

La Cybersécurité

DANS LES ENTREPRISES DU COMMERCE

Le secteur du commerce vit une transition importante vers les plateformes numériques, le e-commerce, la numérisation grandissante des transactions et l'utilisation de l'informatique en nuage. Cette transition peut être facteur de risques importants. En effet, le secteur est une cible pour les cybercriminels. De nombreuses transactions s'effectuent quotidiennement par carte de crédit et débit dans divers points de vente et en ligne. **Une cyberattaque peut représenter une perte du chiffre d'affaires et surtout une baisse de la confiance des clients. C'est pourquoi investir dans la cybersécurité peut représenter un avantage concurrentiel important.**

Afin de minimiser les différents risques qui émanent de ces technologies, le secteur doit s'assurer de mettre en œuvre des politiques, des procédures et surtout d'adapter les compétences de ses salariés.

Dans le cadre de la signature d'un Engagement de Développement des Emplois et des Compétences (EDEC), 7 branches du Forco, conscientes des enjeux de cybersécurité, ont souhaité mener une action visant à analyser et accompagner leurs entreprises dans leur évolution au regard en particulier de la transformation digitale.

Cette étude répond à un double objectif :

- **Identifier les besoins en compétences et en formations** dans le domaine de la cybersécurité spécifiques au secteur,
- **Recenser et qualifier l'offre de formation** en cybersécurité en réalisant une cartographie, à destination des entreprises, notamment des TPE-PME.

LES 7 BRANCHES DU COMMERCE COMMANDITAIRES DE L'ÉTUDE

- Commerce à prédominance alimentaire (détail et gros)
- Commerce de détail de l'horlogerie-bijouterie
- Commerce succursaliste de la chaussure
- Commerce succursaliste de l'habillement
- Grands magasins et Magasins populaires
- Horlogerie commerce de gros
- Import-Export

📍 DONNÉES CLÉS DE LA CARTOGRAPHIE

La cybersécurité est **l'affaire de tous** : chaque usager peut être le maillon faible de la chaîne de sécurité

La cybersécurité est au cœur de la préoccupation de gouvernance et constitue un **enjeu de positionnement stratégique**



50% des formations en cybersécurité sont d'un niveau 7 (bac + 5)



4 formations sur 5 sont à destination des experts IT



La sensibilisation des utilisateurs est la thématique la moins couverte par l'offre de formation.

LA CYBERSECURITE DANS LES ENTREPRISES DU COMMERCE

PRINCIPALES TENDANCES ISSUES DE L'ETUDE

► La cybersécurité est en lien avec de nombreux enjeux

Enjeu business, protection des données, défense des secrets industriels et commerce en ligne.

► Les entreprises ne sont pas suffisamment protégées

Frein financier, tendance à minimiser les risques encourus et sentiment d'invulnérabilité face aux attaques.

► Il y a des besoins en compétences et en formation

Sensibilisation du grand public : le capital humain est le premier risque.

2 idées reçues sur la sécurité informatique

« C'est le problème des services techniques »

Oui, pour le déploiement de la mise en œuvre des systèmes d'information mais :

- C'est un **sujet de gouvernance** à s'approprier par les membres du comité de direction, les directions fonctionnelles et les Managers.
- La sécurité informatique est liée à des actions d'analyse, de coordination et de communication impliquant toutes les équipes.

« C'est trop cher »

Un coût élevé pour la première étape de cartographie/audit des systèmes d'information (SI) mais :

- Une fois réalisée la **mise à jour est moins coûteuse**
- Un **investissement en SI amorti** au vu des risques encourus



L'ANSSI a réalisé un guide des bonnes pratiques en matière de sécurité informatique
<https://www.ssi.gouv.fr/administration/bonnes-pratiques/>

ILS L'ONT DIT

Aujourd'hui, un dirigeant doit se poser la question : en quoi ma politique cyber rassure mes clients et répond à mes besoins propres ?

On n'est pas suffisamment conscients de ce qu'on peut perdre.

La problématique de la cybersécurité renvoie à celle de la sécurité en général, l'esprit de vigilance est l'affaire de tous.

Les cybercriminels s'orientent vers les attaques les plus rentables en particulier en direction des entreprises.

CE QU'IL FAUT RETENIR

- 105 organismes de formation identifiés
- 489 formations en cybersécurité
- Le paysage de l'offre de formation aujourd'hui :
 - 80% des formations à destination des experts IT
 - 50% des certifications de niveau 7 (bac+5)

L'OFFRE DE FORMATION EN CYBERSECURITE

489 formations identifiées en cybersécurité

120 formations certifiantes

- 21 licences professionnelles
- 41 masters
- 16 titres d'ingénieurs
- 13 titres RNCP
- 29 certifications inscrites au répertoire spécifique

369 formations non certifiantes dont

- 221 formations courtes (moins de 28h)
- 12 mastères spécialisés
- 2 Badges

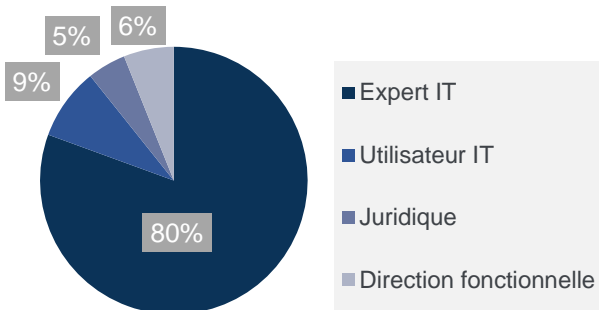
Par qui ?

- 29 organismes de formation (spécialisés ou généralistes)
- 37 écoles d'ingénieurs
- 39 universités

Cette offre de formation regroupe une majorité de **formations courtes**. La moitié des formations dispensées sont d'une durée inférieure à 4 jours.

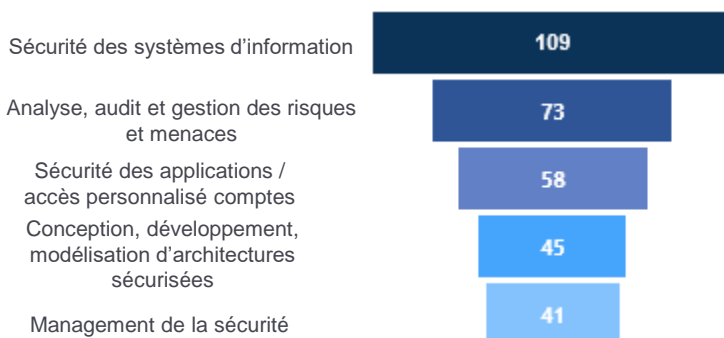
Les cinq organismes dispensant le plus de formations en cybersécurité sont des **organismes de formation privés** proposant des formations **non certifiantes**.

Répartition des formations cartographiées selon le public visé



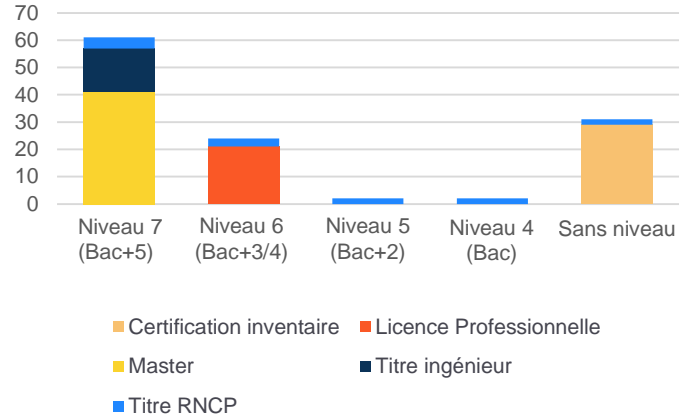
Les **experts IT** constituent le public visé largement majoritaire des formations en cybersécurité (4 formations sur 5).

TOP 5 des thématiques les plus couvertes (en nombre de formations)



Les thématiques **les plus couvertes** par l'offre de formation en cybersécurité sont **les plus généralistes**.

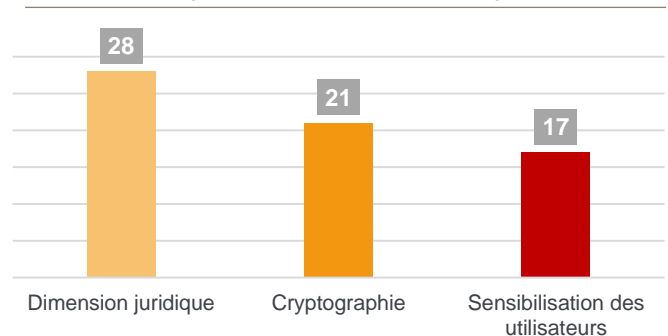
Répartition des types de sanction par niveau (en nombre de formations)



La majorité de l'offre de formations certifiantes en cybersécurité est d'un **niveau élevé**, la moitié des formations sont de **niveau 7** (Bac+5). Elles visent des compétences en **conception** exercées en toute **autonomie**. On constate une large majorité de **Masters**.

ÉLÉMENTS CLÉS

TOP 3 des thématiques les moins couvertes (en nombre de formations)



Les thématiques **les moins couvertes** concernent des **domaines spécifiques**.

Si la **sensibilisation des utilisateurs** apparaît comme un **enjeu** majeur pour les entreprises, cette thématique s'avère être la **moins proposée** par les organismes en matière de cybersécurité.

Toutefois, la formation n'est pas le seul outil mobilisable.

D'autres outils existent.



Réaliser des campagnes de sensibilisation grâce à différents canaux de communication.

Affiches, vidéos en ligne, mailing...



Transmettre les bonnes pratiques en matière de sécurité informatique en agissant directement en situation de travail.

LA CYBERSECURITE DANS LES ENTREPRISES DU COMMERCE

PLATEFORME DES FORMATIONS EN CYBERSECURITE

POUR TROUVER SA FORMATION EN
CYBERSECURITE :

<https://cyberform.forco.org>



SOURCES ET MÉTHODOLOGIE

Etude menée par le cabinet **Lafayette Associés** et pilotée par l'**Observatoire prospectif du commerce** de septembre 2018 à janvier 2019.

Sources de données :

- Cybersecurity : the new source of competitive advantage for retailers – Capgemini- 2018
- Entreprises et Cybersécurité à l'horizon 2020 – CIGREP – 2015
- Cartographie interbranches sur les métiers du web et du numérique dans les entreprises du commerce – Obea FORCO – 2018
- Cartographie des métiers de la cybersécurité – ANSSI
- Cybersécurité en Bretagne l'enjeu des compétences – APEC – 2017
- Les formations et les compétences en France sur la cybersécurité – OPIECC- 2017
- Formation à la cybersécurité des TPE et PME, Référentiel pédagogique pour les organismes de formation – Direction générale des entreprises SISSE – 2017
- Quel référentiel pour les métiers de la Cybersécurité ? – Ceis – 2014
- Les métiers et compétences recherchés dans le Cloud, le Big Data, la Cybersécurité – APEC – 2018

Entretiens qualitatifs :

Entreprises adhérentes aux branches commanditaires de l'étude
Organismes de formation spécialisés en cybersécurité et généralistes
Experts IT et juridique

L'OBSERVATOIRE PROSPECTIF DU COMMERCE A POUR MISSION :



de réaliser un état des lieux
quantitatif des emplois,
des qualifications et de la formation.



de contribuer à adapter
l'offre de formation et à faire
évoluer l'offre de certification.



d'assurer une veille sur l'évolution
des métiers, des qualifications et détecter
les métiers en tension ou émergents.

Retrouvez toutes les publications de l'observatoire sur
www.forco.org/Branche/ObservatoireProspectifDuCommerce

Directeur de la publication : Philippe Huguenin-Génie
Directeur de rédaction : Fanny Coste
Rédaction : Marie-Ingrid Brézé (Forco), Mathieu Hivet, Olivier Erramoun et Lisa Pommier pour le cabinet Lafayette Associés