– CYBERSÉCURITÉ EN BRETAGNE : L'ENJEU DES COMPÉTENCES –

LES ÉTUDES DE L'EMPLOI CADRE

N°2017-25

JUIN 2017

SYNTHÈSE

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE

PRÉFET
DE LA RÉGION
BRETAGNE

Région
BRETAGNE

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. 86 % des informaticiens interrogés par l'Apec jugent que les entreprises sont mal préparées sur le sujet. Les besoins en compétences pour affronter ce défi sont donc 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.

BRETAGNE DÉVELOPPEMENT INNOVATION

PÔLE D'EXCELLENCE CYBER

Apec

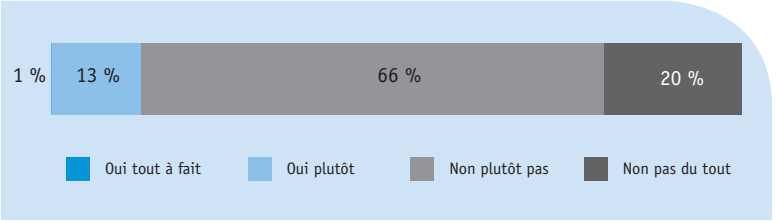
LA CYBERSÉCURITÉ : ENJEU ET DÉFI

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. Les conséquences financières des cyberattaques sont rudes pour les entreprises : 1,5 milliard d'euros de pertes financières sur la seule année 2016 (enquête annuelle de PwC[1]). La probabilité pour les entreprises d'être attaquées, quelle que soit leur taille, devient de plus en plus forte. 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. De surcroît, les évolutions technologiques (dans les domaines transverses du cloud computing, des objets connectés, du big data...) 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. Elle 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].

Mais si une certaine prise de conscience est apparue ces dernières années sur l'enjeu de la cybersécurité, les entreprises ne sont pas matures sur le sujet. Elles le reconnaissent elles-mêmes : seuls 53 % des dirigeants d'entreprises industrielles jugent que leur entreprise est bien préparée sur les questions de cybersécurité[3]. 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 1)**. Ils sont également presque unanimes (83 %) à penser que les salariés ne sont pas bien sensibilisés aux bonnes pratiques en matière d'hygiène informatique. Le travail à accomplir pour implanter une culture de la cybersécurité dans les entreprises apparaît encore très important.

1. PwC, The Global State of Information Security® Survey 2017.
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.
3. Étude L'Usine Nouvelle – Orange Business Services réalisée en novembre 2016 auprès de 347 dirigeants de l'industrie.

– Figure 1–
On parle beaucoup de cybersécurité aujourd'hui. Pensez-vous que les entreprises en général y sont bien préparées ?



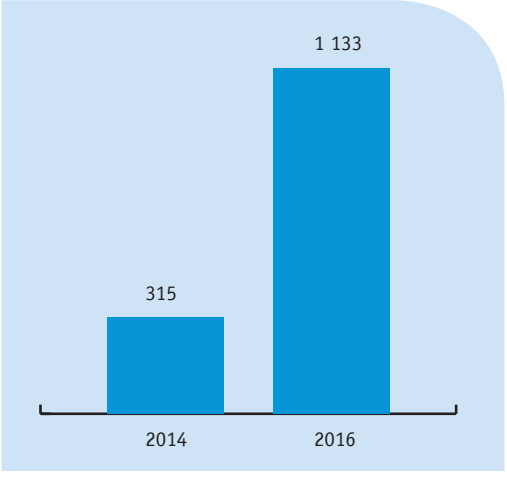
Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

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[4]. 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 2)**.

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

– Figure 2–
Offres d'emploi diffusées par l'Apec en 2014 et 2016 pour des postes en cybersécurité



Source : Apec, 2017

Un marché de l'emploi en cybersécurité commence ainsi à se structurer autour de différents types d'acteurs.

1. Les entreprises utilisatrices de services de cybersécurité. Des entreprises de toutes tailles et de tous secteurs vont chercher à monter en compétences sur le sujet, par des embauches directes ou du recours à l'expertise externe. Les opérateurs d'importance vitale (OIV) sont très actifs. Il s'agit d'entreprises ou de services étatiques dépendant de secteurs (finance, énergie, transports, santé...) particulièrement stratégiques.

2. Les entreprises prestataires de services. Des grandes entreprises du conseil ou des services informatiques (ESN) ont développé des branches d'activités spécifiques en cybersécurité. Elles offrent notamment leur expertise en audits de sécurité, consulting, analyse de risques... Des start-up sont également très actives, tant pour des activités de service très spécialisées que pour le développement de produits (logiciels, plates-formes d'échanges sécurisées, packages de sécurité...).

3. Le secteur de la défense. Des entreprises spécialisées dans le secteur de la défense (Thales, Airbus CyberSecurity...) ont également développé des expertises fortes en cybersécurité. Le ministère de la Défense lui-même est l'un des principaux recruteurs de spécialistes en 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 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 1)**.

– Tableau 1 –

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) ?

	Pour aujourd'hui	D'ici 3 à 5 ans
10	9%	22%
9	5%	22%
8	15%	25%
7	19%	14%
6	19%	7%
5	13%	6%
4	7%	2%
3	8%	1%
2	4%	1%
1	1%	0%
0	0%	0%
Note moyenne	**6**	**8**

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

LA CYBERSÉCURITÉ EN BRETAGNE : UN LEADERSHIP RECONNU

Il existe un véritable écosystème breton favorable à la montée en puissance de la filière cybersécurité. En dehors de l'Île-de-France, il s'agit d'ailleurs de la seule région française à disposer sur son territoire d'une infrastructure aussi riche que complexe[5], bénéficiant 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 dans 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. Pour ce qui concerne la Bretagne, les forces en présence se déclinent ainsi pour ces trois piliers :

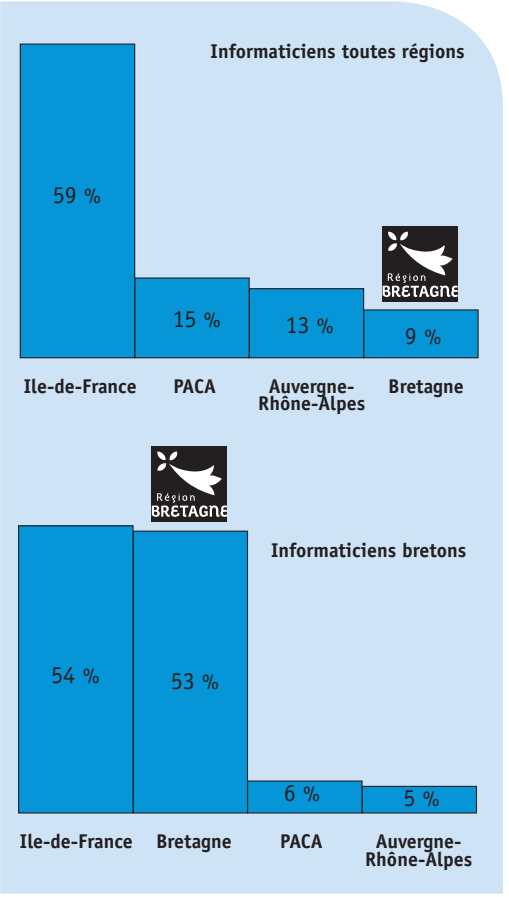
- Formation : une dizaine d'établissements d'enseignement supérieur proposent des formations initiales et continues à la cybersécurité, dont certaines de premier plan.
- Recherche : 200 chercheurs travaillent sur la cybersécurité en Bretagne au sein de centres de recherche de haut niveau.

5. L'Usine Nouvelle, *Cybersécurité : les 40 sites stratégiques*, n° 3452, 21 janvier 2016.

• Développement économique : de grands groupes sont implantés sur le territoire, ainsi qu'un tissu de PME/ETI innovantes.

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 **(figure 3)**.

– Figure 3 –
Les régions les plus à la pointe en matière de cybersécurité selon les informaticiens (deux réponses possibles)

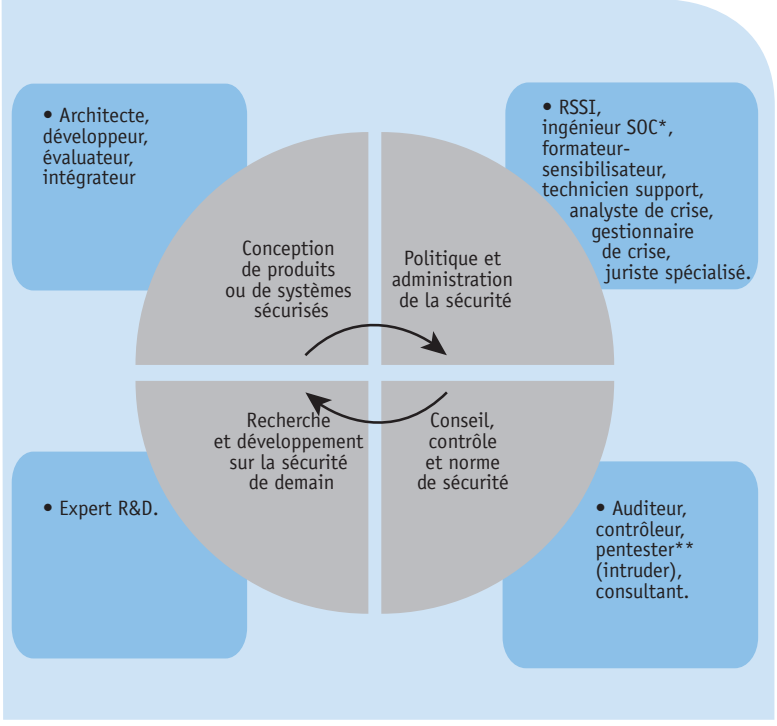


Source : Apec, 2017. Enquête auprès d'informaticiens connectés sur Apec.fr au cours des 12 derniers mois.

DES COMPÉTENCES TRÈS RECHERCHÉES ET EN TENSION

D'après le référentiel des métiers de la cybersécurité établi par le Pôle d'excellence cyber, la quasi-intégralité des métiers de la cybersécurité est de niveau cadre. Dans tous ces métiers **(figure 4)**, des compétences techniques très pointues sont demandées : évaluation de composants ou de logiciels, conception d'architectures sécurisées, détection de test 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.

– Figure 4–
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.

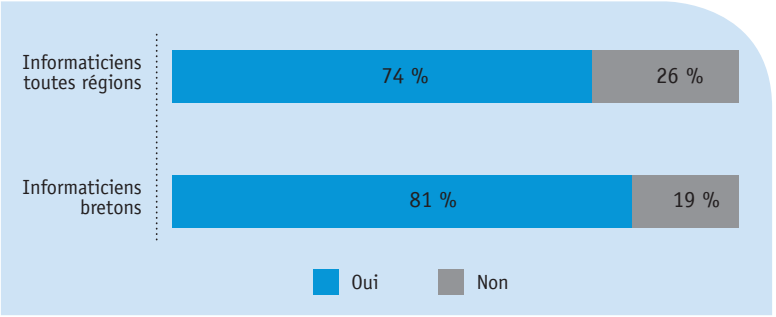
Les entreprises bretonnes s'accordent sur le fait qu'il existe, pour la plupart de ces postes, des difficultés en matière de recrutement. C'est particulièrement criant pour les métiers de consultant cybersécurité, architecte sécurité, développeur sécurité, auditeur de sécurité. Malgré ces difficultés, les entreprises bretonnes parviennent à embaucher, en adaptant leurs modes de recrutement au marché visé. L'utilisation du réseau relationnel et de la cooptation sont notamment largement utilisés. L'implantation en Bretagne semble également constituer un atout de choix pour les entreprises interrogées.

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 Paca.

UNE FORTE ATTRACTIVITÉ DE LA FILIÈRE POUR LES INFORMATICIENS

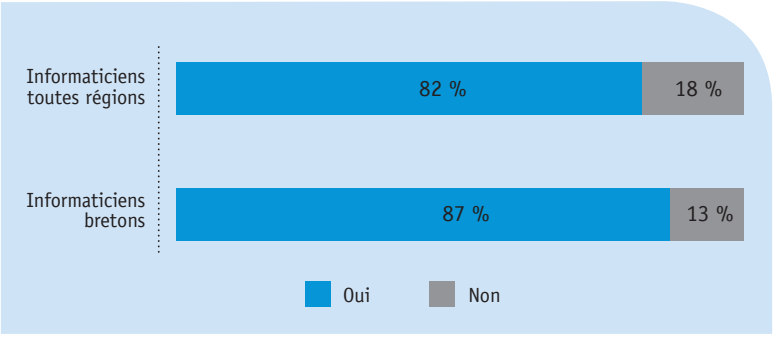
Les entreprises peuvent aussi bénéficier de l'attrait exercé par le domaine de la cybersécurité sur les informaticiens. En effet, 74 % des informaticiens seraient dans l'absolu intéressés pour travailler dans le domaine de la cybersécurité **(figure 5)**. Cette proportion monte à 81 % pour les informaticiens bretons. Et 82 % d'entre eux souhaitent d'une manière générale développer leurs compétences en cybersécurité (87 % en Bretagne) **(figure 6)**. Il convient de noter l'important écart d'opinion entre les femmes et les hommes sur ces questions, 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. De même, les femmes sont également moins nombreuses que les hommes, en proportion, à souhaiter développer leurs compétences en cybersécurité : 67 % contre 85 %. La capacité de la cybersécurité à attirer les femmes est donc problématique et cela doit être considéré comme un signal d'alerte pour l'avenir.

– Figure 5–
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 6–
Souhaiteriez-vous développer vos compétences en cybersécurité ?



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

En outre, 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 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). Pour 9 des 11 domaines, la note moyenne est égale ou inférieure à 5.
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

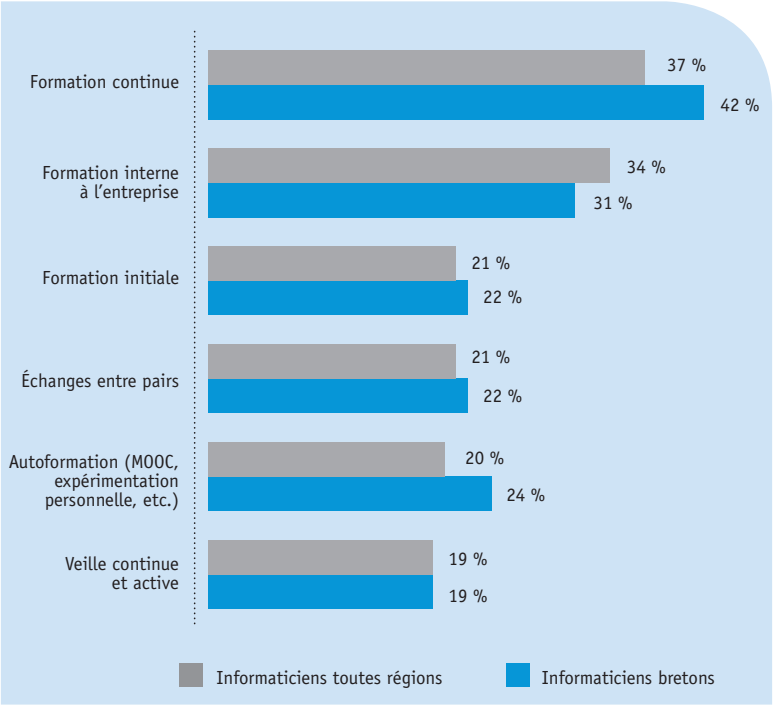
Le tissu de formation cyber est relativement bien fourni, notamment à l'échelle de la Bretagne. Les enseignements spécifiques continuent de se développer que ce soit dans les universités ou les grandes écoles. On remarquera toutefois que les entreprises ne cherchent pas que des juniors. Bon nombre de métiers de la cybersécurité nécessitent de l'expérience. C'est le cas essentiellement des métiers rattachés à la définition de la politique et de l'administration de la cybersécurité dans les entreprises. Mais c'est aussi le cas des métiers de consultants, d'auditeurs et d'architectes. Aussi, l'étude des offres en cybersécurité publiées sur le site 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 d'informaticiens 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 **(figure 7)**.

L'appétence des informaticiens pour la formation continue, en particulier en Bretagne, pose la question du type de formations à construire pour répondre aux besoins exprimés. Les 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 et les formations à mobiliser pour exercer un métier dans la cybersécurité, notamment au sein des référentiels métiers existants ou à créer.

– Figure 7 –

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.

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 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 (conseil, orientation, organisation d'évènements...). Certaines actions seront pérennisées au-delà de 2017.

–MÉTHODOLOGIE–

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 deux phases.

– Une enquête qualitative par entretiens individuels et groupes de travail auprès d'une trentaine d'entreprises, essentiellement bretonnes, recherchant des compétences en cybersécurité. Quelques experts ont également été interrogés.

– Une enquête quantitative en ligne auprès de 1 200 informaticiens issus d'un fichier Apec, dont 44 % résidant en Bretagne. 79 % de ces informaticiens étaient en emploi au moment de l'enquête. Après redressement, la population interrogée est représentative des informaticiens inscrits sur Apec.fr au cours des 12 derniers mois selon l'âge et la région. Il s'agit d'une population en recherche d'emploi ou en veille, ce qui rend d'autant plus intéressante leur vision sur l'évolution du marché et leurs souhaits d'évolution.

Elle débouche sur un plan d'actions concret qui sera mis en œuvre par la délégation Apec Bretagne, en collaboration avec les partenaires de l'étude.

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

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

Région BRETAGNE

BRETAGNE DÉVELOPPEMENT INNOVATION

PÔLE D'EXCELLENCE CYBER

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.
Maquette : Daniel Le Henry.
Direction de l'étude : Maïmouna Fossorier.
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

Apec
www.apec.fr

EDOBSA0236–5–05.17