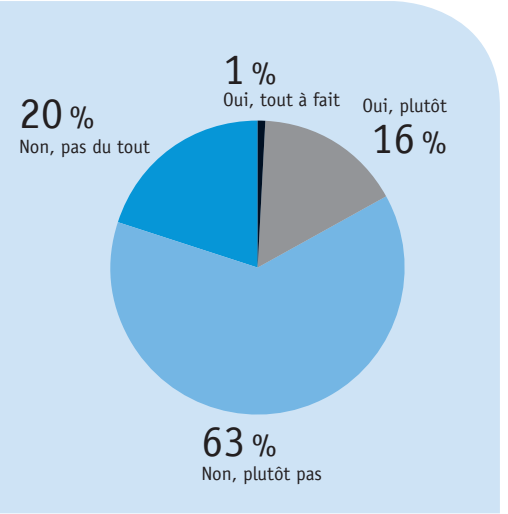
10. Étude L'Usine Nouvelle – Orange Business Services réalisée en novembre 2016 auprès de 347 dirigeants de l'industrie.

– Figure 2 –
On parle beaucoup de cybersécurité aujourd'hui. Pensez-vous que les entreprises en général y sont bien préparées ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

– Figure 3 –
Pensez-vous que les salariés de leur côté sont bien sensibilisés aux bonnes pratiques en matière d'hygiène informatique et de sécurité ?

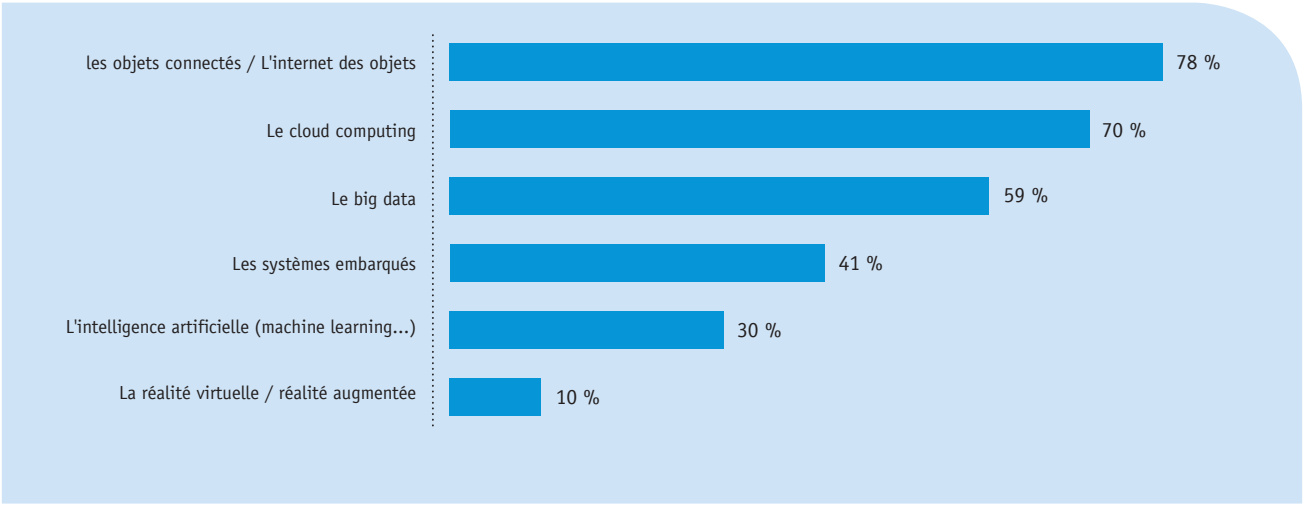


Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

–DE NOUVELLES APPLICATIONS POUR LA CYBERSÉCURITÉ–

La cybersécurité se situe au cœur de l'évolution actuelle des systèmes d'information dans les entreprises. Dans un monde de plus en plus « connecté » tant dans la sphère personnelle (téléphone intelligent, domotique, objets connectés…) que dans le monde des entreprises (systèmes embarqués dans les transports, externalisation des systèmes d'information…), la cybersécurité devient capitale. Les informaticiens interrogés par l'Apec sont d'ailleurs fortement majoritaires à juger que la cybersécurité constitue une problématique majeure pour des enjeux tels que le « *big data* », le « *cloud computing* » ou les objets connectés **(figure 4)**.

– Figure 4–
Selon vous, parmi ces enjeux, quels sont ceux pour lesquels la cybersécurité constitue une problématique majeure ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Dans les années à venir, les entreprises seront amenées à traiter des masses toujours plus importantes de données. De nombreuses entreprises, et notamment les plus emblématiques du XXIe siècle (Facebook, Airbnb, Uber…) ont d'ailleurs construit leur modèle économique autour de l'exploitation de données. Toutes les entreprises, quel que soit leur secteur, s'intéressent aujourd'hui à la manière d'exploiter et de valoriser au mieux leurs données **(encadré 3)**. Les incidences en termes de sécurité informatique sont très importantes. C'est bien sûr l'intérêt des entreprises de pouvoir assurer à leurs clients une sécurité la plus importante possible, mais c'est aussi une obligation réglementaire depuis la Loi informatique et libertés de 1978. Le nouveau règlement européen sur la protection des données, qui sera applicable dans tous les pays de l'Union le 25 mai 2018, impose désormais aux responsables de traitements de données de mettre en œuvre « *toutes les mesures techniques et organisationnelles nécessaires au respect de la protection des données personnelles, à la fois dès la conception du produit ou du service et par défaut.*[11] » Autrement dit, la protection des données doit être assurée par défaut et en amont[12]. Les sanctions en cas de manquement vont devenir significatives : elles pourront atteindre pour les entreprises de 2 % à 4 % du chiffre d'affaires annuel. ●

11. CNIL, *Règlement européen sur la protection des données : ce qui change pour les professionnels*, juin 2016.
12. Il s'agit d'appliquer le concept du « *privacy by design* ».

– Encadré 3–
Verbatim

« Le grand enjeu du XXIe siècle, c'est l'économie numérique mondiale, l'interconnectivité des entreprises par les réseaux de télécommunications et les chaînes de valeur autour de la data. Et l'enjeu de l'enjeu c'est la protection et la confiance dans toute cette infrastructure massivement connectée. Et c'est cette confiance dans cette infrastructure massivement connectée que l'on appelle la cybersécurité. »
(Expert).

« Il y a la problématique d'avoir une data safe massive sur laquelle la sécurité a ses cartes à jouer. Et il y a là tout un enjeu de montée en compétences. »
(Petite entreprise).

« Les sociétés sont de moins en moins propriétaires de leur système d'information. La seule chose qui reste chez elles, ce sont les données. Je pense par contre qu'elles vont avoir besoin de profils sur lesquels elles auront la possibilité d'anticiper sur la protection de leurs données. Et ça ce sont des métiers qui n'existent pas encore totalement. »
(Petite entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

–2–

–LA CYBERSÉCURITÉ : DES OPPORTUNITÉS D'EMPLOI–

La prise de conscience, même imparfaite, du risque majeur que peuvent constituer des failles de sécurité informatique pour les entreprises a entraîné la consolidation d'un marché de la cybersécurité. En effet, beaucoup d'entreprises cherchent à s'outiller et à monter en compétences sur le sujet. Elles peuvent notamment faire appel à des acteurs spécialisés dans la cybersécurité. Ces acteurs constituent un secteur particulièrement dynamique. Le chiffre d'affaires global des entreprises spécialisées en cybersécurité augmente ainsi de 10 % par an[13]. Ce dynamisme se traduit par de nombreux recrutements de personnel dédié. Ainsi, les effectifs des entreprises spécialisées en cybersécurité pourraient augmenter de 7 % par an d'ici 2020.

13. Pipame, *Le secteur industriel français de cybersécurité*, janvier 2016.

–LE MARCHÉ DE LA CYBERSÉCURITÉ–

– LES BESOINS DES ENTREPRISES –

Même si toutes les entreprises sont concernées à différents degrés par la cybersécurité, elles n'ont pas toutes les mêmes besoins **(figure 5)**. Le marché de la cybersécurité est porté en premier lieu par les besoins des grandes entreprises et en particulier celles qui relèvent de secteurs sensibles. Plus de 200 entreprises publiques et privées sont opérateurs d'importance vitale (OIV), car indispensables au bon fonctionnement de la Nation. Cette liste est tenue confidentielle pour des questions de sécurité nationale. Ces OIV sont contraintes par la loi d'appliquer des mesures de protection particulières en matière de cybersécurité. Elles recrutent donc en direct des experts en cybersécurité mais font aussi largement appel à de l'expertise externe. À l'inverse, les PME dans des secteurs moins sensibles s'appuient avant tout sur des compétences informatiques très généralistes.

Entre ces deux positions extrêmes (OIV versus PME sur des secteurs peu sensibles), beaucoup d'entreprises ont besoin à la fois de monter en compétences en interne sur le sujet de la cybersécurité et de faire appel de façon ponctuelle à de l'expertise externe (conseil, audit) pour cibler au mieux les actions à entreprendre. De même, si les PME ne recrutent que rarement en direct des experts en cybersécurité, elles peuvent être intéressées par des actions de sensibilisation et de mutualisation de ressources.

L'enjeu pour toutes les entreprises est avant tout d'opérer leur transformation digitale en toute confiance, par l'intégration dans cette stratégie des questions de cybersécurité.

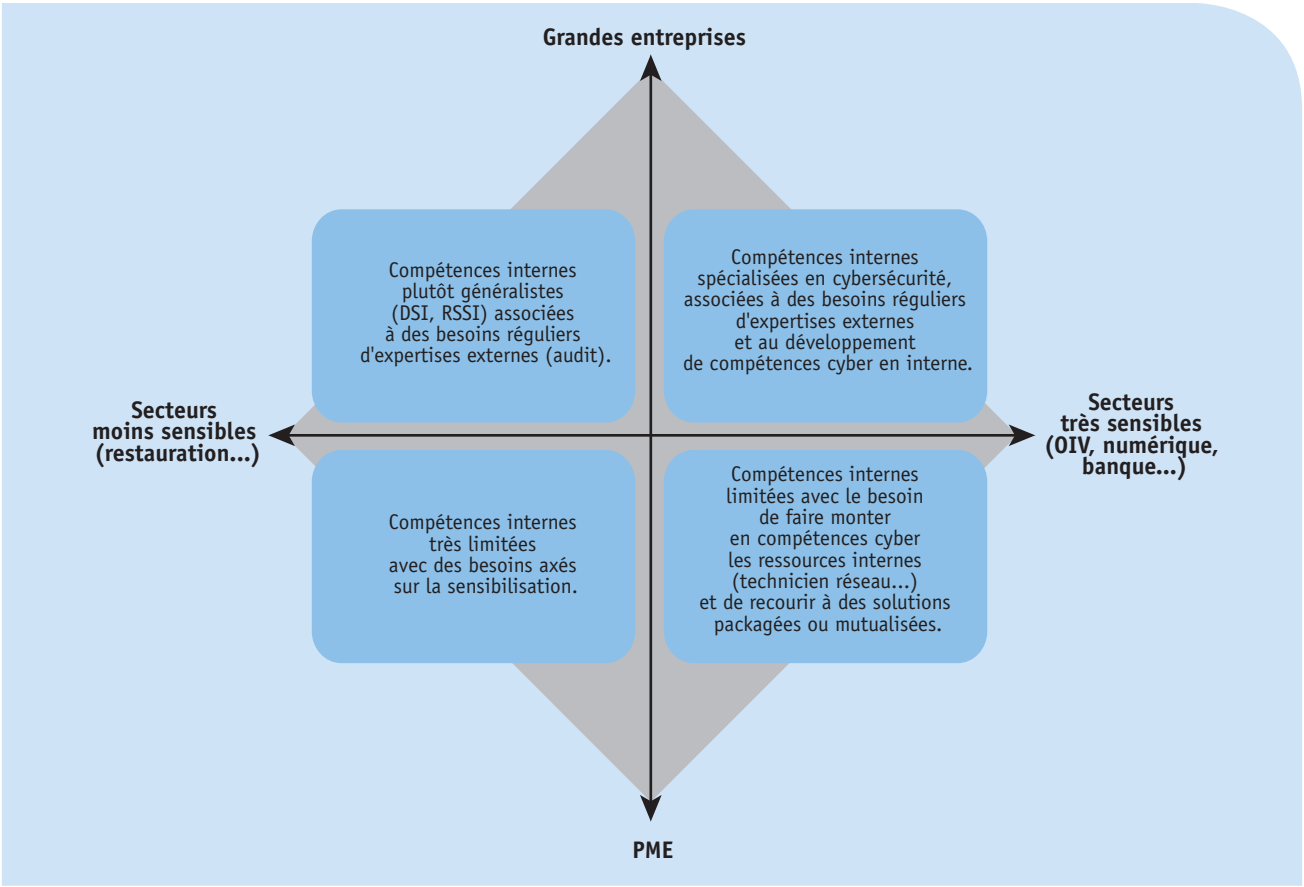
Le déploiement de ressources partagées est une solution déjà adoptée dans certains secteurs, comme celui de la santé. Sur ce domaine, un groupement d'intérêt économique (GIE) a par exemple été créé en 2013 pour répondre aux exigences de sécurité posées par le développement de l'hôpital numérique (protection des données de patients, gestion informatisée de parcours de soin...).

– LES ENTREPRISES SPÉCIALISÉES EN CYBERSÉCURITÉ –

Pour répondre aux besoins des entreprises en matière de cybersécurité, des acteurs spécialisés proposent leurs services. On trouve trois types d'acteurs principaux :

1. Des grandes entreprises du conseil (Deloitte, E&Y...) ou des services informatiques (Capgemini Sogeti, Sopra Steria, Atos-Bull, Orange Business Services...) qui ont développé des branches d'activité spécifiques en cybersécurité.
2. Des entreprises spécialisées dans le secteur de la défense et qui ont à ce titre développé des expertises en cybersécurité (Thales, Airbus CyberSecurity...). Il convient également de noter que le ministère de la Défense lui-même a développé une expertise extrêmement forte sur le sujet. C'est l'un des principaux recruteurs de spécialistes en cybersécurité.
3. Des PME, des start-up qui vont développer des activités de service très spécialisées en cybersécurité (en audit par exemple), mais aussi des produits (logiciels, plates-formes d'échanges sécurisées, packages de sécurité...).

– Figure 5 –
Des besoins en cybersécurité différenciés selon la taille et le secteur des entreprises



Source : Apec, 2017

L'ANSSI

Le marché de la cybersécurité est réglementé en partie par l'Agence nationale de la sécurité des systèmes d'information (Anssi). L'Anssi est rattachée au secrétaire général de la défense et de la sécurité nationale. Elle assure une mission de défenseur des systèmes d'information de l'État. À ce titre, elle prescrit des règles en matière de cybersécurité et s'assure de leur mise en application. L'Anssi agrée aussi des entreprises sur le domaine de l'audit sécurité[14], délivre et labellise des formations spécialisées et assure une veille permanente en matière de cybersécurité. ●

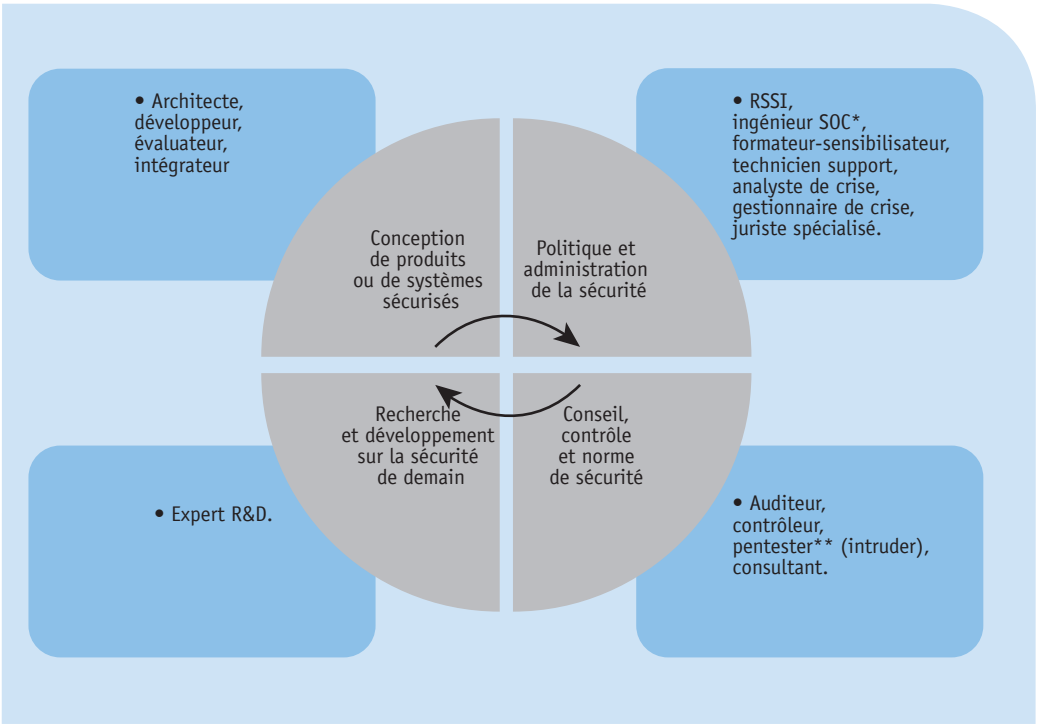
14. En mars 2017, 23 structures ont reçu un agrément pour mener des missions d'audit partielles ou totales, parmi lesquelles Amossys, Airbus Defence and Space, Sopra Steria, Intrinsec Sécurité, Lexsi, Orange Cyberdéfense, Pwc, Sogeti, Thales...

–LES PRINCIPAUX MÉTIERS CADRES DE LA CYBERSÉCURITÉ–

Le Pôle d'excellence cyber a établi un référentiel des métiers de la cybersécurité, que l'on peut articuler autour de quatre grandes familles de métiers[15] **(figure 6)**. La quasi-intégralité de ces métiers est de niveau cadre. La segmentation présentée ci-dessous constitue avant tout une illustration des métiers qu'il est possible d'exercer en lien direct avec la cybersécurité.

15. Travaux du groupe de travail Référentiel du Pôle d'excellence cyber en accord avec les travaux de La nouvelle France industrielle et de l'Anssi.

– Figure 6–
Les métiers de la cybersécurité



Source : Apec, 2017. D'après les travaux du groupe de travail Référentiel du Pôle d'excellence cyber.

* Le SOC (security operation center) est un centre de supervision et d'administration de la sécurité. Il collecte des éléments (par exemple des logs de connexion), détecte des anomalies et propose des réactions.
** Le pentester est un spécialiste des tests d'intrusion (« penetration test » ou « pentest » en anglais). Dans le cadre d'un audit, il pénètre dans un système informatique afin de détecter les failles de sécurité.

Conception de produits ou de systèmes sécurisés

La première famille de métiers est celle de la conception de produits ou de systèmes sécurisés. Elle regroupe les architectes, les développeurs ou encore les intégrateurs. Les premiers formalisent et définissent les choix technologiques d'un système, d'un logiciel répondant à des exigences de sécurité. Les seconds assurent les activités d'ingénierie nécessaires à la réalisation de ces systèmes. Les troisièmes sont chargés des volets sécurité dans ce qui relève de la conception de systèmes d'information. Les évaluateurs font aussi partie de cette famille de métiers. Ce sont eux qui recherchent les vulnérabilités dans un système. Bon nombre d'experts en sécurité informatique et de consultants techniques sont aussi comptabilisés dans cette famille de métiers.

Politique et administration de la sécurité

La deuxième catégorie de métiers est dédiée à l'administration de la sécurité jusque dans la sphère organisationnelle et la gouvernance de l'entreprise. On y retrouve des RSSI destinés à mettre en place des procédures de sécurité dans les entreprises, et à sensibiliser les acteurs aux risques liés à l'utilisation des systèmes d'information. Ce sont des initiateurs de la conduite du changement auprès de tout type de métiers. Leur métier intègre de plus en plus une dimension juridique eu égard aux différentes mesures prises à l'échelle nationale et européenne pour protéger les biens et les personnes. Cette famille de métiers regroupe aussi des analystes chargés d'anticiper les risques pesant sur les systèmes d'information. Ils doivent prioriser les menaces, évaluer leur criticité, pour participer à la mise en place de solutions techniques en cas de défaillances. Leur analyse peut être complétée par celle que mènent des experts sur les impacts d'une cyberattaque sur les systèmes de production industriels. Les problématiques de sûreté des équipements, des outils de contrôle sont autant d'éléments pris en compte par les experts pour définir des process visant à réduire les prises de risque. Des gestionnaires de crise complètent cette catégorie de métiers. Ils définissent les conduites à adopter en cas d'attaque (mise en sécurité des réseaux, plan de reprise de l'activité, collecte de preuves, stratégies de communication...). Ils peuvent être accompagnés de juristes spécialisés en droit des technologies de l'information et de la communication.

Contrôles et normes de sécurité

La troisième famille de métiers est spécifique aux contrôles. Elle est composée d'auditeurs intervenant depuis la prise en compte des process de sécurité jusqu'à la réponse à incident. Ces postes sont rarement internalisés du fait des normes qui contraignent les entreprises à faire appel à des organismes certifiés pour la réalisation d'audits. On y retrouve aussi des profils dont la spécificité est d'identifier les vulnérabilités d'un système comme les pentesters[16].

Penser la cybersécurité de demain

Enfin, un dernier type de métier peut être identifié. Il s'agit du métier hautement qualifié d'expert R&D dont les travaux et références académiques permettent d'imaginer ce que sera la cybersécurité de demain. Il a la charge d'identifier des technologies à venir susceptibles d'avoir une incidence sur l'univers de la cybersécurité, notamment les technologies de rupture pouvant devenir des relais de croissance pour la filière.

Mais la cybersécurité n'est pas du seul ressort de spécialistes du domaine. Elle peut être perçue comme un domaine transverse plus que comme un métier. C'est le cas dans les petites entreprises, où il n'existe pas de besoins ni de moyens pour des profils dédiés à temps plein, et où des dirigeants ou des informaticiens comptent parmi leurs missions d'œuvrer à la sécurisation du système d'information, sans que cela ne constitue véritablement une dominante de leur métier. De la même façon, dans les grandes entreprises, elle est considérée comme une compétence et des bonnes pratiques à acquérir, et ce à n'importe quel échelon et poste que ce soit. D'où l'idée communément partagée qu'il faille assurer la montée en compétences de tout un chacun en ce domaine, et que les besoins sont particulièrement forts à ce niveau **(encadré 4)**. •

16. Le pentester est un spécialiste des tests d'intrusion (« penetration test » ou « pentest » en anglais). Dans le cadre d'un audit, il pénètre dans un système informatique afin de détecter les failles de sécurité.

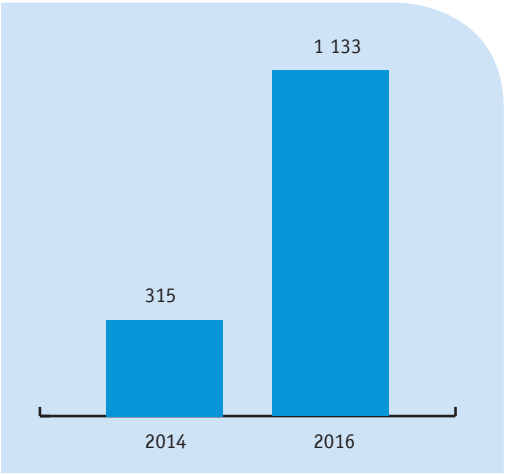
– Encadré 4 –
Verbatim

« Il y a une problématique "expertise" versus "généraliste". Certains profils très spécialisés peuvent avoir des difficultés à se placer parce que les entreprises cherchent des généralistes. Elles peuvent avoir peur de profils trop spécialisés. Elles ne savent pas ce sur quoi elles vont les faire travailler sachant qu'ils ne seront pas forcément à 100 % sur une problématique cybersécurité. »
(Expert).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

–DES OFFRES D'EMPLOI EN NETTE PROGRESSION–

– Figure 7 –
Offres d'emploi diffusées par l'Apec en 2014 et 2016 pour des postes en cybersécurité



Source : Apec, 2017

L'ensemble des études disponibles font état d'une forte progression de l'emploi depuis quelques années pour les métiers dédiés à la cybersécurité. Et ces mêmes études tablent sur une poursuite de cette dynamique dans les années à venir[17]. L'évolution du nombre d'offres diffusées par l'Apec pour des postes de cadres en cybersécurité témoigne également de cette tendance. Le nombre d'offres d'emploi diffusées par l'Apec pour des postes en cybersécurité a été multiplié par 4 entre 2014 et 2016, passant de 315 offres à 1 133 offres **(figure 7)**. Ces offres ont été repérées à partir de l'intitulé du poste proposé par les entreprises (cf. méthodologie en annexe). Les offres diffusées par l'Apec en 2016 concernent en premier lieu les métiers de consultant cybersécurité (20 % des offres) et de RSSI (10 %).

17. Cf. par exemple Pipame, *Le secteur industriel français de cybersécurité,* janvier 2016.

–LA BRETAGNE, UN TERRITOIRE « CYBER »–

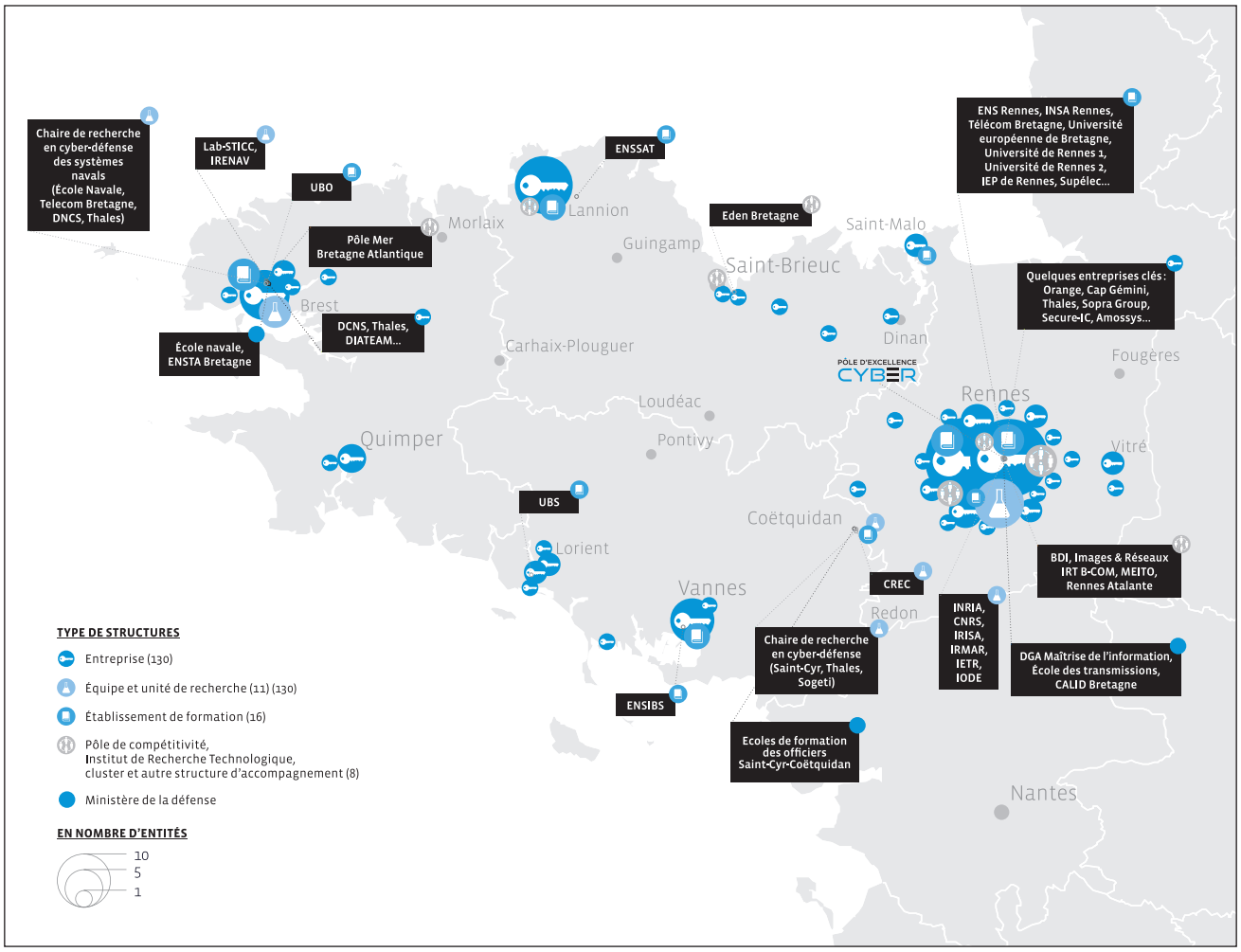
Les télécommunications et l'électronique sont des secteurs emblématiques de l'activité cadre en Bretagne. 6 % des cadres bretons travaillent dans ces deux secteurs, ce qui est deux fois plus que la proportion nationale[18]. Ceci est lié à la politique menée dans les années 1960-1970 de faire de la Bretagne une place forte sur ces secteurs. La délocalisation du Centre national d'études des télécommunications à Lannion, l'implantation du Centre commun d'études de télédiffusion et télécommunications à Rennes puis de la direction technique de Transpac (filiale de France Télécom), sont quelques-uns des événements qui ont permis à la région de se construire cette identité. La Bretagne confirme actuellement cette spécificité, avec la présence sur son territoire d'importants sites : Orange, Thales, STMicroelectronics, Oberthur Technologies, Sagem Défense, Nokia… En lien avec ces secteurs, l'informatique est également une spécificité forte du tissu cadres en Bretagne, en particulier à Rennes. Les labellisations, d'une part, de Rennes / Saint-Malo et, d'autre part, de Brest, Lannion, Morlaix et Quimper au rang des French Tech nationales démontrent l'ancrage breton dans ce domaine.

Forte de ce positionnement, la Bretagne a fait des technologies pour la société numérique un de ses axes d'innovation stratégique. Internet du futur, images et contenus, conception logicielle, modélisation numérique, réseaux convergents mais aussi cybersécurité sont ainsi identifiés comme des axes majeurs de développement économique pour la région.

Il existe un véritable écosystème breton favorable à la montée en puissance de la filière cybersécurité. En dehors de l'Île-de-France, la Bretagne est d'ailleurs la seule région française à disposer sur son territoire d'une infrastructure aussi riche que complexe[19], celle-ci bénéficiant à la fois de l'implantation ancienne de centres étatiques (en particulier les équipes de la DGA-MI : Direction générale de l'Armement – Maîtrise de l'information), de la présence d'acteurs privés majeurs dans ce domaine et d'un tissu dense de centres de formation et de recherche **(figure 8)**. Ainsi, initié par le ministère de la Défense et la Région Bretagne en 2014, le Pôle d'excellence cyber, qui a pris naissance en Bretagne, a pour mission d'accompagner au niveau national le développement de la filière de cybersécu-

18. Données Insee, base Activité professionnelle du recensement, 2012. Traitement Apec.
19. L'Usine Nouvelle, *Cybersécurité : les 40 sites stratégiques*, n° 3452, 21 janvier 2016.

– Figure 8–
Les acteurs clés de la cybersécurité en Bretagne



Source : BDI, 2016-2017.

rité et de cyberdéfense sur les trois piliers indissociables que sont la formation, la recherche et le développement industriel. Pour ce qui concerne la Bretagne, les forces en présence se déclinent ainsi pour ces trois piliers :

- Formation : une dizaine d'établissements d'enseignement supérieur proposent des formations initiales et continues à la cybersécurité, dont certaines de premier plan.
- Recherche : 200 chercheurs travaillent sur la cybersécurité en Bretagne au sein de centres de recherche de haut niveau.
- Développement économique : de grands groupes sont implantés sur le territoire, ainsi qu'un tissu de PME/ETI innovantes.

Bretagne Développement Innovation[20] recense 130 entreprises bretonnes travaillant dans le domaine de la cybersécurité, dont 50 pour lesquelles la cybersécurité constituerait l'activité principale (« pure-players »).

On retrouve cette spécificité bretonne autour de la cybersécurité dans les offres d'emploi diffusées par l'Apec. Ainsi, 9 % des offres pour des postes en cybersécurité diffusées en 2016 sur Apec.fr concernent la Bretagne **(tableau 1)**, ce qui représente une centaine d'offres. C'est la troisième région qui propose le plus d'offres d'emploi en cybersécurité, loin derrière l'Île-de-France (59 % des offres) mais juste derrière l'Occitanie (11 %) et devant des régions de taille importante comme Auvergne-Rhône-Alpes, Provence-Alpes-Côte d'Azur, Hauts-de-France ou Nouvelle-Aquitaine.

20. BDI, *Segmentation de l'offre et cartographie des acteurs de la cyber en Bretagne*, 2016-2017.

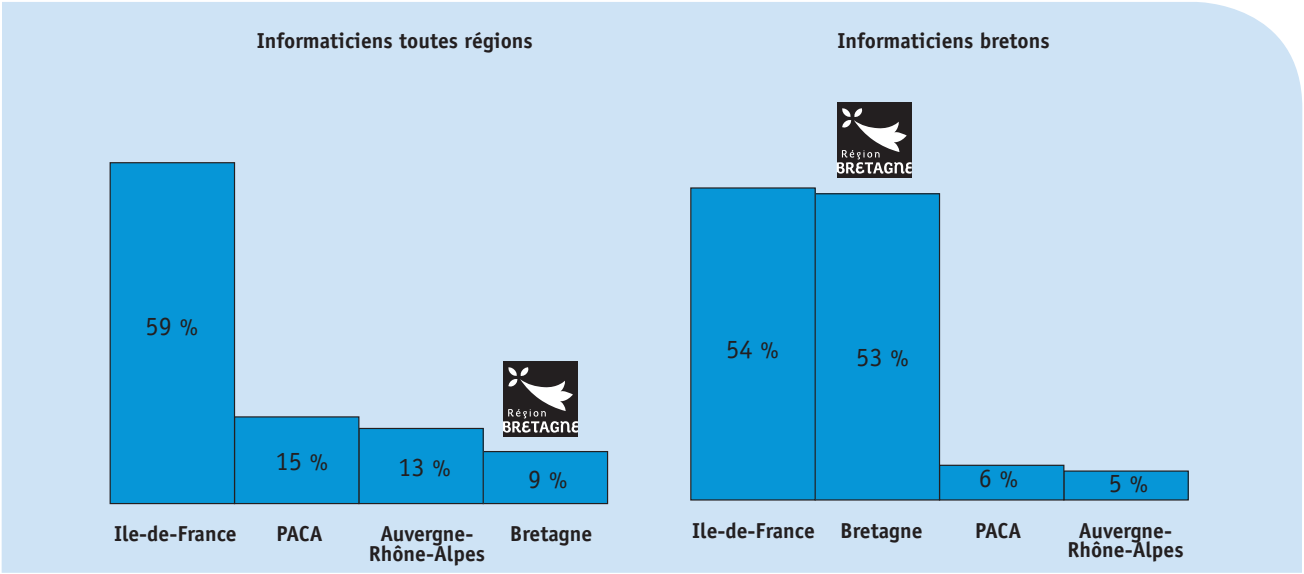
– Tableau 1–
Les offres diffusées sur Apec.fr concernant des postes en cybersécurité en 2016 selon la région

Régions	% d'offres
Île-de-France	59 %
Occitanie	11 %
Bretagne	9 %
Auvergne-Rhône-Alpes	6 %
Provence-Alpes-Côte d'Azur	6 %
Hauts-de-France	3 %
Nouvelle-Aquitaine	2 %
Pays de la Loire	2 %
Grand Est	1 %
Centre - Val de Loire	< 1%
Normandie	< 1%
Bourgogne-Franche-Comté	< 1%
Corse et DOM	0%
Total	**100 %**

Source : Apec, 2017.

L'excellence bretonne en matière de cybersécurité est reconnue. Ainsi, les informaticiens bretons interrogés par l'Apec citent la Bretagne en 2e position des régions françaises qu'ils jugent particulièrement à la pointe en matière de cybersécurité, juste derrière l'Île-de-France **(figure 9)**. Les actions entreprises en Bretagne en matière de cybersécurité trouvent donc un écho au sein de la population des informaticiens résidant sur le territoire. De surcroît, cette réputation dépasse les frontières de la région, les informaticiens français plaçant la Bretagne au 4e rang des régions les plus à la pointe sur la cybersécurité, devant des régions comme l'Occitanie ou les Hauts-de-France. Il convient toutefois de nuancer ce point en notant qu'un tiers des informaticiens interrogés ont indiqué ne pas savoir répondre à cette question. ●

– Figure 9–
Les régions les plus à la pointe en matière de cybersécurité selon les informaticiens (deux réponses possibles)



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

–3–

–CYBERSÉCURITÉ EN BRETAGNE : REGARDS CROISÉS ENTREPRISES / CADRES INFORMATICIENS–

La Bretagne a constitué un écosystème autour de la cybersécurité, associant grands acteurs publics et privés, entreprises innovantes, centres de recherche et organismes de formation. La demande de compétences sur le domaine est donc très importante. Les entreprises bretonnes ont ainsi été interrogées quant à leurs besoins, aux métiers recherchés et aux difficultés qu'elles pouvaient rencontrer lors des recrutements. Les informaticiens bretons ont quant à eux été questionnés sur leur vision du marché de l'emploi, leur niveau de compétences en cybersécurité, l'attractivité que revêtait pour eux ce domaine et leur souhait de monter en compétences sur ce sujet. Le regard croisé entre les entreprises bretonnes et les informaticiens présents dans la région permet de mettre en évidence l'intérêt pour tous d'une montée en compétences en cybersécurité des informaticiens bretons. Des informaticiens d'autres régions ont par ailleurs été interrogés sur les mêmes questionnements. Cela permet de mettre en évidence certaines singularités propres au marché de l'emploi en cybersécurité en Bretagne.

–UN MARCHÉ DE NICHE EN EXPANSION–

Tous les documents l'affirment, le marché de la cybersécurité est en voie d'expansion. Les acteurs de la cybersécurité en Bretagne formulent des annonces concrètes en matière de perspective d'embauche, venant ainsi étayer cette affirmation. En 2017, 90 recrutements sont ainsi attendus à la DGA-MI et une cinquantaine chez Orange Cyberdéfense. Des embauches sont aussi annoncées sur le site Nokia de Lannion, chez Thales ou dans les grandes ESN présentes en Bretagne (Sopra Steria, Sogeti…). Côté PME bretonnes, des embauches sont aussi annoncées : par exemple entre 5 et 10 par an chez Amossys[21]. Entre 2014 et 2016, BDI a recensé plus de 66 emplois créés dans les 119 TPE/PME bretonnes du secteur soit une augmentation de plus de 7 %.

Ces recrutements – bien que représentant une part modeste du marché de l'emploi numérique et donc une véritable « niche » – témoignent du potentiel généré par l'activité cybersécurité.

La plupart des entreprises interrogées considèrent que cette activité n'est pas près de se tasser, eu égard aux besoins grandissants dans le domaine. Dans ce contexte, former des ingénieurs et des cadres à la cybersécurité garde tout son sens. Il n'y a pas d'effet « bulle » attendu sur ce marché, la structuration du marché de la cybersécurité ayant permis de réguler la problématique de l'offre et de la demande, protégeant le secteur de tout risque d'inflation **(encadré 5)**.

21. Chiffres annoncés dans : Acteurs publics (26/01/2016) et Ouest-France (25/01/2016) pour DGA-MI ; Le Télégramme (24/11/2016) pour Thalès ; Rennes-Atalante technopole (21/10/2016) pour Orange Cyberdéfense ; Portail de l'innovation Bretagne (19/04/2016) pour Amossys ; Ouest France (12/12/2016) pour Nokia.

– Encadré 5–
Verbatim

« Il y a de plus en plus besoin de cybersécurité. C'est un vecteur pour assurer la démocratie, la vie sociétale. De plus en plus de choses critiques sont en ligne. La cybersécurité c'est la régulation du net. Dans un village, il y a besoin d'un shérif, d'un pompier. Plus le village s'agrandit, plus il y a besoin de personnes chargées de la sécurité. »
(Expert).

« Aujourd'hui, on est dans une bulle. Mais cette bulle ne risque pas d'éclater. C'est une bulle en ciment. »
(Petite entreprise).

« L'effet bulle a été évité grâce à la structuration du marché, notamment des offres de formation. La mise en place de certifications, de prestataires agréés a également permis d'éviter l'effet bulle. »
(Expert).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

La cybersécurité constitue ainsi un domaine porteur pour l'emploi informatique et devrait continuer à se développer dans les années à venir. Les informaticiens en sont convaincus. Invités à juger sur une échelle de 0 à 10 si la cybersécurité constitue aujourd'hui un secteur porteur pour l'emploi, 29 % d'entre eux attribuent une note de 8, 9 ou 10. Mais si on leur demande d'attribuer une même note en se projetant dans 3/5 ans, la proportion grimpe à 69 % **(tableau 2)**. Les informaticiens bretons attribuent sur ce point des notes très proches de celles relevées pour l'ensemble des informaticiens interrogés. Ainsi, les informaticiens, quelle que soit leur région de résidence, indiquent une note moyenne de 6 sur 10 pour qualifier l'aspect porteur de la cybersécurité aujourd'hui contre 8 sur 10 s'ils se projettent d'ici 3 à 5 ans. ●

– Tableau 2 –

Sur une échelle de 0 à 10, diriez-vous que la cybersécurité est un secteur porteur pour l'emploi (0 pas du tout porteur, 10 très porteur) ?

	Informaticiens toutes régions		Informaticiens bretons	
	Pour aujourd'hui	D'ici 3 à 5 ans	Pour aujourd'hui	D'ici à 3 à 5 ans
10	9%	22%	8%	21%
9	5%	22%	5%	24%
8	15%	25%	17%	26%
7	19%	14%	22%	10%
6	19%	7%	17%	8%
5	13%	6%	14%	5%
Moins de 5	20%	4%	17%	6%
Note moyenne	**6 / 10**	**8 / 10**	**6 / 10**	**8 / 10**

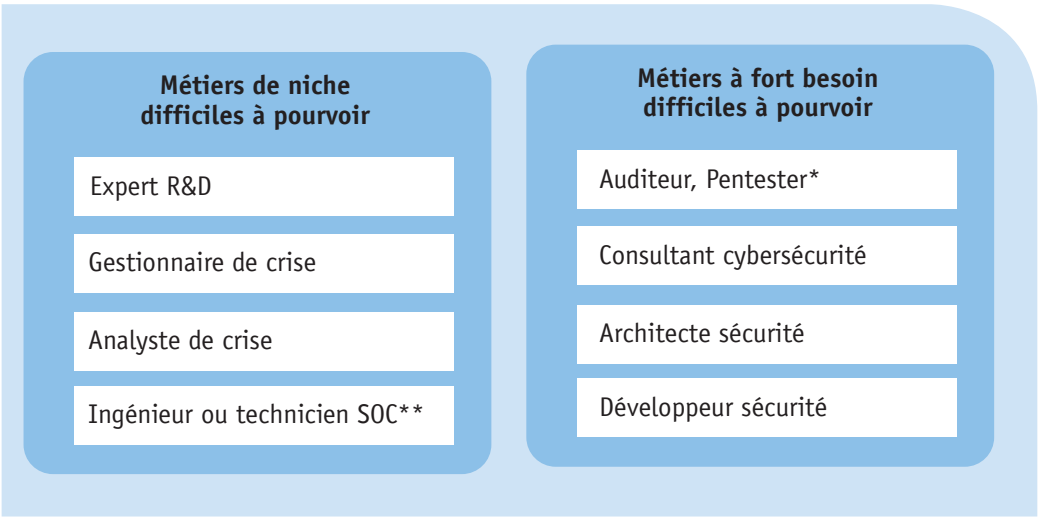
Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

–LE DÉFI DU RECRUTEMENT ET DE LA FIDÉLISATION–

LA CYBERSÉCURITÉ : UN MARCHÉ DE L'EMPLOI TENDU

Les entreprises bretonnes indiquent toutes rencontrer des difficultés à recruter des spécialistes en cybersécurité. Leurs difficultés concernent globalement l'ensemble des métiers de la cybersécurité, qu'il s'agisse de métiers de niche ou de métiers à forts volumes de recrutement **(figure 10)**. L'essentiel des difficultés concerne des métiers de niveau cadre. Toutefois, certaines entreprises évoquent également le besoin de mise en œuvre plus opérationnelle des solutions de cybersécurité (installation chez les clients de solutions par exemple, supervision), qui peuvent relever du niveau technicien.

– Figure 10–
Typologie des principaux besoins à pourvoir sur le marché breton de la cybersécurité



Source : Apec, 2017

*Le pentester est un spécialiste des tests d'intrusion (« penetration test » ou « pentest » en anglais). Dans le cadre d'un audit, il pénètre dans un système informatique afin de détecter les failles de sécurité.
** Le SOC (security operation center) est un centre de supervision et d'administration de la sécurité. Il collecte des éléments (par exemple des logs de connexion), détecte des anomalies et propose des réactions.

Les métiers de niche difficiles à pourvoir

Des métiers de niche sont touchés par ces difficultés. C'est le cas des profils d'experts R&D et de gestionnaires de crise. Il s'agit de postes prisés essentiellement par les très grandes entreprises. Les candidatures sont rares car ils demandent une expertise peu commune et une expérience forte qui empêchent les jeunes d'être éligibles aux postes. Ce sont aussi, pour certains de ces métiers, des postes qui nécessitent de comprendre la sphère organisationnelle des entreprises pour définir des scénarios de crise (identification des risques, réponses aux crises...).

Les métiers à fort besoin difficiles à pourvoir

D'autres métiers, à fort besoin de recrutement, souffrent également d'une pénurie de candidats. C'est le cas de métiers qui peuvent potentiellement concerner toutes les entreprises quel que soit leur secteur d'activité (comme les profils d'architectes sécurité par exemple) ou qui sont liés essentiellement aux entreprises spécialisées en cybersécurité (comme les profils d'auditeurs ou de consultants). Dans certains cas, l'attractivité du métier peut être en cause dans la difficulté des entreprises à trouver des candidats. La taille de l'entreprise et son secteur d'activité peuvent également jouer un rôle, certaines structures réussissant davantage que d'autres à capter et à retenir les candidats **(encadré 6)**.

– Encadré 6 –
Verbatim

« Les métiers d'architecte et d'auditeur : c'est là que les tensions sont les plus fortes. Il y a globalement un manque de ressources à l'échelle régionale et nationale. Aujourd'hui, il n'y a pas assez de diplômés par rapport aux besoins. »
(Grande entreprise).
« Sur le métier d'auditeur, on a de gros besoins. »
(Grande entreprise).
« Il y a une demande très forte sur les métiers de consultants. »
(Petite entreprise).
« Le métier d'architecte est complexe et peu attractif car connoté trop technique. Or les jeunes se projettent plus sur l'envie de devenir manager. Ils sont peu attirés par le côté technique. »
(Grande entreprise).
« Il y a une pénurie sur les développeurs en général. Les développeurs sécurité : ce serait un vrai plus mais c'est très utopique. Les profils sont rares... Les développeurs qui sont actuellement en place sont sortis de l'école il y a 10 ans, et ils n'ont pas ce socle de compétences-là. »
(Petite entreprise).
« On a un métier avec une continuité de services : 24h sur 24, 7 jours sur 7, 365 jours par an car les systèmes d'information comme les sites Internet ou Web ne peuvent pas s'arrêter... Donc ce n'est pas forcément attirant parce que la génération Y ou Z n'a pas forcément cette amplitude du service à tout prix. »
(Grande entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

UNE TENSION GLOBALE DU MARCHÉ DE L'EMPLOI INFORMATIQUE

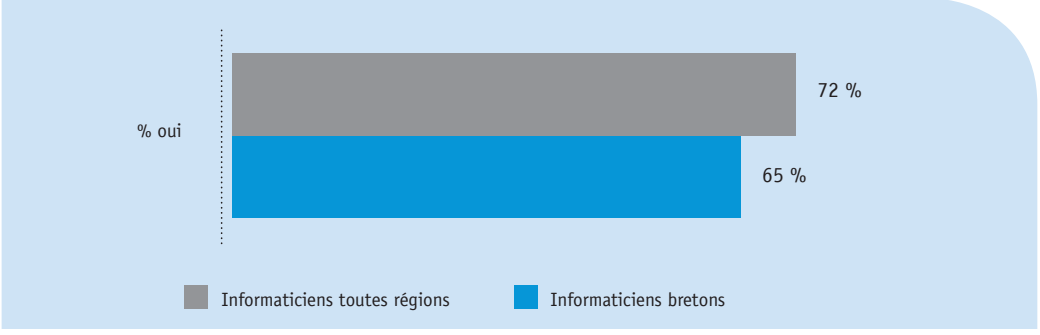
D'une manière générale, les entreprises souhaitant recruter des cadres de l'informatique se livrent à une véritable concurrence. Ainsi, les entreprises en cybersécurité ne sont pas les seules à rencontrer des difficultés à recruter. Dans la dernière enquête sur les Besoins en main-d'œuvre publiée par Pôle emploi, près de 63 % des entreprises disent éprouver des difficultés à recruter des ingénieurs spécialisés en maintenance informatique, des cadres d'étude, R&D en informatique, et des chefs de projets informatiques, les difficultés étant de l'ordre de 61 % en Bretagne[22]. Pour les entreprises spécialisées dans les activités informatiques, les recrutements sont également tendus. Selon le baromètre publié conjointement par l'Apec et Syntec Numérique, 64 % d'entre elles ont ressenti des difficultés en la matière sur l'année 2016, cette proportion étant plus élevée qu'en 2015[23].

Les cadres informaticiens ressentent ce dynamisme. 72 % d'entre eux (65 % en Bretagne) jugent que le marché de l'emploi informatique dans leur région est porteur **(figure 11)**. Ils sont également une majorité à penser qu'il est facile de trouver un emploi dans l'informatique dans leur région **(figure 12)**. Toutefois, la proportion d'informaticiens jugeant que cela est difficile est loin d'être négligeable, surtout chez les plus âgés. 74 % des informaticiens de moins de 30 ans jugent facile de trouver un emploi dans leur région, contre seulement 31 % des informaticiens âgés de 50 ans et plus.

Ainsi, beaucoup d'informaticiens ont exprimé spontanément leur sentiment d'exclusion du marché de l'emploi : « *Ce n'est pas les postes qui manquent, c'est plutôt qu'ils ne cherchent pas les personnes de plus de 50 ans.* » ; « *Mon profil semble trop expérimenté et sénior par rapport aux opportunités dans la région.* » ; « *Cela devient difficile lorsque l'on a plus de 50 ans et aussi lorsqu'on est une femme.* » ; « *51 ans, considéré comme sénior...* ».

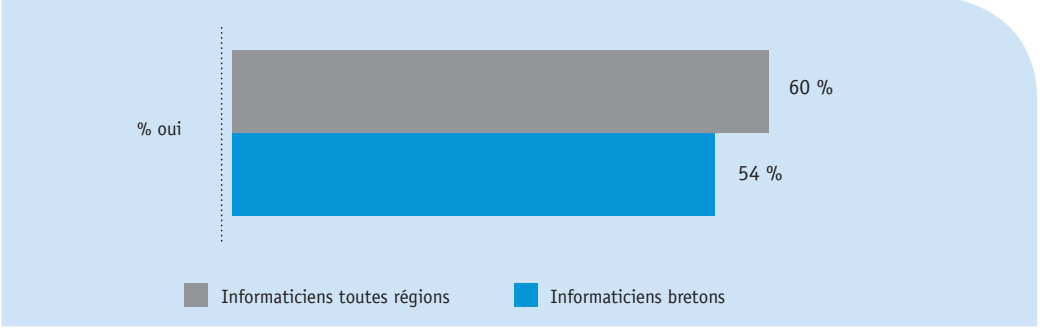
22. Source : BMO 2017.
23. *Le marché de l'emploi cadre dans les activités informatiques, Apec / Syntec numérique*, novembre 2016.

– Figure 11 –
Considérez-vous que le marché de l'emploi informatique dans votre région est dynamique et porteur ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

– Figure 12 –
Trouver un emploi dans le domaine de l'informatique dans votre région est-il globalement facile ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

DES STRATÉGIES POUR RECRUTER ET POUR FIDÉLISER

Malgré ces difficultés, les entreprises de la cybersécurité parviennent à embaucher, en multipliant les canaux de recrutement et en tentant de renforcer leur attractivité sur le marché.

Pour ces entreprises, les principaux opérateurs de l'emploi sont jugés comme des relais peu efficaces en matière de sourcing et de recrutement. Aussi, la publication d'offres d'emploi sur des sites généralistes n'est pas systématique. Elle est toutefois régulièrement utilisée, notamment par les grands groupes, pour affirmer un positionnement et une visibilité sur le marché. Mais les employeurs préfèrent sur ce secteur recourir au réseau, et notamment leur réseau personnel, pour recruter. Avec la cooptation, cela leur offre des garanties de qualité jugées inégalables **(encadré 7)**.

Pour élargir leurs chances de trouver de bons candidats, les recruteurs font parfois appel à des challenges techniques. Ceux-ci sont perçus comme des alternatives aux modes de sourcing classiques permettant de jauger directement les compétences des candidats. Les challenges de types « hackaton » organisés sur le territoire breton apparaissent extrêmement populaires[24]. À la fois challenge permettant de valoriser les compétences des structures de formation, pré-forum de recrutement pour les entreprises et compétition collective, ce type d'évènements apparait aujourd'hui comme un vecteur intéressant pour mettre en rapport offres et besoins de compétences en cybersécurité sur le territoire régional.

24. À titre d'exemple, le Breizh CTF 2017, organisé par BDI avec plus de 14 entreprises, PME ou grands groupes régionaux, aura vu ses 185 inscriptions closes en moins d'une nuit.

– Encadré 7 –
Verbatim

« On est sur des PME. Ça se fait beaucoup par le bouche à oreille. Il y a quelques dispositifs plus originaux comme des concours de hacking ou de sites qui construisent des profils de spécialistes. »
(Expert).

« Processus de recrutement : un challenge technique (3 heures sur un ordinateur à résoudre un problème et 1 heure de débriefing), un entretien avec le manager (intégration dans l'équipe, éthique, management, etc.) et un entretien de ressources humaines (motivation, adaptabilité, etc.). Le challenge technique est lié à l'activité du poste et a pour but de détecter des potentiels, voir la motivation, l'état d'esprit, la méthode, l'innovation, la recherche de problème. »
(Grande entreprise).

« La cybersécurité, ça échappe un peu aux filières classiques du recrutement. Ça marche par réseau, par connaissances… Pour recruter, on appelle les copains. »
(Petite entreprise).

« C'est le réseau personnel surtout et les réseaux sociaux. Parfois les écoles aussi car nous on est anciens élèves de ces écoles. Il y a un bon moyen : on utilise le stage de fin d'études. Le stage, pour nous, c'est de la pré-embauche. »
(Petite entreprise).

« En 2016 : 500 CV reçus pour 60 postes. La moitié des candidats a été reçue. Tous les postes ont été pourvus. »
(Grande entreprise).

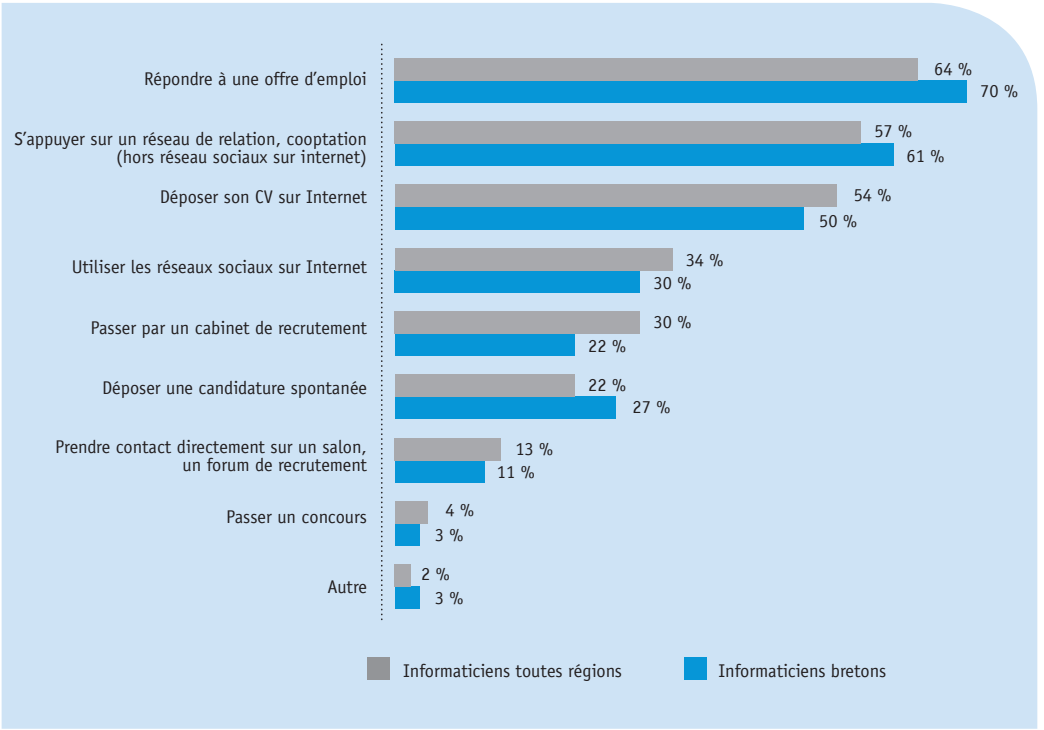
Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

Les cadres informaticiens connaissent la diversité de ces pratiques de recrutement qui semblent concerner toutes les entreprises informatiques quel que soit le domaine[25]. L'offre d'emploi, le réseau de relations et les CVthèques sont jugés par les informaticiens comme les canaux les plus efficaces pour être recruté dans le secteur de l'informatique **(figure 13)**. Il existe quelques différences entre les répondants, notamment du fait de leur âge. Typiquement, le réseau de relations se construisant dans le temps et au fil de l'expérience, son efficacité est davantage soulignée par les cadres informaticiens les plus âgés qui détiennent un cercle de référents auxquels ils peuvent s'adresser. Il n'existe en revanche aucune différence significative sur ce point entre les informaticiens bretons et les informaticiens des autres régions, à l'exception des cabinets de recrutement jugés moins efficaces par les informaticiens bretons. Cela peut s'expliquer par le poids important de l'Île-de-France dans la population des informaticiens interrogés, région où les cabinets de recrutement spécialisés dans l'informatique jouent un rôle important sur le marché.

25. Cf. Apec, *Sourcing Cadres, édition 2016.*

– Figure 13–

Quels sont selon vous les moyens les plus efficaces pour être actuellement recruté dans le secteur de l'informatique ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Les recrutements étant jugés complexes, les entreprises de la cybersécurité cherchent aussi à décliner des stratégies pour fidéliser leurs salariés et limiter le turn-over. La question de la fidélisation pose notamment le problème de la concurrence entre grandes sociétés de services généralistes et PME spécialisées. Malgré les efforts réalisés par les PME, il leur est parfois difficile de rivaliser avec les grands groupes, notamment en termes de salaires.

Le salaire n'est toutefois pas le seul critère de fidélisation. Les entreprises n'hésitent pas à valoriser un certain nombre d'éléments pour se démarquer de la concurrence. Les conditions de travail, la possibilité d'organiser son temps de travail, la liberté dans le choix de l'équipement matériel, les challenges proposés, les technologies utilisées sont autant d'éléments jugés essentiels par les entreprises pour fidéliser leurs salariés **(encadré 8)**. Il s'agit là encore d'une caractéristique commune de beaucoup d'entreprises du domaine informatique. Ainsi, les informaticiens interrogés jugent que les facteurs les plus importants pour rester dans une entreprise sont avant tout l'intérêt des missions, la rémunération proposée et les conditions de travail. ●

– Encadré 8 –
Verbatim

« Il faut les motiver. Le salaire joue, mais pas que. »
(Petite entreprise).
« Chez nous, ils peuvent s'équiper avec ce qu'ils veulent. Après c'est surtout avec les à-côtés type mutuelle, la prise en charge partielle des tickets resto (60 %), des transports. C'est aussi la possibilité de travailler à distance. On a une personne qui a décidé de partir à Orléans et on a accepté qu'il y aille et qu'il ne monte que 2 jours par semaine. On ne le fait pas directement et immédiatement mais on le fait pour des gens dont on sait qu'ils bossent et en qui on a confiance. »
(Petite entreprise).
« Sur le Bassin rennais, la problématique du turn-over a évolué car aujourd'hui il y a plus d'offres cybersécurité. Les entreprises se sont mises à monter des pôles cyber. Donc hier, les employés étaient relativement captifs de structures qui maitrisaient le sujet, aujourd'hui ça explose du fait que beaucoup de choses se créent. La concurrence est plus rude. »
(Petite entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

–L'ATTRACTIVITÉ BRETONNE–

La tension sur le marché de l'emploi informatique en cybersécurité existe en Bretagne mais elle reste limitée par rapport à la région parisienne. Pour les entreprises implantées localement, la Bretagne présente avant tout des avantages, comme de plus grandes facilités à décrocher des financements. La cybersécurité y est identifiée comme un axe de développement stratégique, avec des opportunités de financements, un tissu de formations spécialisées et une certaine visibilité **(encadré 9)**. Les coûts salariaux sont également moins élevés qu'en région Île-de-France[26] et l'attractivité de la région, en termes de qualité de vie notamment, est réelle.

26. Cf. Apec, *Rémunération des cadres, la singularité francilienne*, 2017.

– Encadré 9–
Verbatim

« La chance de la Bretagne, ce sont des coûts de production 20 à 30 % plus faibles qu'en Île-de-France.»
(Grande entreprise).
« On est tous sous pavillon du Pôle d'excellence cyber, ce qui n'est pas forcément un atout en soi, mais qui est identifié et identifiable. Ça permet de se faire bien flécher. »
(Petite entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

De tous les départements bretons, l'Ille-et-Vilaine se démarque plus particulièrement. Son attractivité est d'autant plus forte qu'elle concentre autour de la plate-forme rennaise les plus grands acteurs de la cybersécurité et qu'elle est proche géographiquement du Bassin parisien où sont implantés les sièges sociaux des plus grandes entreprises utilisatrices de services en informatique. En effet, les entreprises rennaises de la cybersécurité ont le plus souvent un rayonnement national voire international. Leur marché s'étend au-delà des frontières régionales. L'agglomération rennaise pourrait de fait être considérée comme une plate-forme de *nearshoring*[27] dans le domaine de la cybersécurité. Certains acteurs soulignent ainsi une forme de fragilité en l'absence sur le territoire de grande spécialité industrielle de pointe pouvant servir de locomotive à la filière de la cybersécurité, comme c'est par exemple le cas de l'aéronautique dans la région de Toulouse[28].

L'agroalimentaire, 1re industrie bretonne, n'est encore que peu sensibilisée aux enjeux de la cybersécurité alors que les risques sont importants : blocage de l'appareil de production, falsification de contrôles sanitaires sur les produits... De son côté, l'industrie automobile, bien implantée en Bretagne, pourrait jouer le rôle d'un vecteur de croissance de l'activité de cybersécurité. En effet, l'avenir de cette industrie passe en partie par une transition numérique (véhicule connecté, véhicule intelligent...) pour laquelle la cybersécurité sera incontournable. Il convient également de rappeler que le secteur de la défense joue en partie ce rôle de moteur de l'activité de cybersécurité dans la région.

27. Le nearshoring, par différence à l'offshoring, est le fait de délocaliser une activité économique, mais dans une autre région du même pays ou dans un pays proche.
28. Meito / Pierre Audoin Consultants, *La cybersécurité en Bretagne*, 2013.

– Figure 14–
Êtes-vous attaché à la région dans laquelle vous résidez ?
Réponse à la modalité « oui »

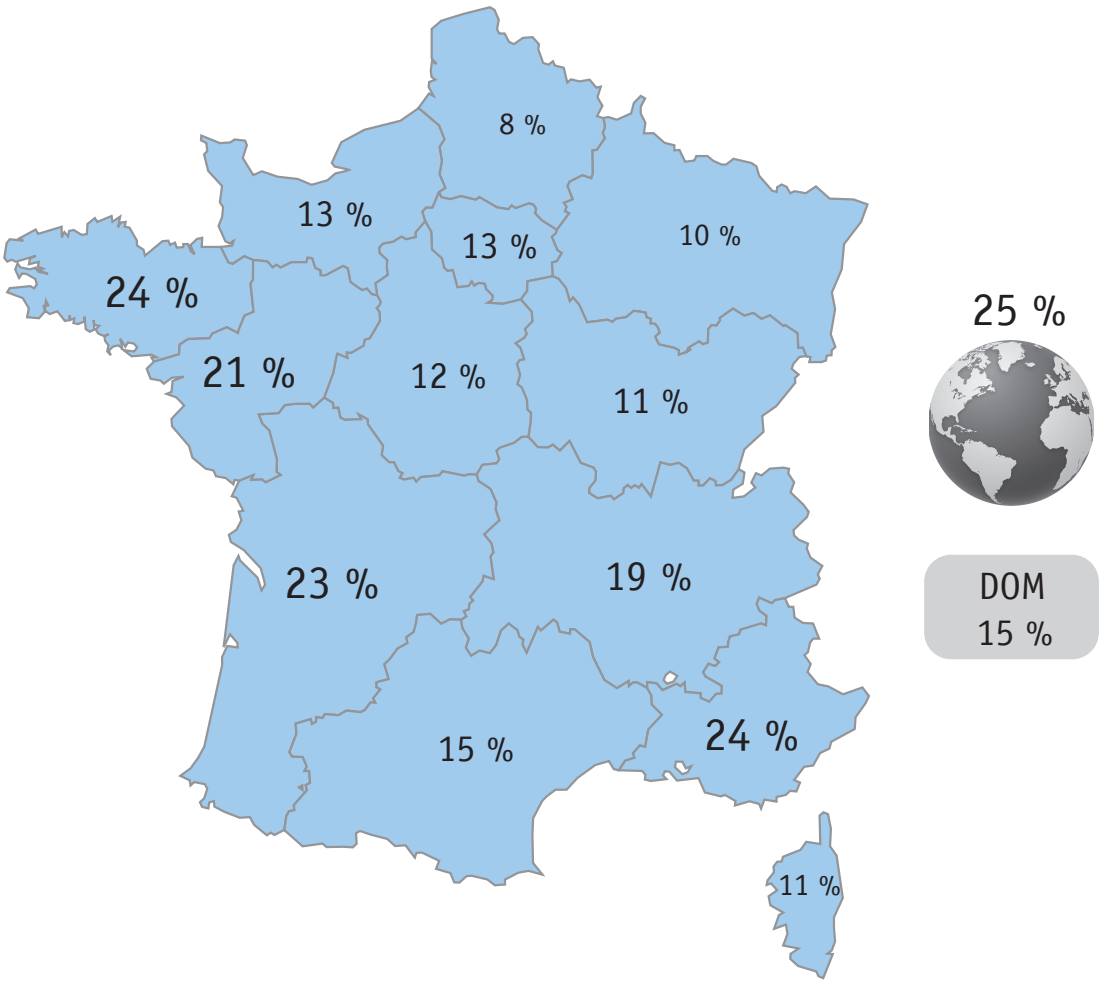
Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

– Figure 15–
Dans le cas d'un changement de poste, accepteriez-vous de déménager dans une autre région ?
Réponse à la modalité « oui »

Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

La Bretagne bénéficie par ailleurs d'une très forte attractivité auprès des cadres informaticiens, ce qui constitue globalement un atout important pour développer la filière numérique en général et donc la cybersécurité. En particulier, l'attachement à la région Bretagne est important, ce qui limite l'éventualité d'une mobilité géographique vers d'autres régions. Ainsi, 86 % des informaticiens bretons se disent attachés à leur région **(figure 14)**, contre 68 % en moyenne en France (et 55 % en Île-de-France). Et seulement 38 % des informaticiens bretons se disent prêts à changer de région contre 52 % en moyenne en France **(figure 15)**. Du fait de ces mêmes atouts, la région attire et intéresse aussi des cadres venus d'ailleurs **(figure 16)**. Elle est, avec Provence-Alpes-Côte d'Azur et la Nouvelle-Aquitaine, la région de prédilection des cadres informaticiens en cas de changement de région, loin devant l'Île-de-France, les Hauts-de-France ou le Grand Est. On peut également noter qu'un quart des informaticiens interrogés se déclarent prêts à déménager à l'étranger. •

– Figure 16–
Régions envisagées par les informaticiens prêts à changer de région en cas de changement de poste
(plusieurs réponses possibles)



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Parmi les informaticiens prêts à changer de région en cas de changement de poste, 24 % envisagent la région Bretagne comme une destination possible.

–LES COMPÉTENCES RECHERCHÉES : UNE EXPERTISE TECHNIQUE AVANT TOUT–

Quel que soit le métier de la cybersécurité concerné, une très bonne culture technique est exigée par les employeurs **(encadré 10)**. Le champ du socle technique requis est potentiellement vaste.

– Encadré 10–
Verbatim

« La cyber est très demandeuse en termes de profils techniques spécifiques et où il faut des bases très saines pour pouvoir exercer dans la cyber et ça va être compliqué de former des gens de but en blanc s'ils n'ont pas été formés a minima. »
(Petite entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

Selon les métiers, certaines de ces compétences se recoupent ou pas. Typiquement, une très bonne connaissance des architectures web et réseaux va être demandée pour un poste d'architecte sécurité comme pour un poste d'auditeur sécurité. Une maîtrise des solutions de sécurité logicielle va également être requise dans les deux cas (Owasp, Cwe/Sans...).
Cependant, le recruteur va attendre d'un auditeur qu'il maîtrise spécifiquement les démarches d'audit (établissement de son périmètre, préparation et exécution de l'audit, élaboration et restauration des résultats...) et qu'il soit un expert dans les outils et principes de test d'intrusion (Nessus, Kali Linux, Metasploit...). Quant à l'architecte, il pourra être plus spécifiquement attendu sur sa maîtrise des systèmes industriels (Scada), son expertise en matière de protection de postes de travail (antivirus, antimalware, chiffrement...) ou en gestion des identités et des accès (IAM).
L'anglais est très souvent requis pour la plupart des postes. Il constitue la première langue de travail dans de nombreux secteurs d'activité. Une expérience des méthodes agile ou des fonctionnements en mode projet peut également être requise par certaines entreprises **(figure 17)**.

– Figure 17–
Exemples de profils requis pour des offres d'emploi concernant des métiers de la cybersécurité publiées par l'Apec

Consultant sécurité

- *Au moins 4 ans d'expérience en cybersécurité.*
- *Une expérience en cabinet de conseil est appréciée.*
- *Maitrise de l'anglais (indispensable).*
- *Compétences en gouvernance, stratégie et politiques de sécurité.*
- *Méthodes d'analyse des risques (ISO 27005, Ebios, etc.).*
- *Compréhension globale de l'architecture en matière de sécurité fonctionnelle et technique.*
- *Connaissance des normes et réglementations principales (ISO 2700X).*
- *Notions sur les techniques de sécurisation, composants et produits de sécurité (pare-feu, pki, SIEM, IAM, ...).*
- *Notions de gestion de projet.*

Architecte sécurité

- *De formation ingénieur Bac +4/5 ou équivalent, vous justifiez de minimum 3 ans d'expérience.*
Vous avez défini ou participé à la définition d'architectures sécurisées pour des grands comptes nationaux et internationaux.
- *Vous maîtrisez les architectures et la mise en oeuvre de solutions techniques visant à sécuriser les postes de travail et serveurs, les terminaux mobiles, les applications, la gestion des identités et des accès (AD/ADFS, LDAP, IAM, PKI, webSSO), les data centres et les infrastructures (sécurité des serveurs et réseaux WAN/LAN, des accès distant/VPN et du stockage, des plates-formes de ToIP/VoIP, détection d'intrusion, solutions de haute disponibilité et environnements virtuels - SDDC).*

Ingénieur cyber

- *Respect de la confidentialité : le poste nécessitant l'accès à des informations pouvant relever du secret de la défense nationale, des habilitations de type « Confidentiel Défense » et/ou « Secret Défense » pourront être requises.*
- *De formation ingénieur ou universitaire Bac+5, vous possédez de solides compétences dans les métiers de la sécurité et des systèmes d'information. Vous devez avoir des connaissances dans les domaines techniques suivants :*
- Connaissances générales en sécurité des systèmes d'information.
- Connaissances de langages de développement (Python , ASM, Perl, C).
- Habitué à travailler dans un environnement complexe.
- Connaissance des systèmes Windows et Linux.
- Analyse de journaux d'événements (système, réseau, applicatif).
- Analyse de protocoles réseaux (wireshark).
- Une certification sur les normes ISO 27001 ou CISSP est un plus.

RSSI

- *Vous êtes diplômé(e) d'une formation supérieure de niveau Bac +5 (Ecole d'Ingénieurs ou cursus universitaire) avec idéalement une spécialisation en sécurité informatique et une certification CISSP ou équivalent.*
- *Vous disposez d'une expérience significative d'au moins 10 ans dans des fonctions similaires acquise dans une société de services ou en entreprise, au sein d'une direction des systèmes d'information avec au moins une expérience en définition et déploiement d'une politique de sécurité des systèmes d'information groupe à configuration multi-sites.*
- *Vous démontrez une forte crédibilité juridique en matière de Sécurité & Droits informatiques.*
- *En véritable professionnel(le) de confiance, vous garantissez un fort niveau de confidentialité des informations sensibles et stratégiques grâce à votre grand sens de la confidentialité, de l'intégrité, et de l'éthique.*
- *Vous êtes reconnu(e) pour vos qualités relationnelles et de communication.*
- *Votre agilité et votre ouverture d'esprit vous permettent de comprendre les métiers et leurs contraintes.*
- *Vous parlez anglais couramment.*

Auditeur sécurité

• Titulaire d'un diplôme de niveau Bac +5 (ingénieur, master 2 ...), expérimenté.
• Vous disposez de compétences sur l'un ou plusieurs des sujets suivants : systèmes d'exploitation Windows et Linux, systèmes d'exploitation temps réel, systèmes de contrôle industriels (ICS, SCADA), réseaux, applicatifs, produits et solutions de sécurité, systèmes de supervision de la sécurité, sondes et systèmes de détection d'intrusion. Vous êtes également familiarisé avec les domaines suivants : technique d'audit, technique d'entretien, SMSI (2700x,...), méthodes d'analyse de risque (EBIOS...), réglementation SSI.
• Vous possédez des connaissances sur les principales technologies de l'information et votre intérêt pour la sécurité informatique vous incite à développer vos compétences par une veille régulière dans le domaine de la cybersécurité.
• D'un naturel curieux, vous avez de bonnes facultés d'adaptation, un très bon relationnel et le goût du travail en équipe. Les déplacements réguliers (environ 10 semaines par an) ne vous posent pas de problème.
• Une expérience en audit de sécurité ou RSSI serait un plus.

Ingénieur SOC

• De formation ingénieur ou universitaire en informatique, vous disposez d'une première expérience au sein d'un SOC. Vous disposez également des compétences et connaissances suivantes :
- Utilisation avancée d'un outil SIEM (Splunk, Arcsite...).
- Utilisation des sondes IDS/IPS.
- Adaptation des IOC au besoin client (contextualisation).
- Protocoles réseau et outils de trace.
- OS Linux, Unix, Windows.
- Langages de script.
- Connaissance des interactions entre SOC, CSIRT et NOC dans la remédiation.

Source : Apec, 2017, offres publiées en 2016 sur Apec.fr.

De surcroît, les menaces, les technologies et environnements professionnels évoluent : traitement en temps réel des systèmes de contrôle des machines, objets connectés, nomadisme... Côté organisationnel, on rencontre des entreprises qui redéfinissent les modes de pilotage de certains projets informatiques. Aussi, les entreprises recherchent des spécialistes de la cybersécurité en capacité de réaliser de la veille et de tenir compte des contextes évolutifs qui les entourent pour définir des mesures défensives et correctives adaptées. Elles doivent en conséquence assurer la montée en compétences de leurs ressources face à ces différentes mutations **(encadré 11)**. •

– Encadré 11–
Verbatim

« On s'aperçoit aussi qu'on travaille de plus en plus avec la sûreté et moins avec les DSI. Dans certains grands groupes industriels, les réflexions et modifications d'urbanisme et ce qui fait la partie nouvelle de la cyber, c'est en train de migrer de pilotage. La DSI est plutôt orientée vers des offres de production, et ce qui est de l'ordre de l'innovation est en train de migrer parfois vers la direction du digital. Cela est important, nous on l'anticipe aussi. »
(Petite entreprise).
« Les ingénieurs techniques doivent entretenir leurs compétences de manière permanente. Ils doivent pratiquer, faire de la veille, de l'expérimentation. Ce sont des domaines où les connaissances se perdent vite, ce qui peut poser un frein à la mobilité. Il existe pour eux une prise de risque à se désinvestir, à passer du côté organisationnel, puisqu'ils auront plus de difficulté à revenir en arrière. »
(Expert).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

–DES SAVOIR-ÊTRE À CONSOLIDER–

Au-delà de leurs compétences techniques, les candidats sont aussi attendus sur leur état d'esprit. Ainsi, l'éthique et le sens du service sont considérés par les entreprises comme des qualités essentielles pour travailler dans la cybersécurité. La curiosité, l'agilité ou le sens relationnel sont également des aptitudes personnelles à mobiliser dans l'univers professionnel d'un futur spécialiste de la cybersécurité. Ces qualités rompent avec les représentations que certains peuvent se faire des métiers de la cybersécurité montrant un certain isolement centré uniquement sur la technique (l'image du « geek »). Pourtant, elles constituent des compétences clés, surtout pour les métiers qui font intervenir la relation client. Dans les métiers de l'administration des politiques de cybersécurité, une aptitude à comprendre et à se saisir des modes d'organisation des entreprises est aussi jugée indispensable par les employeurs **(encadré 12)**.

– Encadré 12–
Verbatim

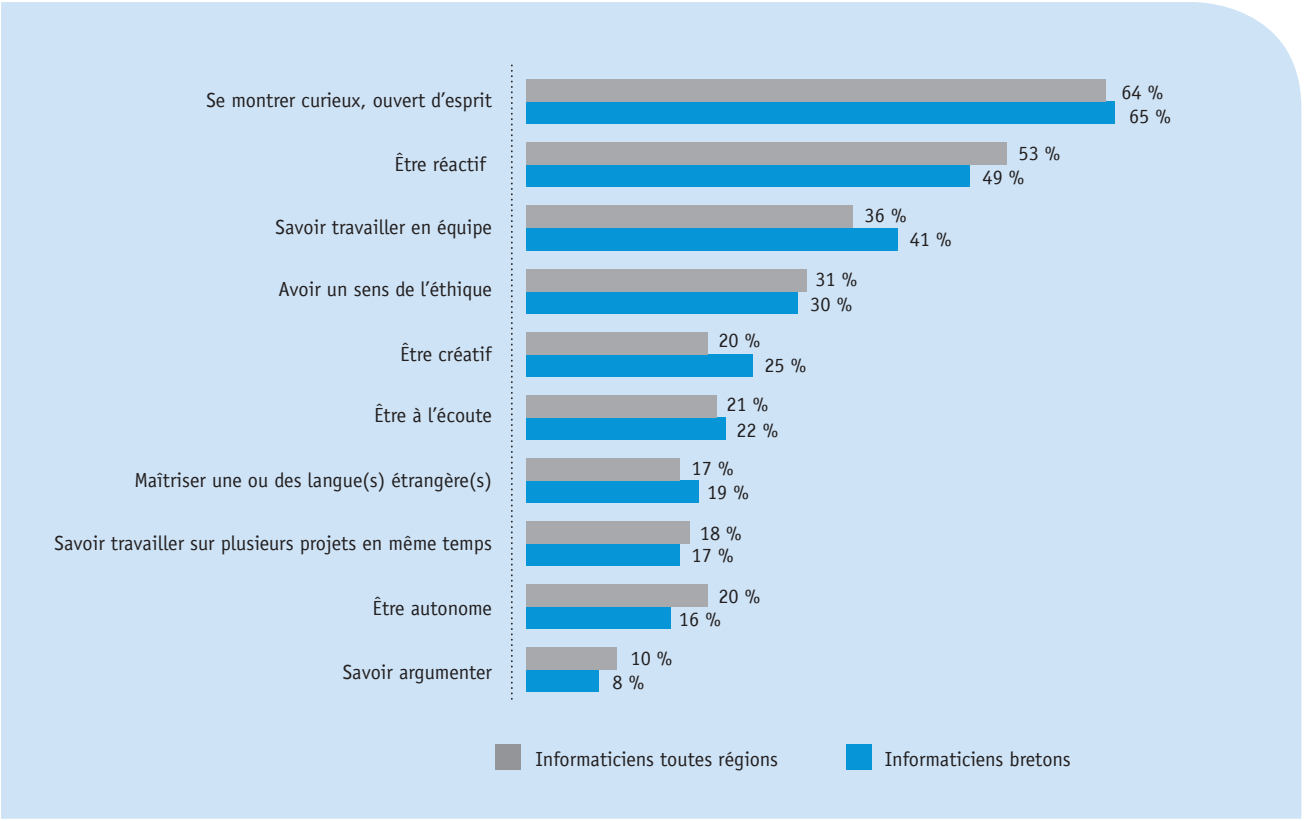
« Les profils que l'on aime bien, ce sont les gens qui savent prendre du recul, garder la tête froide. De pouvoir aussi se mettre à la place d'un attaquant. Par exemple, un pentester doit imaginer des manières de rentrer. Il faut de la créativité. Il faut aussi être capable de plaider, de soutenir, d'argumenter un rapport devant un conseil d'administration. Ça va jusque-là lorsqu'à l'issue d'un audit vous remettez en cause l'architecture d'un système qui a coûté des millions. Il faut savoir vulgariser ses résultats auprès de personnes qui ne sont pas techniques. »
(Petite entreprise).
« La cyberdéfense, c'est l'art de protéger des pépites nationales face à des cyberattaques. Donc c'est un métier d'engagement, un métier de passion pour pouvoir protéger les entreprises en permanence face à tout ce qui peut leur arriver. Ce n'est pas un métier froid. Ce n'est pas qu'un métier technique, même s'il y a beaucoup de technique. Il y a du management, de l'organisationnel, de la méthodologie. »
(Expert).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

Les entreprises considèrent ces savoir-être comme des qualités globalement difficiles à acquérir par la formation. Le recours au réseau de relations et à la cooptation pourrait leur permettre de détecter plus facilement ces différentes aptitudes personnelles et professionnelles lors d'une nouvelle embauche.

Les informaticiens, qu'ils aient ou non des compétences techniques dans le champ de la cybersécurité, reconnaissent globalement la nécessité de se montrer curieux et réactif pour exercer dans le domaine de la cybersécurité. En revanche, les autres qualités ne sont pas jugées autant indispensables **(figure 18)**. Différents aspects soulevés par les entreprises interrogées comme importants pour travailler dans la cybersécurité, comme la maîtrise des langues étrangères ou le fait de posséder des qualités d'argumentation, ne sont pas perçus tels quels par les informaticiens.
Interrogés sur leur niveau de compétences sur ces différents aspects, la grande majorité des informaticiens se considèrent comme curieux, réactifs, autonomes, sachant travailler en équipe ou ayant un sens de l'éthique. Ils se sentent en revanche moins à l'aise sur la maîtrise des langues étrangères, la créativité et la capacité à argumenter. Ces points constituent donc des points de progrès à travailler pour les informaticiens qui souhaiteraient travailler dans la cybersécurité. ●

– Figure 18–
Pour travailler dans la cybersécurité, pensez-vous qu'il faille... ? (% de oui)



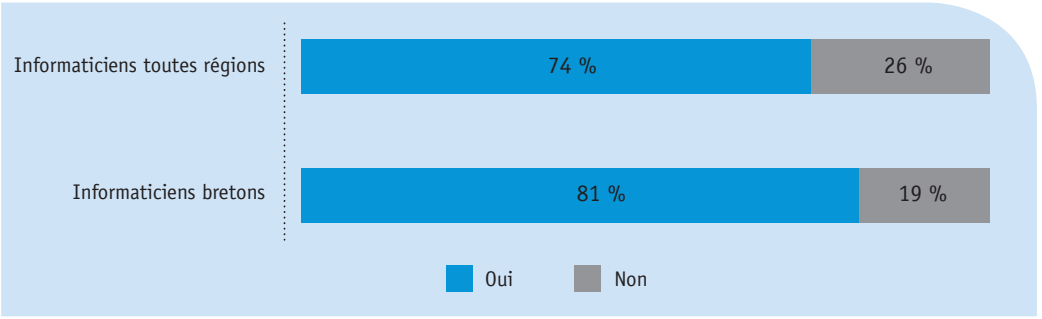
Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

–UNE FORTE ATTRACTIVITÉ DE LA FILIÈRE MAIS DES COMPÉTENCES À DÉVELOPPER–

Les entreprises de la cybersécurité pourraient potentiellement bénéficier de l'attrait porté à ce domaine par les informaticiens. En effet, 74 % des informaticiens seraient dans l'absolu intéressés pour travailler dans le domaine de la cybersécurité **(figure 19)**.

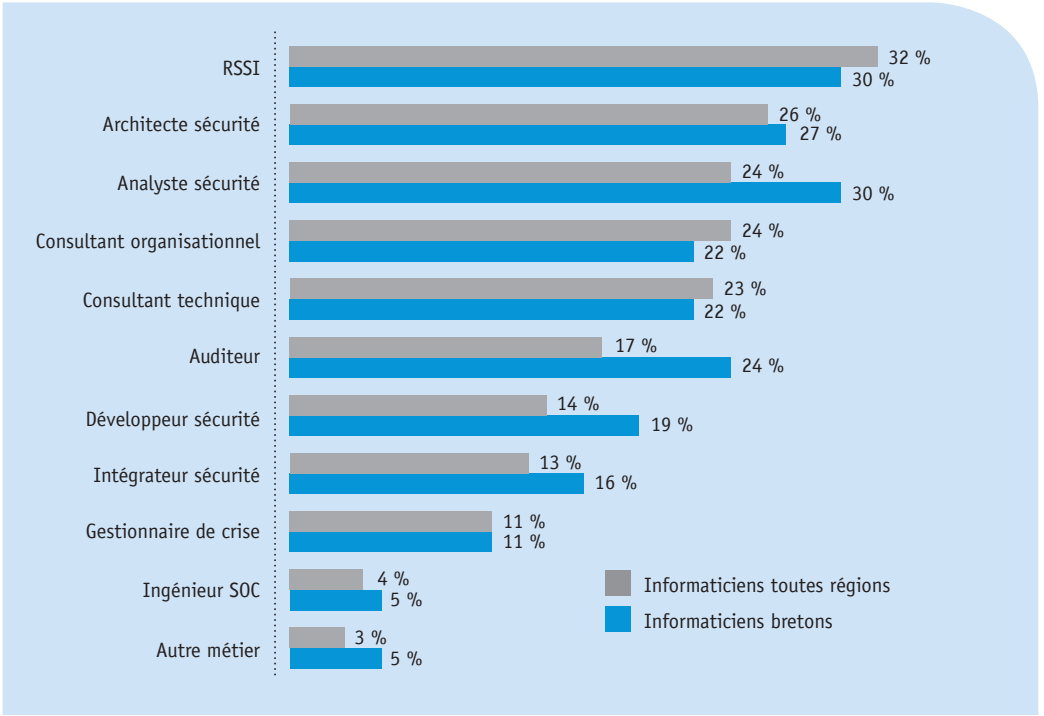
Cette proportion s'élève à 81 % pour les informaticiens bretons. Les informaticiens intéressés par la cybersécurité ciblent un panel vaste de métiers potentiels même si les métiers de RSSI, analyste sécurité et architecte sécurité sont les plus plébiscités **(figure 20)**.

– Figure 19–
Dans l'absolu, seriez-vous intéressé pour travailler dans le domaine de la cybersécurité ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

– Figure 20–
Parmi les métiers suivants spécialisés en cybersécurité, lequel ou lesquels aimeriez-vous éventuellement exercer dans le futur ? *(3 réponses possibles)*
Population des informaticiens se déclarant intéressés pour travailler dans le domaine de la cybersécurité



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Il convient de noter l'important écart d'opinion entre les femmes et les hommes sur cette question, alors que les résultats sont très proches sur les autres points. En effet, alors que 79 % des informaticiens hommes se déclarent intéressés dans l'absolu pour travailler dans le domaine de la cybersécurité, ce n'est le cas que de 54 % des femmes, soit 25 points de moins **(tableau 3)**. L'écart est quasi-identique en Bretagne (83 % des hommes, contre 60 % des femmes). La capacité de la cybersécurité à attirer les femmes est donc posée et cela doit être considéré comme un signal d'alerte pour l'avenir, d'autant plus que la place des femmes dans les métiers de l'informatique – actuellement fortement minoritaire[29] – se renforce progressivement. Dans un marché de l'emploi tendu, il est capital pour la filière d'être en capacité d'attirer aussi bien des hommes que des femmes.

29. Dans l'échantillon d'informaticiens interrogés, 80 % des répondants sont des hommes. Ils sont 86 % en Bretagne. À l'heure actuelle, les femmes ne représenteraient que 11 % de la communauté de la sécurité informatique selon *Women's Society of Cyberjutsu* (WSC), une association qui promeut l'émancipation des femmes afin qu'elles réussissent dans le secteur de la cybersécurité. https://www.sentryo.net/fr/cybersecurite-11-portraits-femmes-influentes.

– Tableau 3 –
Part des femmes et des hommes intéressés dans l'absolu pour travailler dans le domaine de la cybersécurité

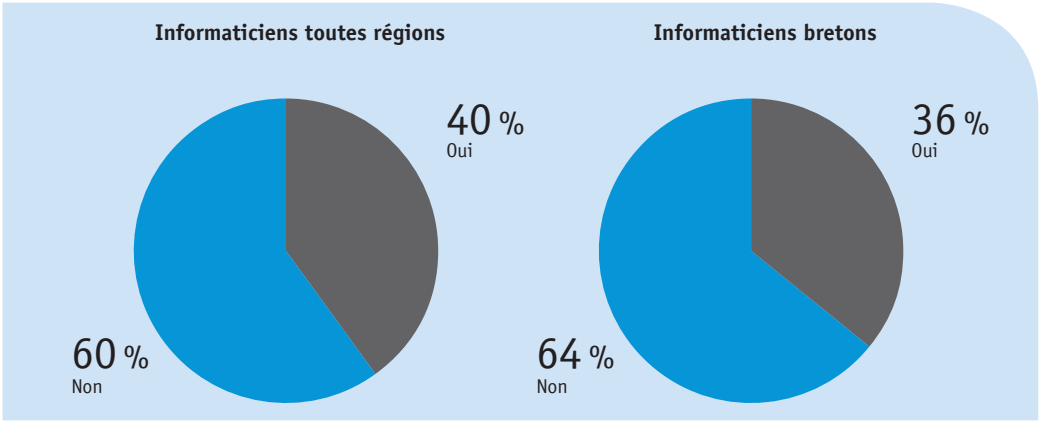
	Informaticiens toutes régions		Informaticiens bretons	
	Oui	Non	Oui	Non
Hommes	79%	21%	83%	17%
Femmes	54%	46%	60%	40%
Ensemble	**74%**	**26%**	**81%**	**19%**

Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

De plus, le processus de montée en compétences peut potentiellement être lourd puisque seulement 40 % des informaticiens interrogés (36 % en Bretagne) indiquent posséder des compétences techniques en cybersécurité **(figure 21)**. De véritables différences s'observent entre classes d'âge. Plus les cadres sont jeunes, plus ils sont nombreux en proportion à indiquer qu'ils possèdent de telles compétences. Ainsi, 45 % des moins de 30 ans jugent posséder des compétences techniques en cybersécurité, contre seulement 27 % des 50 ans et plus. Précisons qu'il s'agit ici d'autoévaluation. Aussi, les différences de résultats liées à l'âge peuvent être dues aux réelles différences de compétences des personnes, mais aussi en partie à la capacité des plus jeunes à davantage se valoriser, notamment dans le cadre d'une recherche potentielle d'emploi.

On peut observer également des différences notables selon le sexe. Alors que 46 % des hommes interrogés indiquent posséder des compétences techniques dans le domaine de la cybersécurité, ce n'est le cas que de 14 % des femmes interrogées. Les proportions sont respectivement de 41 % et 20 % en Bretagne.

– Figure 21 –
Possédez-vous des compétences techniques dans le domaine de la cybersécurité ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Mais même les informaticiens qui indiquent posséder des compétences techniques en cybersécurité font état de compétences limitées. Ainsi, lorsqu'on leur demande de s'autoévaluer de 0 à 10 sur différents sujets techniques (conception d'architectures sécurisées, détection d'intrusion, tests de sécurité, cryptographie…), peu considèrent qu'ils ont un très bon niveau de connaissance. Les informaticiens ne s'attribuent une note moyenne supérieure à 6 sur 10 que pour l'un des 11 domaines de compétences techniques en cybersécurité sur lesquels ils ont été interrogés (la sensibilisation des utilisateurs, qui peut d'ailleurs être considérée comme le domaine le moins technique). Pour 9 des 11 domaines, la note moyenne est égale ou inférieure à 5 **(tableau 4)**. Les informaticiens bretons affichent des notes moyennes inférieures aux informaticiens des autres régions dans 10 des 11 domaines, même si les différences restent peu importantes.

Il convient de noter que les informaticiens indiquant occuper actuellement un poste dans le domaine de la cybersécurité (environ 5 % des répondants) s'attribuent eux des notes supérieures à la moyenne sur la plupart des compétences techniques listées, mais de façon limitée. Leur autoévaluation est en moyenne supérieure à 6 sur 10 pour seulement trois points : sensibilisation aux utilisateurs (7,6), audit de sécurité (6,3) et conception-développement-modélisation de logiciels sécurisés (6,1).

La question de la montée en compétences sur le sujet de la cybersécurité pour l'ensemble des informaticiens actuellement sur le marché est donc très clairement posée. ●

– Tableau 4 –

Comment évaluez-vous vos connaissances en matière de cybersécurité, sur une échelle allant de 0 à 10 ?
(Question posée uniquement aux informaticiens indiquant posséder des compétences techniques en cybersécurité)

	Note moyenne informaticiens toutes régions	Note moyenne informaticiens bretons
Sensibilisation des utilisateurs	6,9	6,5
Conception, développement, modélisation d'architectures sécurisées	5,1	4,8
Évaluation de composants, logiciels, produits	5	4,8
Audit de sécurité	5	4,8
Gestion des crises en cas d'incident	4,9	5,2
Conception d'antivirus, analyses de malware	4,8	3,8
Cryptographie	4,5	3,7
Dimension juridique (protection des données, collectes de preuves en cas d'incident…)	4,4	3,7
Détection d'intrusion / pentest	4,4	4,3
Conception, développement, modélisation de logiciels sécurisés	4,3	4,1
Modélisation des menaces et attaques	4,3	3,8

Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

– D'IMPORTANTES ATTENTES EN MATIÈRE DE FORMATION CONTINUE –

Le tissu de formation à la cybersécurité est relativement bien fourni, notamment à l'échelle de la Bretagne[30]. Les enseignements spécifiques continuent de se développer que ce soit dans les universités ou les grandes écoles. Pour autant, leur mise en place reste relativement récente et elles accueillent encore un nombre limité d'étudiants, ce qui, dans les discours recueillis, participe à créer un décalage entre l'offre et la demande. Des ajustements sont toujours possibles au niveau des formations initiales pour répondre davantage aux attentes des entreprises : augmenter les promotions, ouvrir de nouveaux cursus, rendre la filière et les métiers plus attractifs pour les jeunes diplômés... Il faut sans doute aussi travailler à rendre attractives ces formations et former les formateurs. Cela peut également consister à distiller davantage de notions de cybersécurité dans les formations généralistes existantes **(encadré 13)**.

30. 5 des 26 formations qui ont reçu par l'Anssi le label SecNumedu sont situées en Bretagne : https://www.ssi.gouv.fr/particulier/formations/secnumedu/formations-labellisees-secnumedu/. En outre, le catalogue de l'offre de formation cyber édité par le Pôle d'excellence cyber donne accès à l'ensemble des formations à la cybersécurité proposées en région Bretagne et dans d'autres régions : http://www.bdi.fr/notre-action/cybersecurite.

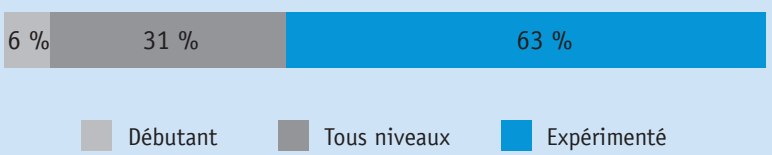
– Encadré 13 –
Verbatim

« Il ne suffit pas de faire des formations spécifiques pour des jeunes qui sortent de l'école. Il faut que dans les formations initiales en informatique soit systématiquement ajouté dans tous les programmes un pan sécurité. Aujourd'hui, les jeunes qui sortent d'écoles d'ingénieurs n'ont aucune notion de base en la matière (nécessité de choisir un mot de passe efficace, de sécuriser son stockage de données, de couper son Bluetooth dans les espaces publics). Les notions de base d'hygiène informatique ne sont pas acquises. »
(Grande entreprise).
« Il faut des modules à la cybersécurité partout. »
(Expert).
« Même parmi les étudiants en informatique, la cybersécurité n'est pas forcément celle qui attire le plus. Un travail de valorisation de la filière est à faire. Il faut que des gens qui travaillent dans la cybersécurité vendent ce métier. Il faut le rendre plus attrayant, plus accessible. Il y a un vrai travail de séduction à faire. On pourrait aussi favoriser le développement du mentorat. »
(Expert).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

Toutefois, on remarquera que les entreprises ne cherchent pas que des juniors. Bon nombre de métiers de la cybersécurité nécessitent de l'expérience. C'est le cas essentiellement des métiers rattachés à la définition de la politique et de l'administration de la cybersécurité dans les entreprises (notamment le métier de RSSI). Mais c'est aussi le cas des métiers de consultants, d'auditeurs et d'architectes. L'étude des offres d'emploi en cybersécurité publiées sur le site Apec montre d'ailleurs qu'une grande majorité des offres ne sont pas accessibles aux débutants et jeunes diplômés **(figure 22)**.

– Figure 22 –
Répartition des offres Apec en cybersécurité publiées en 2016 selon le niveau d'expérience demandé



Source : Apec, 2017.

Aussi, un réel effort est attendu au niveau de la formation continue, non seulement pour permettre d'ajuster les compétences des spécialistes sur des techniques et pratiques en constante évolution, mais aussi pour assurer une montée en compétences sur le sujet pour tous les métiers. Le recours à la formation continue permettrait enfin d'améliorer l'employabilité de cadres sans emploi, et de les repositionner au sein d'entreprises qui cherchent à recruter. L'importance à accorder à la formation est clairement identifiée chez certains acteurs de la cybersécurité **(encadré 14)**.

– Encadré 14–
Verbatim

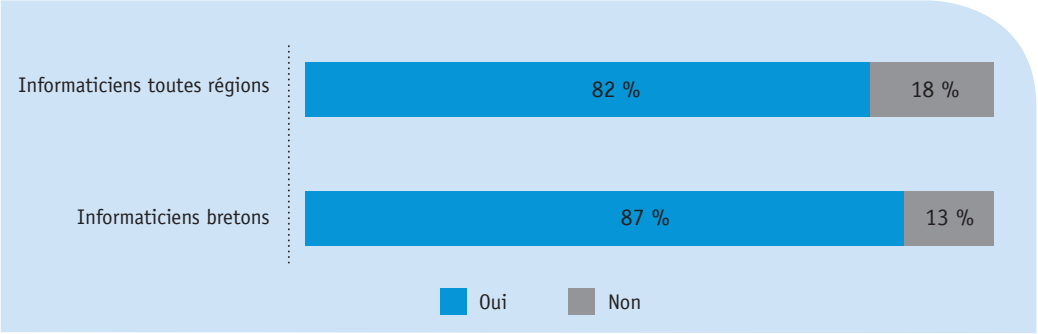
« Aussi, faut-il, car cela permettrait d'avancer vite sur cet enjeu, favoriser la montée en compétences d'informaticiens sur ce domaine. Par exemple, il pourrait s'agir de développer des formations d'un an en matière de cybersécurité, ce qui permettrait aussi de faciliter le retour à l'emploi d'informaticiens. Typiquement, le métier d'ingénieur système n'avait pas le vent en poupe à une époque, même si ça revient. Un ingénieur système se recycle facilement dans les problématiques de firewall, antivirus, déploiement de solutions sécurité. On aurait là un moyen de remettre au travail des gens qui sont soit au chômage soit en difficulté car ils ont des connaissances technologiques qui ne sont plus très à jour. »
(Grande entreprise).
« Aujourd'hui, il n'y a pas assez de diplômés par année par rapport aux besoins, ce qui fait que de plus en plus on s'oriente vers des formations en interne de collaborateurs qu'on va recentrer sur des enjeux et savoir sécurité, et ce pour pallier le manque de ressources sur le marché. »
(Grande entreprise).

Source : Apec, 2017. Entretiens auprès d'entreprises recrutant dans le domaine de la cybersécurité.

Cela rejoint pleinement les besoins exprimés par les cadres informaticiens. En effet, 82 % des informaticiens souhaitent d'une manière générale développer leurs compétences en cybersécurité **(figure 23)**. Ils sont 87 % en Bretagne. La volonté de monter en compétences sur le sujet est donc très nettement présente parmi les informaticiens sur le marché. Les résultats sont de plus semblables quel que soit l'âge des informaticiens interrogés ou leur situation professionnelle. Il convient également de noter que la quasi-totalité des informaticiens (91 %) ayant indiqué posséder des compétences techniques en cybersécurité souhaitent développer leurs compétences en la matière, tout comme 76 % des informaticiens qui ne possèdent pas de compétences techniques sur le sujet. La question de la montée en compétences concerne donc bien un large public possédant déjà ou non des notions techniques en cybersécurité.

En revanche, les femmes, moins attirées par la cybersécurité, sont également moins nombreuses que les hommes, en proportion, à souhaiter développer leurs compétences en cybersécurité : 67 % contre 85 %. Les proportions en Bretagne sont respectivement de 67 % et 90 %.

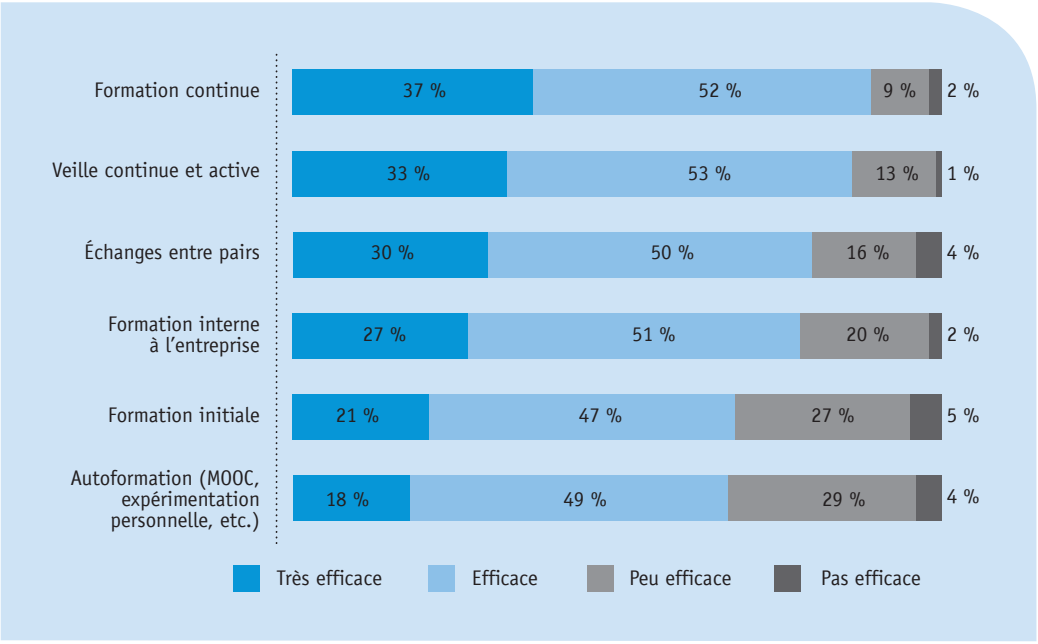
– Figure 23 –
Souhaiteriez-vous développer vos compétences en cybersécurité ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Pour développer des compétences en cybersécurité, la formation continue est jugée parmi d'autres moyens comme le plus efficace. 9 informaticiens sur 10 jugent qu'il s'agit d'un moyen efficace pour développer des compétences en cybersécurité **(figure 24)**. La veille et les échanges entre pairs sont également jugés très efficaces. Les informaticiens possédant déjà des compétences techniques en cybersécurité sont nettement plus nombreux, en proportion, à juger très efficaces la veille, les échanges entre pairs et l'autoformation. Les résultats sont en revanche proches quel que soit le lieu de résidence.

– Figure 24 –
Pour développer des compétences en cybersécurité, les moyens suivants sont-ils d'après vous efficaces ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

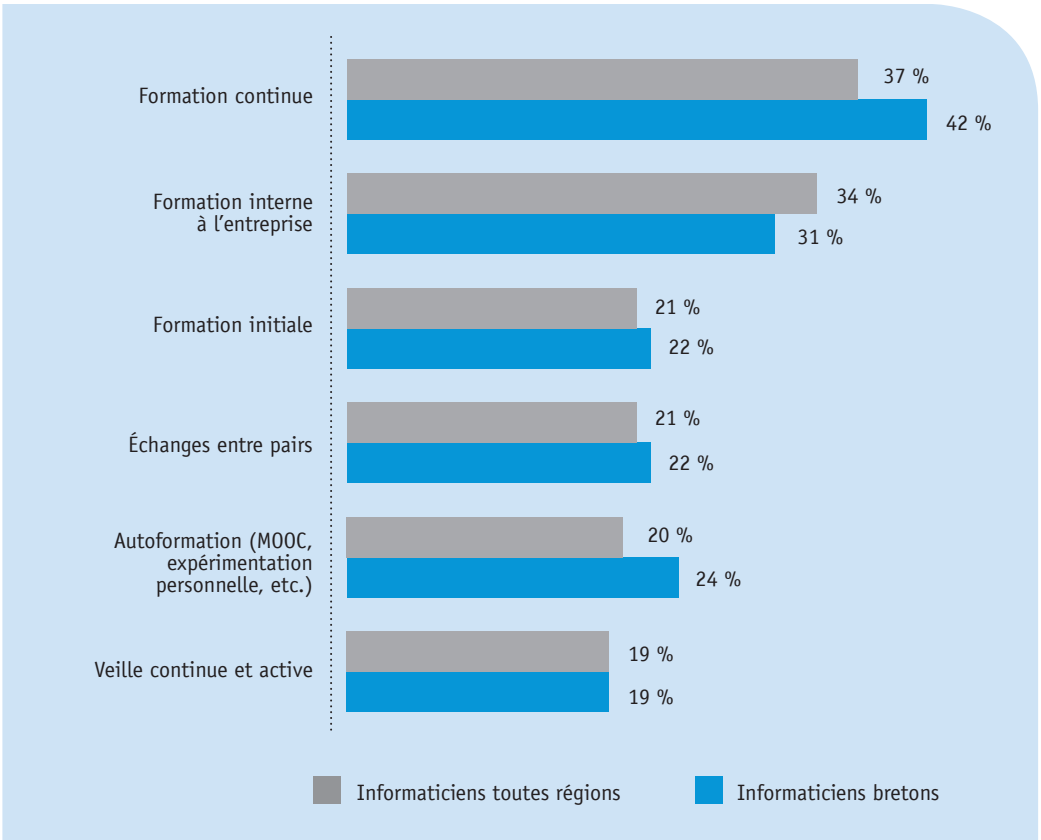
Interrogés sur leurs besoins personnels, les informaticiens mettent aussi en avant la formation continue. 37 % indiquent avoir besoin d'une formation continue, un chiffre qui atteint 42 % en Bretagne. Au global, 9 sur 10 auraient besoin d'une formation, que ce soit sous la forme d'une formation continue (y compris en reprise d'études) ou d'une formation interne à leur entreprise **(figure 25)**.

La formation continue joue donc un rôle central, tant en termes d'efficacité perçue que de besoin personnel.

En revanche, la veille ou les échanges entre pairs sont jugés comme des besoins moins prioritaires par les informaticiens interrogés, alors qu'ils les jugent très efficaces pour développer leurs compétences. Les informaticiens possédant déjà des compétences techniques en cybersécurité sont eux nettement plus enclins à juger en avoir besoin pour développer leurs compétences. Il semblerait donc que l'autoformation quelle qu'elle soit (Mooc, échanges entre pairs, veille...) constitue bien un besoin fort pour développer ses compétences en cybersécurité, mais que cela n'est pas perçu comme tel par les informaticiens qui ne possèdent pas de compétences en la matière. Les formations en cybersécurité devraient ainsi non seulement permettre d'acquérir des compétences techniques en cybersécurité, mais aussi permettre d'apprendre à apprendre afin d'assurer un continuum dans le développement des compétences après la formation. ●

– Figure 25 –

De quoi auriez-vous besoin avant tout pour développer vos compétences en cybersécurité (2 réponses maximum) ?



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

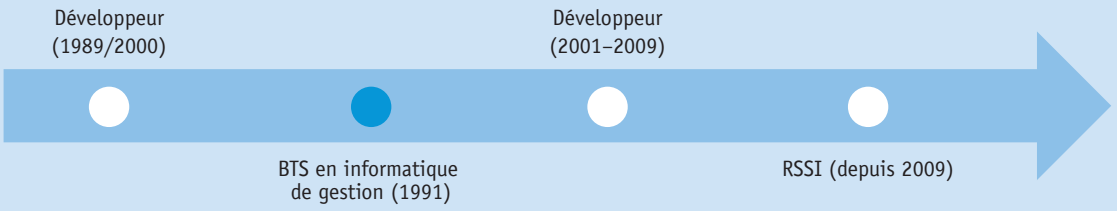
–DES PASSERELLES ENTRE MÉTIERS À CONSTRUIRE–

Il semble d'autant plus nécessaire de renforcer la formation continue que cela correspond à la réalité des situations professionnelles des informaticiens dont les parcours ne sont pas toujours linéaires. L'analyse de leurs CV met en avant des changements de postes, de métiers, des formations professionnelles... même après leur insertion sur le marché du travail **(figure 26)**.

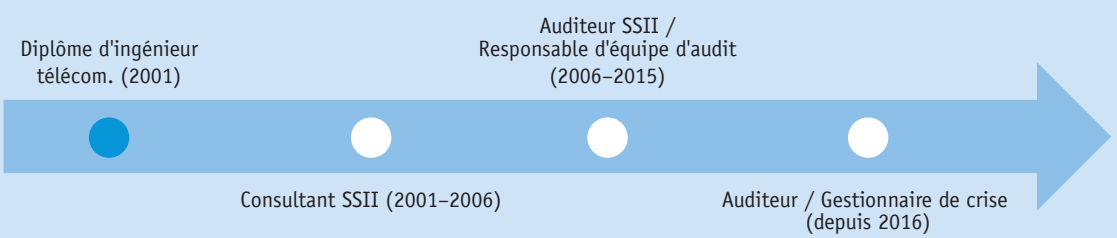
Ces différentes voies d'accès vers les métiers de la cybersécurité ne sont pas toujours bien identifiées par les cadres comme par les entreprises. Il conviendrait de rendre plus lisibles les trajectoires possibles, les parcours de formation et les compétences à mobiliser pour exercer un métier dans la cybersécurité, notamment au sein des référentiels métiers existants ou à créer.

– Figure 26–
Exemples de trajectoires de cadres de l'informatique vers les métiers de la cybersécurité

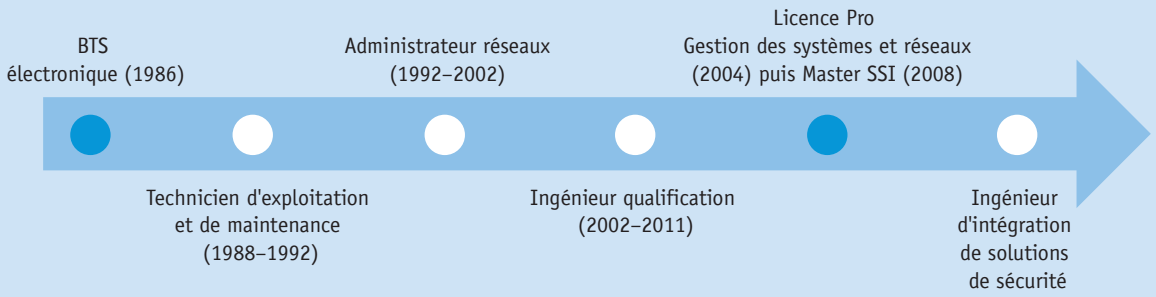
1er cas - Paul occupe un poste de RSSI au sein d'une entreprise du secteur de la défense. Ses missions sont essentiellement tournées vers les problématiques de cybersécurité. Son parcours montre une évolution forte de ses compétences en la matière puisqu'il a commencé comme développeur systèmes et réseaux, intervenant au sein de différentes structures de province et d'Île-de-France. L'évolution vers le domaine de la défense a également été progressive, Paul ayant travaillé auparavant pour d'autres secteurs comme celui des assurances.



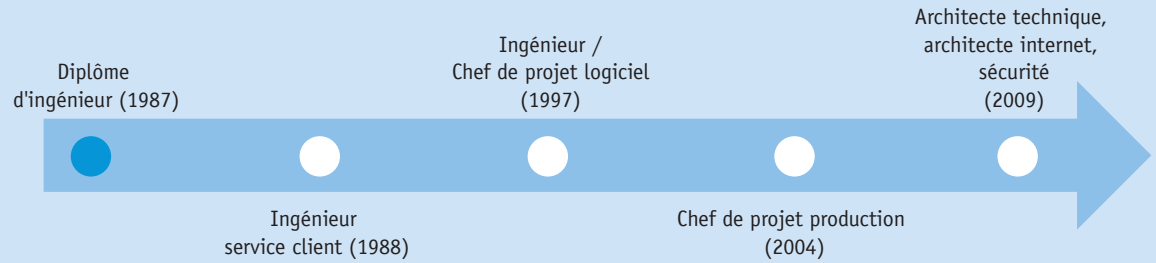
2e cas - Sébastien exerce un poste de gestionnaire de crise depuis 2016 chez un hébergeur de sites web. Ses missions actuelles sont centrées sur le pilotage des analyses de risques (élaboration, suivi, définition de plans d'actions). Elles font appel aux capacités managériales qu'il a acquises au cours de son précédent poste de responsable d'équipe d'audit sécurité. L'audit est d'ailleurs le domaine dans lequel il s'est spécialisé après avoir été diplômé d'une école d'informatique en 2001.



3e cas - Christophe est diplômé de l'université de Rennes où il a obtenu un BTS en électronique au milieu des années 1980. Pendant près de 15 ans, il a occupé un poste de technicien informatique (maintenance, exploitation, administration des systèmes et des réseaux...). Depuis, ses missions ont fortement évolué. En tant qu'ingénieur intégration de systèmes de sécurité, il gère dorénavant des projets liés à l'étude et l'intégration de solutions de sécurité. Cette transition a été facilitée par la reprise d'études. Entre 2004 et 2014, Christophe a suivi plusieurs formations dont un mastère spécialisé sécurité des systèmes d'information. Elle a aussi été rendue possible par la très forte expérience que Christophe a acquise dans le secteur des télécommunications, un domaine d'activité dans lequel il a exercé depuis plus de 10 ans, et qui est très en pointe en matière de cybersécurité.



4e cas - François est diplômé d'une école d'ingénieurs, spécialité informatique. À la fin de ses études, il intègre le service client d'un constructeur informatique, et ce pour une durée de près de 10 ans. En 1997, il s'oriente vers des éditeurs de logiciels et de solutions sécurisées. Il y exercera les postes d'ingénieur puis chef de projet logiciel. Au milieu des années 2000, François intègre une ESN et s'attachera à concevoir des plates-formes sécurisées pour de grands comptes du secteur de la finance et des télécommunications. Depuis 2012, il assure des missions d'expert technique dans ce domaine en tant que freelance, après avoir effectué une transition de quelques années chez un éditeur de logiciels en tant qu'architecte et pilote d'activités d'ingénierie informatique.



Source : Apec, 2017. Exploitation des CV déposés sur Apec.fr

L'appétence des informaticiens pour la formation continue, en particulier en Bretagne, pose également la question du type de formations à construire pour répondre aux besoins exprimés. Et cela pose des difficultés non négligeables tant les profils des informaticiens bretons prêts à travailler dans la cybersécurité et souhaitant monter en compétences sur le sujet sont divers. Leur âge, leur formation initiale, leur situation professionnelle, leur parcours, leurs compétences sont extrêmement variés, comme le montrent les quelques exemples suivants **(figure 27)**. Développer les compétences en cybersécurité en région Bretagne demandera donc de varier les approches et de multiplier les initiatives, tout en gardant une cohérence d'ensemble. En effet, certaines attentes exprimées apparaissent réalisables moyennant un accompagnement léger quand d'autres nécessitent une importante remise à niveau technique. Il sera par exemple difficile à un développeur en informatique de gestion sans notion technique en cybersécurité de devenir auditeur en cybersécurité. En revanche, un chef de projet AMOA expérimenté dans la banque avec déjà de solides compétences en cybersécurité pourrait devenir RSSI moyennant une formation continue courte. ●

– Figure 27 –
Exemples de profils d'informaticiens bretons intéressés pour travailler dans le domaine de la cybersécurité et souhaitant développer leurs compétences en la matière

Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

–4–

–PLAN D'ACTIONS DE L'APEC POUR FAVORISER LE DÉVELOPPEMENT DES COMPÉTENCES EN CYBERSÉCURITÉ EN BRETAGNE–

Cette étude débouche sur des perspectives d'actions concrètes. Afin de développer les compétences en cybersécurité en Bretagne, l'Apec et les partenaires de l'étude vont s'engager à la suite de cette étude dans un plan d'actions qui vise à développer la connaissance des métiers de la cybersécurité, à conseiller les entreprises bretonnes de la cybersécurité, et à accompagner les cadres et les jeunes diplômés bretons intéressés par la cybersécurité. Certaines actions ont vocation à être pérennisées au-delà de 2017.

–DÉVELOPPER LA CONNAISSANCE DES MÉTIERS DE LA CYBERSÉCURITÉ–

Cette étude constitue en soi un outil pour faire connaître les métiers de la cybersécurité et l'aspect porteur de cette filière. Elle pourra aussi être partagée avec l'ensemble des partenaires régionaux de l'emploi et de la formation afin de construire progressivement une vision commune des enjeux de cette filière. Cette étude sera par ailleurs complétée par la réalisation de fiches métiers dédiées à la cybersécurité qui pourront être diffusées sur l'annuaire des métiers présenté sur Apec.fr. Ces fiches métiers porteront sur les métiers les plus porteurs de la cybersécurité et insisteront sur les parcours permettant d'y accéder tant en termes de formation que d'expérience professionnelle.

Aussi, dans un environnement en constante et rapide évolution, l'actualisation de la présente étude prendrait tout son sens dans l'intérêt général. •

–CONSEILLER LES ENTREPRISES BRETONNES DE LA CYBERSÉCURITÉ–

Cette étude permettra une montée en compétences des consultants et conseillers Apec dédiés aux entreprises : ils seront outillés sur le sujet de la cybersécurité, en capacité de conseiller avec réactivité et pertinence les entreprises en recherche de compétences.

Aussi, toutes les entreprises bretonnes ayant participé à l'étude pourront bénéficier d'un rendez-vous avec un consultant de l'Apec afin d'échanger sur les résultats et de travailler directement sur leurs besoins (recrutement, fidélisation, gestion des compétences...).

Au-delà des entreprises participantes à l'enquête, des entreprises bretonnes en lien avec la cybersécurité seront conviées à une matinale d'information sur la question des compétences en cybersécurité. La matinale pourrait être organisée en partenariat, par exemple avec le Pôle d'excellence cyber.

Les actions pourront s'inscrire sur la durée, en travaillant avec les différentes structures qui accompagnent les entreprises présentes en Bretagne dans le domaine de la cybersécurité. •

–ACCOMPAGNER LES CADRES ET LES JEUNES DIPLÔMÉS INTÉRESSÉS PAR LA CYBERSÉCURITÉ–

Les consultants et conseillers Apec dédiés aux cadres et aux jeunes diplômés seront également outillés sur le sujet de la cybersécurité. Ils seront notamment en capacité de conseiller les cadres et les jeunes diplômés en recherche d'opportunité ou de mobilité dans le secteur de la cybersécurité. Ils pourront notamment relayer l'information sur l'offre de formation existante en Bretagne et dans d'autres régions via le catalogue réalisé par le Pôle d'excellence cyber.

L'Apec réalisera par ailleurs à l'automne 2017 un évènement spécialement sur le sujet « Cybersécurité en Bretagne ». Cet évènement prendra la forme d'un « afterwork » permettant des échanges d'expérience, des témoignages d'itinéraires professionnels, des analyses d'experts. Les informaticiens bretons ayant manifesté leur intérêt via l'enquête pour recevoir des informations sur la cybersécurité en Bretagne pourront être conviés à cet évènement.

Le salon Apec de recrutement organisé à Nantes le 29 juin 2017 sera en outre l'occasion de tenir une conférence sur la cybersécurité associant l'Apec et un partenaire de l'étude. Certains acteurs de la cybersécurité de Bretagne pourront également venir y présenter leurs offres d'emploi. Enfin, compte tenu de l'attractivité de la Bretagne pour les informaticiens qui sont prêts à changer de région, les acteurs de la cybersécurité en Bretagne pourraient également participer aux deux salons annuels organisés par l'Apec en région parisienne. Cela permettrait de promouvoir l'écosystème breton de la cybersécurité et de favoriser les recrutements des entreprises bretonnes en la matière[31]. ●

31. Notons que la Région Bretagne, avec sa campagne « Passons à l'Ouest », présente notamment dans le métro parisien, fait actuellement la promotion de l'ouverture de la nouvelle ligne TGV plaçant Rennes à 1 h 30 de Paris à partir de juillet 2017.

–5–

–ANNEXE : MÉTHODOLOGIE–

L'Apec, via son département études et recherche et sa délégation territoriale Bretagne, a répondu en mars 2016 à un appel à projets pour des études-actions sur l'emploi-formation lancé par la Région Bretagne et l'État dans le cadre du contrat de plan État-Région 2015-2020. Cet appel à projets vise à développer la connaissance des secteurs, des filières et des territoires dans le but de préparer le futur Contrat de plan régional de développement des formations et de l'orientation professionnelles (CPRDFOP), outil de référence essentiel à la politique de formation en région ces prochaines années. La proposition de l'Apec sur la filière de la cybersécurité a été retenue et les travaux ont démarré à l'été 2016.

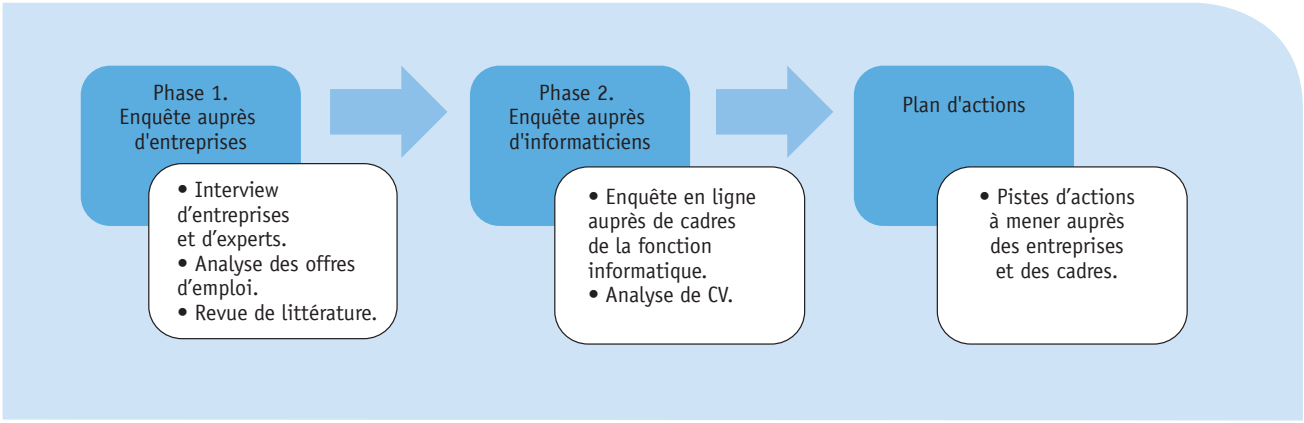
–OBJECTIFS DE L'ÉTUDE–

L'objectif de l'étude était de :

- Comprendre le fonctionnement de la filière de la cybersécurité, en particulier en région Bretagne.
- Cerner les compétences cadres indispensables au développement de la filière cybersécurité en Bretagne.
- Faire un état des lieux des compétences présentes et de la concordance avec les compétences stratégiques recherchées par les entreprises.
- Mettre en avant l'intérêt des informaticiens bretons pour la filière et leur appétence pour une montée en compétences dans ce domaine.
- Proposer des pistes d'actions en matière de compétences permettant le développement de la filière cybersécurité en région Bretagne.

Ainsi, l'étude a reposé sur une méthodologie multifocale : revue de littérature, étude de données propres à l'Apec (offres d'emploi et CV publiés sur le site Apec.fr), entretiens individuels, focus-groupes, questionnaire. L'étude s'est déroulée en deux phases et a débouché sur un plan d'actions concret **(figure 28)**.

– Figure 28–
Déroulement de l'étude



Un comité de pilotage a été constitué pour le suivi de cette étude **(tableau 5)**. Ce comité réunissait des représentants de la Région Bretagne, de la Direccte Bretagne (Direction régionale des entreprises, de la concurrence, de la consommation, du travail et de l'emploi), du Pôle d'excellence cyber, de BDI (Bretagne Développement Innovation) et de l'Apec. Le comité de pilotage s'est réuni le 11 juillet 2016, le 16 décembre 2016 et le 9 mars 2017. ●

– Tableau 5 –
Composition du comité de pilotage de l'étude

Annie Audic	Conseil régional Bretagne Directrice de projets « continuum formation, recherche, innovation »
Anne-Véronique Cap	Conseil régional Bretagne Chef du service Analyse et prospective Emploi-Formation
Isabelle Cupit	Conseil régional Bretagne Chargée de mission service Analyse et prospective Emploi-Formation
Damien Rolland	Direccte Bretagne Chargé de mission développement économique
Yann Dieulangard	Bretagne Développement Innovation Chef de projet Pôle Ingénierie, Europe & Cartographie
Paul-André Pincemin	Pôle d'excellence cyber Délégué général
Frédéric Cuppens	Pôle d'excellence cyber Animateur du Club Formation
Patrick Erard	Pôle d'excellence cyber Club Formation
Anne Savatier	Apec Déléguée territoriale Bretagne
Pierre Lamblin	Apec Directeur du département études et recherche
Maïmouna Fossorier	Apec Responsable du pôle insertion, parcours, métiers
Gaël Bouron	Apec Responsable d'études, activité prospective territoriale
Caroline Legrand	Apec Chargée d'études
Sophie Roux	Apec Chargée d'études

–ENQUÊTE AUPRÈS DES ENTREPRISES–

Elle visait à mettre en avant les enjeux de la cybersécurité pour les principaux acteurs de la filière en région Bretagne, et en particulier les PME positionnées sur ce secteur. Elle avait également pour but d'identifier leurs besoins en recrutements et leurs éventuelles difficultés. Pour ce faire, deux demi-journées de travail avec 17 représentants d'entreprises ont été organisées à Rennes au cours du dernier trimestre 2016. En complément, 25 entretiens individuels ont été réalisés, par téléphone ou en face-à-face.

Au total, 42 professionnels ont été interviewés, représentant en tout 31 entreprises. 42 % des structures interrogées sont des PME en cybersécurité. 84 % des acteurs interrogés travaillent en Bretagne, essentiellement dans le département d'Ille-et-Vilaine **(tableau 6)**. Quelques acteurs franciliens à dimension nationale ont également été interrogés.

42 % des personnes interrogées travaillent dans des PME spécialisées en cybersécurité et 23 % dans des grandes structures publiques ou privées de la cybersécurité **(figure 29)**. Plus de 4 personnes interrogées sur 10 travaillent au sein d'une direction informatique et près de 3 sur 10 au sein d'une direction générale.

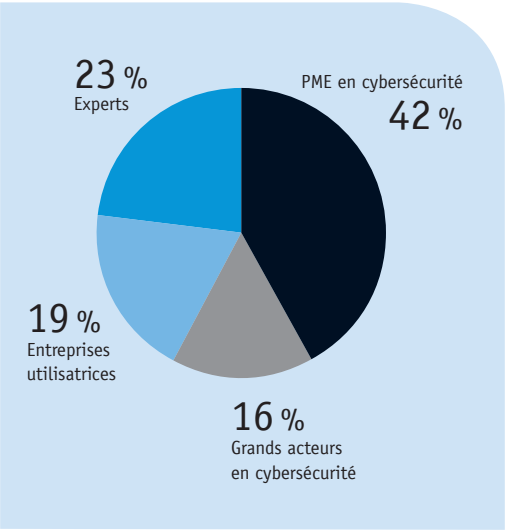
En complément de l'enquête auprès des entreprises, la base des offres diffusées par l'Apec en 2014 et en 2016 a été exploitée. L'intitulé du poste ouvert à candidature est le principal critère qui a été retenu pour la sélection des offres à analyser, les termes spécifiques aux métiers de la cybersécurité y apparaissant de manière claire (cybersécurité, cyberdéfense, RSSI, sécurité informatique...). ●

– Tableau 6 –
Caractéristiques des entreprises interrogées

Fonction des acteurs interrogés	Effectif
Direction informatique	18
Direction générale	12
RH	8
Communication, commercial, R&D, services techniques	4
Total	**42**
Nature des entreprises interrogées	
PME en cybersécurité	13
Expert	5
Grands acteurs de la cybersécurité	7
Entreprises utilisatrices	6
Total	**31**
Lieu d'implantation des entreprises interrogées	
Ille-et-Vilaine	18
Morbihan	4
Paris	4
Côtes-d'Armor	3
Finistère	1
Autres départements	1
Total	**31**

Source : Apec, 2017.

– Figure 29 –
Types d'acteurs interrogés



Source : Apec, 2017

–ENQUÊTE AUPRÈS DES INFORMATICIENS–

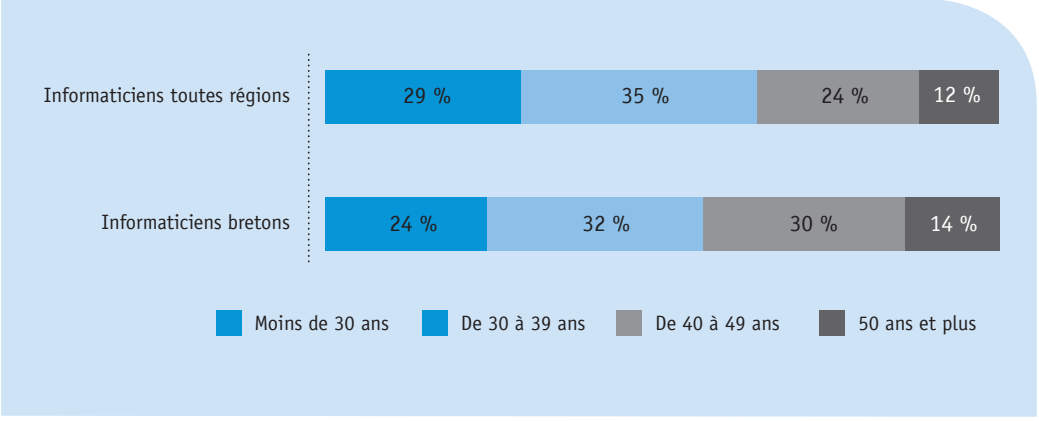
Une enquête en ligne a été administrée par l'Apec auprès d'un échantillon de cadres informaticiens, qu'ils soient en poste ou en recherche d'emploi dans ce domaine. Il s'agit de personnes inscrites sur Apec.fr dans la fonction informatique et ayant activé leur profil au cours des 12 derniers mois. Ces informaticiens sont donc à tout le moins en veille sur le marché de l'emploi, ce qui rend d'autant plus pertinente leur interrogation sur des questions liées à l'évolution professionnelle ou à la montée en compétences sur certains sujets. L'enquête s'est déroulée du 5 au 24 janvier 2017.

Au total, 1 186 réponses ont été recueillies. 44 % des répondants sont des informaticiens résidant en Bretagne (soit 527 répondants). Les résultats ont ensuite été redressés selon les critères de l'âge et de la région. Les résultats présentés au niveau national sont donc représentatifs selon ces deux critères des informaticiens identifiés sur Apec.fr au cours des 12 derniers mois. Les résultats présentés pour la Bretagne sont représentatifs des informaticiens identifiés sur Apec.fr et résidant en Bretagne.

L'enquête avait pour objectif de recueillir la vision des informaticiens en recherche plus ou moins active de mobilité professionnelle sur le marché de l'emploi informatique en général, et sur le domaine de la cybersécurité en particulier. L'appétence de ces informaticiens pour les métiers de la cybersécurité, leur connaissance du marché national et breton de la cybersécurité et les expériences qu'ils avaient acquises ou qu'ils souhaitaient développer dans ce domaine ont été particulièrement investiguées. Les résultats des informaticiens bretons ont systématiquement été comparés aux résultats nationaux. Cela a permis de mettre en évidence certaines singularités du marché de l'emploi en cybersécurité en Bretagne.

Les cadres interrogés sont 80 % à être des hommes (86 % pour les enquêtés bretons). Les enquêtés résidant en Bretagne sont plus âgés que l'ensemble des répondants : 24 % ont moins de 30 ans et 44 % ont 40 ans et plus, contre respectivement 29 % et 36 % pour l'ensemble des enquêtés **(figure 30)**. Le niveau de formation des répondants est élevé puisqu'ils sont 6 sur 10 à être titulaires d'un diplôme de type Bac +5 et plus.

– Figure 30–
Âge des enquêtés



Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

Près de 8 répondants sur 10 sont en emploi (76 % pour les enquêtés bretons).
31 % des répondants travaillent dans des fonctions relatives au développement-ingénierie logiciel-conception web. Les Bretons sont plus nombreux que l'ensemble des enquêtés à exercer leur emploi dans les domaines des télécommunications-systèmes-réseaux-données (+ 5 points).

46 % des enquêtés sont employés par une ESN (SSII). Les Bretons travaillent pour près des trois quarts dans des entreprises appartenant au secteur d'activité des services, ce qui est supérieur de 9 points à l'ensemble des enquêtés **(tableau 7)**.
En complément de cette enquête, la CVthèque de l'Apec a également été exploitée, afin d'analyser des parcours d'informaticiens occupant un poste dans le domaine de la cybersécurité. ●

– Tableau 7 –
Part des femmes et des hommes intéressés dans l'absolu pour travailler dans le domaine de la cybersécurité

	Informaticiens toutes régions	Informaticiens bretons
Fonction		
Direction informatique	10%	12%
Maintenance, exploitation	14%	12%
Développement, ingénierie logiciel, conception web	31%	31%
Maîtrise d'ouvrage et fonctionnel	17%	15%
Télécommunications, systèmes, réseaux, données	13%	18%
Autres	15%	12%
Travaille dans une ESN (ex SSII)		
Oui	47%	46%
Non	53%	54%
Secteur d'activité de l'entreprise*		
Industrie	20%	17%
Construction	2%	0%
Commerce, distribution	14%	10%
Services	64%	73%

Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.
*Les informaticiens travaillant dans une ESN ont été classés dans le secteur des services quel que soit le secteur d'activité de l'entreprise cliente pour laquelle ils travaillaient au moment de l'enquête.

N°2017-25

JUIN 2017

–CYBERSÉCURITÉ EN BRETAGNE : L'ENJEU DES COMPÉTENCES–

Dans un environnement sociétal, technologique et réglementaire en pleine évolution, la cybersécurité constitue un enjeu de plus en plus important, notamment pour l'emploi cadre. Cette étude montre combien les besoins en compétences pour affronter ce défi sont majeurs. Dotée d'un véritable écosystème en cybersécurité, la Bretagne joue un rôle notable dans ce domaine. Les besoins concernent des métiers très techniques, mais le savoir-être est aussi crucial. Faciliter le recrutement des entreprises passe notamment par la formation continue. En effet, 87 % des informaticiens bretons souhaiteraient monter en compétences en cybersécurité. Cette étude débouche ainsi sur un plan d'actions concret qui sera mis en œuvre par la délégation Apec Bretagne, en collaboration avec les partenaires de l'étude*.

**Cette étude a été réalisée par l'Apec et cofinancée par la Région Bretagne et l'État dans le cadre d'un appel à projets pour des études-actions sur l'emploi-formation prévu dans le contrat de plan État-Région. Le Pôle d'excellence cyber et Bretagne Développement Innovation ont été associés à cette démarche.*

ISBN 978-2-7336-1014-5
JUIN 2017

L'étude a été réalisée par le département études et recherche de l'Apec en lien avec la délégation territoriale Apec Bretagne
Pilotage de l'étude : Gaël Bouron.
Analyse et rédaction : Caroline Legrand, Sophie Roux.
Direction de l'étude : Maïmouna Fossorier.
Maquette : Daniel Le Henry.
Direction du département : Pierre Lamblin.
Déléguée territoriale Apec Bretagne : Anne Savatier.

ASSOCIATION POUR L'EMPLOI DES CADRES
51 BOULEVARD BRUNE – 75689 PARIS CEDEX 14

POUR CONTACTER L'APEC
0 809 361 212 Service gratuit + prix appel
DU LUNDI AU VENDREDI
DE 9H À 19H

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BRETAGNE

Région BRETAGNE

BRETAGNE DÉVELOPPEMENT INNOVATION

PÔLE D'EXCELLENCE CYBER

Apec

EDOBSA0236–05.17