MAJORS CONSULTANTS

Observatoire prospectif du commerce

Etude sur les besoins en compétences des entreprises du bureau et du numérique en matière d'IT et de Cybersécurité

Phase d'approfondissement des résultats

Macro planning du projet

Préparation

- Elaboration premières versions questionnaires
- Audit fichiers + qualification
- Préparation des éléments de communication
- Collecte sources documentaires,
- Réunion lancement, (validations, ajustements)

Phase 1 (étude doc + entretiens cadrage)

- Analyse documentaire
- Sélection contacts + communication
- Réalisation 5 entretiens qualitatifs
- Synthèse + préconisations suite du dispositif
- Restitution/partages/ + ajustements questionnaire

Phase 2 (enquête web/tel)

- lancement enquête web + relances
- Brief des enquêteurs
- Réalisation entretiens téléphoniques (après 2 semaines) : objectif global = 400 réponses
- Synthèse + préconisations suite du dispositif
- Restitution résultats + ajustements suite dispositif

Phase 3 (entretiens RH + audit offre formation)

- Sélection contacts + communication
- Réalisation 15 entretiens qualitatifs
- Etude offre de formation/ certification

Conclusions + restitutions

- Analyse approfondie des résultats + préconisations
- Restitutions des résultats/atelier de travail (x2)
- Edition synthèse communicante

Analyse documentaire et entretiens qualitatifs

Premiers enseignements

Rappel préalable : la cybersécurité = un enjeu majeur pour les entreprises

Des risques de cybersécurité en augmentation du fait de :

- La numérisation de l'économie (e-commerce, digitalisation des process), accélérée avec le confinement lié au développement du télétravail et au déploiement de la fibre ;
- La professionnalisation de la cybercriminalité, facilitée par sa « plateformisation », son industrialisation, et le développement des cryptomonnaies ;
- La difficulté de la prévention et de la répression, lesquelles nécessitent à la fois la prise de conscience de tous et une coopération internationale efficiente ;
- L'intégration du cyberespace comme nouveau vecteur de la conflictualité géopolitique dont les entreprises sont soit les cibles soit les victimes collatérales.

Dans ce contexte, les PME et les TPE sont les plus démunies face à ce phénomène ; au-delà des infrastructures et de la possession d'un pare-feu/antivirus, ce sont souvent les utilisateurs qui constituent le principal risque face aux attaques (ex : phishing) car souvent peu sensibilisés/acculturés aux risques de cyberattaque ➔ une opportunité majeure pour les entreprises du bureau et du numérique qui peuvent renforcer leur rôle de prescripteur et de sensibilisation auprès de ces entreprises.

En parallèle, le marché du cloud tend à s'imposer (possédé à 70% par des sociétés américaines) ce qui tend à structurer l'offre informatique des entreprises de la branche et conditionne en partie les actions en matière de cybersécurité. Toutefois les premiers entretiens révèlent des positionnements contrastés sur le sujet.

Premiers enseignements

Face à ce phénomène, les institutions et le marché s'organisent pour mieux accompagner les entreprises

Un état qui « muscle » les dispositifs

- Mise en application de la directive NIS-2 (octobre 2024) qui étoffe la réglementation autour de la cybersécurité et de manière plus prescriptive, élargie le nombre d'entreprises concernées
- Déploiement/promotion d'un service d'urgence aux entreprises (cybermalveillance.gouv.fr)
- Adaptation du droit de la commande publique pour favoriser la cybersécurité
- Renforcement des réponses/procédures pénales à la cybersécurité
- Mise en place de plans nationaux de prévention à la cybersécurité
- Subventions pour aider les entreprises à auditer leur risque de sécurité (chèque diagnostic cyber en IDF ; CyberPME/ BouclierCyber au niveau national via Bpifrance)
- Développement et promotion des métiers de la cybersécurité

Un marché qui se structure

- Développement d'offres cybersécurité parmi des acteurs du IT/Numérique/sécurité : Microsoft (Copilot) Thales (Imperva), Docaposte (Package Cyber PME) ; Vinci energie (Fernao), …
- Développement du marché de l'assurance en matière de cybersécurité (ex : Axa, Allianz, Stoïk, …) intégrant parfois en amont des actions de sensibilisation/formations des collaborateurs et un diagnostic
- Labellisation des entreprises de services IT avec une certification « Expert certification » ; développement d'accompagnements notamment sur les diagnostics de sécurité
- Développement d'offres de sensibilisation à la cybersécurité auprès des salariés (formation, sensibilisation, guides pour les TPE/PME, …)
- Quelques chiffres clés sur le marché français :
  - En 2024 : 7 milliards d'euros
  - Prévision 2029 : 13 milliards d'euros

Premiers enseignements

Focus : les impacts de la directive NIS-2 pour les entreprises concernées

Les obligations des entreprises concernées

- Devoir de notification, de contacts de déclaration des incidents majeurs (notification, rapport d'avancement, rapport final)
- Obligation de mise en place de mesures de sécurité pour l'ensemble de leur réseau/système d'information (plus seulement essentiel) :
  - analyse des risques,
  - gestion des incidents,
  - gestion de la continuité des activités (sauvegarde),
  - mise en place de procédures de gestion, vis-à-vis de la cryptographie,
  - **sécurisation des fournisseurs/prestataires ; des acquisitions,**
  - sécurisation des accès, de l'authentification

➔ En cas de non-respect, des sanctions peuvent aller jusqu'à 2% du chiffre d'affaires de l'entreprise.

Les secteurs/entreprises concernés

	Chiffre d'affaires	Nombre d'employés
Entités essentielles + certaines importantes	>50 millions	> 250 salariés
Entités importantes	10 à 50 millions	50 à 250 salariés

- **Entités essentielles** ; ex : energie, transport, banque/marché financier, infrastructure numérique, administration publique, santé, …
- **Entités importantes :** fabrication, recherche, alimentation, gestion déchets, fournisseurs numériques

➔ Soit environ 18 secteurs et 10 000 entreprises concernées vs 300 par la NIS1.

Premiers enseignements

Les entreprises du bureau et du numérique : impacts de l'évolution de l'environnement des entreprises sur l'offre :

I. Le développement de l'offre de cybersécurité : un changement de « paradigme » dans la relation aux entreprises

- Des nouvelles offres de cybersécurité au-delà des antivirus/sécurisation des serveurs : mise en place de diagnostics de cybersécurité ; sessions de sensibilisation/formation des collaborateurs à la cybersécurité ; partenariat avec des assureurs cybersécurité (mise en place des outils de surveillance).
- Un rôle de « prescripteur » auprès des entreprises qui tend à s'affirmer : sensibilisation accrue sur le minimum d'équipement/procédure à adopter par l'entreprise ; voire un minimum contractuel.

➔ Des changements qui concernent a priori davantage les entreprises orientées vers les services IT. Parmi les entreprises plus généralistes (bureautique), l'offre peut s'orienter vers la sécurité au sens large (sécurité des locaux et des infrastructures dont la cybersécurité) avec le développement d'une approche « Service Manager » (définition du besoin client et maintien dans le temps) ce qui implique un changement dans l'approche et le mode de contractualisation.

Des évolutions de marché qui constituent de fortes opportunités pour les entreprises et des perspectives de croissance importantes. Dans le cadre de la NIS-2, les entreprises de la branche pourront peut-être aller au-delà de l'accompagnement à la mise en conformité des process et infrastructures, en conseillant leur client dans le développement des compétences en interne.

Premiers enseignements

Les entreprises du bureau et du numérique : impacts de l'évolution de l'environnement des entreprises sur l'offre :

II. Le développement l'offre Cloud : une tendance qui tend à s'imposer mais avec des positionnements qui peuvent être contrastés parmi les entreprises de la branche

- Un marché du Cloud qui tend à s'imposer et impactent la stratégie des entreprises :
  - Diminution/suppression des solutions d'hébergement en propre.
  - Prescription aux entreprises qui ont leur propre serveur à passer progressivement sur des solutions cloud.

➔Des changements qui peuvent être en rupture avec le positionnement initial des entreprises, provoquant parfois des résistances/adaptations des équipes.

Toutefois, la tendance ne semble pas uniforme. Certaines entreprises de la branche spécialisées dans les services IT restent pour le moment attachées au modèle des infrastructures physiques (« culture » du hardware) ; les entreprises plus généralistes peuvent parfois développer plus facilement l'offre Cloud ➔ un risque pour les spécialistes de l'IT qui n'auront pas pris le virage rapidement ?

Premiers enseignements

Les entreprises du bureau et du numérique : impacts de l'évolution de l'environnement des entreprises sur l'offre :

III. L'IA : un enjeu identifié comme majeur, mais qui ne trouve pas encore une vraie formalisation dans l'offre. Les enjeux évoqués :

1. Le développement de l'IA sur les activités de diagnostic/maintenance des installations (IT/Print) avec l'émergence potentiel de 2 types de profils : des développeurs et des techniciens de maintenance gérant les outils IA.

2. L'automatisation de la gestion des demandes (Chatbox), avec notamment du contenu sur les procédures liées à l'impression et à l'informatique.

3. L'accompagnement sur l'implémentation de nouvelles offres sur le marché comme Copilot de Microsoft, sans forcément proposer des solutions plus personnalisées/sur mesure (implique une connaissance métier très forte et du développement).

4. Plus classiquement, l'accompagnement des entreprises dans un équipement (ordinateurs/infrastructures) en adéquation avec les exigences de performance du développement l'IA dans leurs activités.

Premiers enseignements

Les impacts de l'évolution de l'offre sur les organisations et les métiers

L'impact du développement de l'offre de cybersécurité sur les organisations et les métiers

Au niveau des organisations :

- Tendance au renforcement des équipes à la fois techniques mais aussi au niveau commercial sans forcément opter pour des profils spécialisés : à la fois parce que la cybersécurité s'intègre dans l'ensemble des offres informatiques ; et parce qu'un profil spécialisé pourrait se sentir limité dans ses missions.
- Structuration forte des procédures et de la méthodologie d'intervention adaptées à la cybersécurité (travail de veille/formation, collaboration avec des experts, création de poste de directeur des opérations pour mieux coordonner les métiers technique et commercial, …)

Au niveau des métiers :

- Métiers techniques : des impacts à la fois sur le discours client ; la mise en place d'une méthodologie plus structurée, la nécessité de feedback systématiques et plus précis au client. Une coordination plus importante avec les métiers commerciaux (du fait du formalisme plus important).
- Métiers commerciaux : des changements dans le discours, avec une approche potentiellement plus directive, de prescripteur
- Métiers de la communication : pour certains, un travail de veille et de communication/sensibilisation plus fréquent et structuré auprès de leurs clients (ex : édition et diffusion de newsletters mensuelles).

Premiers enseignements

Les impacts de l'évolution de l'offre sur les organisations et les métiers

L'impact du développement de l'offre Cloud sur les organisations et les métiers

Au niveau des organisations :

- Pour certains, recentrage sur l'offre Cloud, avec une diminution des solutions d'hébergement.

Au niveau des métiers :

- Métiers techniques : des impacts marginaux au-delà de la formation technique au cloud, une offre de formation jugée bien structurée.

- Métiers commerciaux : des changements de discours parfois en « rupture » avec l'argumentaire initial, ce qui peut nécessiter un accompagnement au changement et potentiellement un « vernis » technique pour s'approprier le discours.

Premiers enseignements

Les pratiques de formation et les attentes éventuelles pour couvrir les besoins des entreprises

Développement de l'offre de cybersécurité

- Pour la plupart des spécialistes en IT, le travail de formation en interne (veille, de collaboration avec des experts) et l'obtention de la certification « ExpertCyber » sont jugés suffisants pour couvrir leurs besoins.
- Pour autant, certains estiment que l'offre de formation initiale est plutôt orientée vers profils ingénieurs, pas forcément adaptés aux besoins des entreprises de la branche (trop techniques et exigeants compte tenu des missions qui leur sont confiées).
- Dans ce cadre, il conviendrait de former davantage de profils BTS avec des compétences pour gérer les activités au quotidien : mis à jour de la sécurité des équipements, réponses aux incidents, activité de surveillance et d'alerte, diagnostic, … ➔ A noter que 40% des diplômés d'un BTS cybersécurité poursuivent leur étude, ce qui peut expliquer en partie ce ressenti.

Développement l'offre Cloud

- Pas de besoin côté technique compte tenu de la densité de l'offre formation.
- Côté commercial, développer une formation/un module pour renforcer le discours technique sur l'hébergement.

Premiers enseignements

Les profils recherchés par les entreprises de la branche : plutôt des profils généralistes avec des compétences en cybersécurité et non des spécialistes.

Veille sur les profils recherchés par les entreprises de la branche

- **Intitulés de poste :** technicien support ; ingénieur réseaux et sécurité ; technicien sûreté électronique ; ingénieur Commercial Logiciels de Gestion ; technicien télécom et réseaux ; technicien expert ; technicien informatique ; technicien maintenance, technicien Systèmes et Réseaux Services Managés, chargé d'affaires,…

- **Compétences techniques recherchées (ex de profils techniques) :** Connaissances en matériel informatique et systèmes d'exploitation ; Installation / Administration des environnements serveurs Windows ; virtualisation ; systèmes de sauvegarde ; réseaux informatiques et protocoles de communication ; Cloud & Hébergement ; Infrastructure

- **Compétences comportementales généralement valorisées :** relationnel client et avec les équipes ; capacité d'adaptation ; pédagogie ; capacité à préparer un chantier/réaliser une installation (rigueur), …

Un premier travail de veille d'offres d'emploi (>50 annonces auditées) d'entreprises de la branche a montré :

- Qu'aucun profil spécialisé « cybersécurité » n'est recherché
- Que les compétences techniques recherchées sont généralement relatives à des environnements techniques ; quasiment aucune annonce aborde la notion de cybersécurité ou de sécurité.
- Au-delà des compétences techniques, les compétences comportementales sont souvent plus valorisées dans la sélection des candidatures

➔la cybersécurité semble donc être une compétence sous-jacente aux activités techniques avec peut-être un accompagnement interne sur le sujet.

Vue générale de la consultation

Rappel Phase 2

- Déploiement d'une enquête Web/téléphonique auprès d'un panel d'entreprises, réalisée par des enquêteurs de haut niveau, selon la méthode des quotas. Un objectif de 300 réponses au total (dont 200 au téléphone) afin de garantir des résultats fiables et une analyse par taille/activité.
- Objectifs : obtenir des résultats représentatifs sur le développement de l'IT et de la Cybersécurité dans l'offre des entreprises ; sur les évolutions réalisées/anticipées et les éventuelles difficultés rencontrées ; les impacts et actions réalisées : profils des salariés impactés, pratiques de recrutements et de formations, …

Bilan de la phase 2 :

Fichier transmis l'Opcommerce = 1 825 (SIREN)

1 586 entreprises a priori dans le périmètre de l'étude

239 entreprises (13%) hors périmètre de l'étude : pas de service informatique (168), qui ne sont pas dans le secteur (23), qui n'existent plus a priori (48)

204 entreprises répondantes (13%)

984 injoignables sur la période / qui n'ont pas trouvé du temps à nous consacrer

431 refus (27%) : pas intéressé/pas le temps ; barrage de l'accueil de l'entreprise

171 entretiens réalisés par téléphone

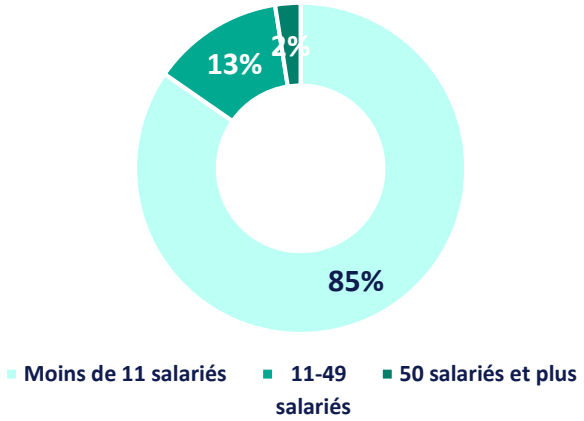
33réponses web (2%)

- Au bilan, une phase de recueil difficile avec en particulier peu de réponses web (>100 réponses espérées) qui s'explique à la fois par la part d'entreprises non concernées (27% des entreprises joignables), par le volume important de refus (431) qui démontre l'intérêt limité sur le sujet notamment concernant la cybersécurité.
- L'échantillon répondants garantit toutefois une bonne fiabilité des résultats au global (fiabilité ±5,2%) et autorise une analyse par taille et activités.

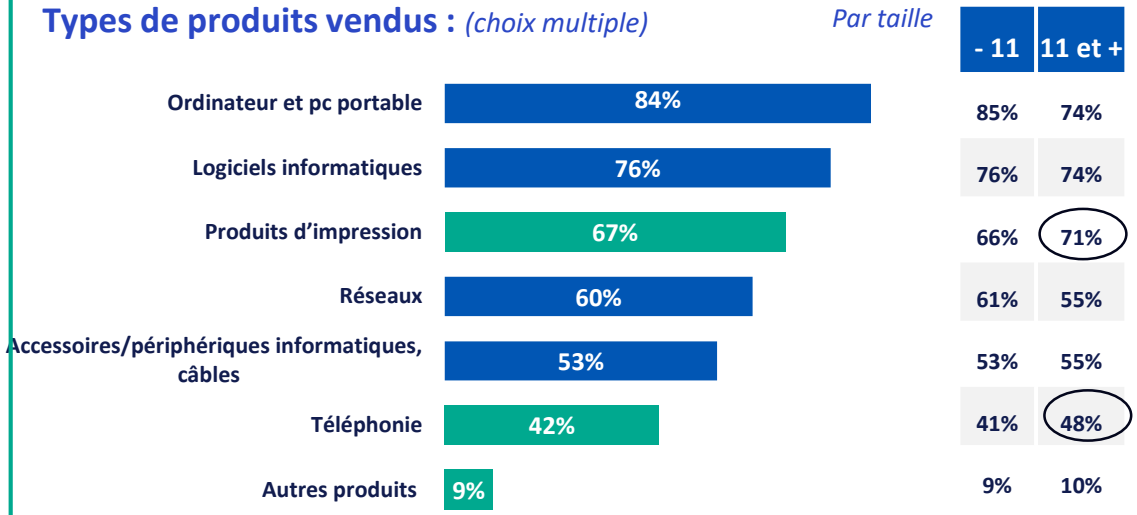
Caractéristiques des entreprises qui proposent des services informatiques

Typologie des produits proposés par les entreprises qui proposent des services informatiques

Taille d'entreprise :



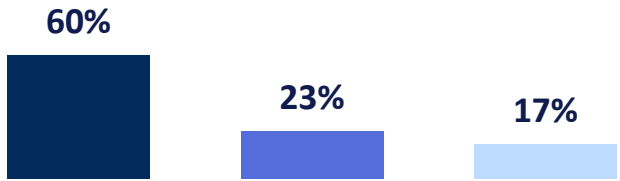
Types de produits vendus : *(choix multiple)*



- 85% des entreprises qui proposent des produits et services en rapport avec l'informatique comptent moins de 11 salariés (vs 91% à l'échelle de la branche).
- Les 2/3 d'entre-elles proposent également des produits d'impression et 42% des produits de téléphonie ➔davantage les entreprises de 11 salariés et plus.

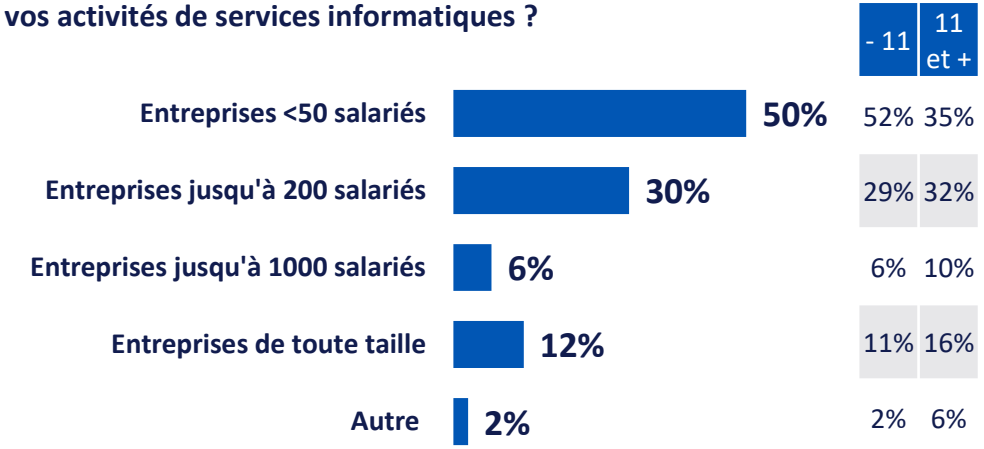
Activités de services informatiques

Que représente aujourd'hui votre activité de services informatiques dans votre chiffre d'affaires ?



	Activité principale/unique	Activité importante	Activité secondaire
-11	63%	21%	16%
11 et +	44%	38%	19%

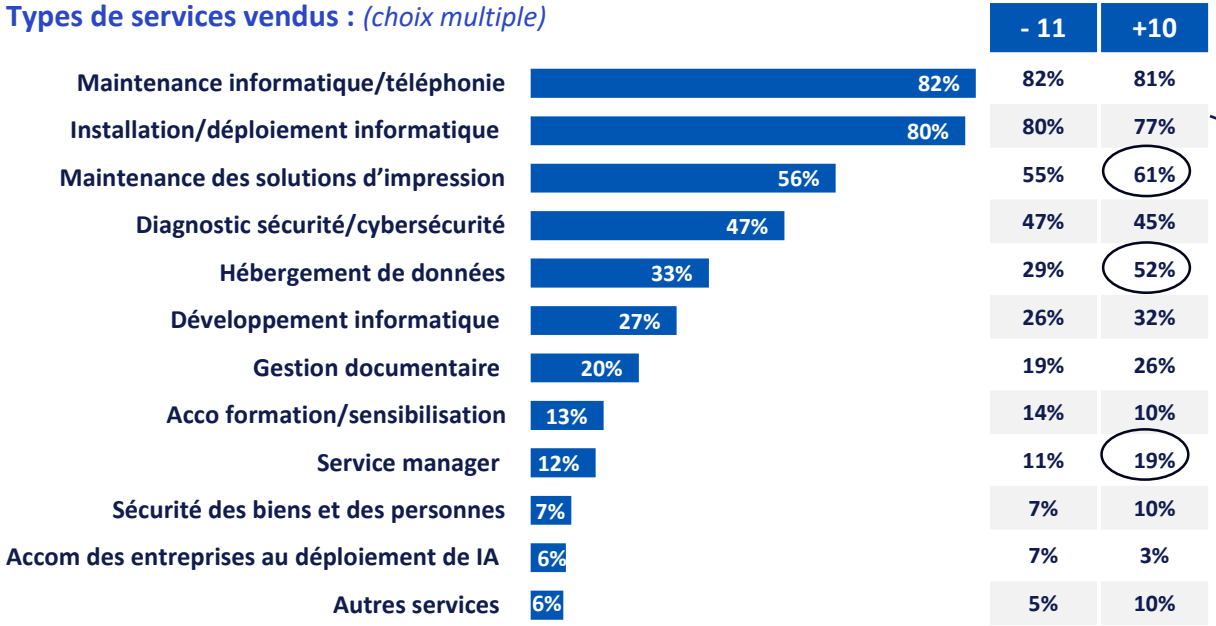
De quelles tailles sont les entreprises que vous accompagnez dans vos activités de services informatiques ?



- Pour 60% des entreprises, les services informatiques représentent l'activité unique/principale, cela passe à 63% pour les petites structures.
- La moitié d'entre elles n'accompagne que des entreprises de moins 50 salariés quand 18% proposent leur service à des entreprises de plus de 200 salariés (26% parmi les structures de plus de 10 salariés).

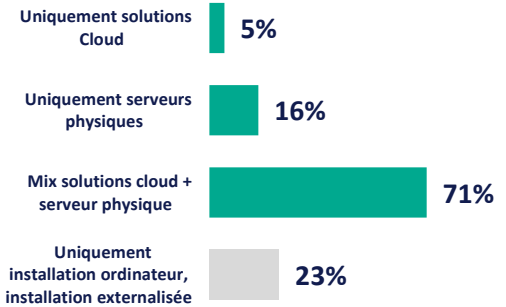
Typologie des services proposés

Types de services vendus : *(choix multiple)*



	- 11	+10
Maintenance informatique/téléphonie	82%	81%
Installation/déploiement informatique	80%	77%
Maintenance des solutions d'impression	55%	61%
Diagnostic sécurité/cybersécurité	47%	45%
Hébergement de données	29%	52%
Développement informatique	26%	32%
Gestion documentaire	19%	26%
Acco formation/sensibilisation	14%	10%
Service manager	11%	19%
Sécurité des biens et des personnes	7%	10%
Accom des entreprises au déploiement de IA	7%	3%
Autres services	5%	10%

Concernant les serveurs, quelles sont les solutions proposées :



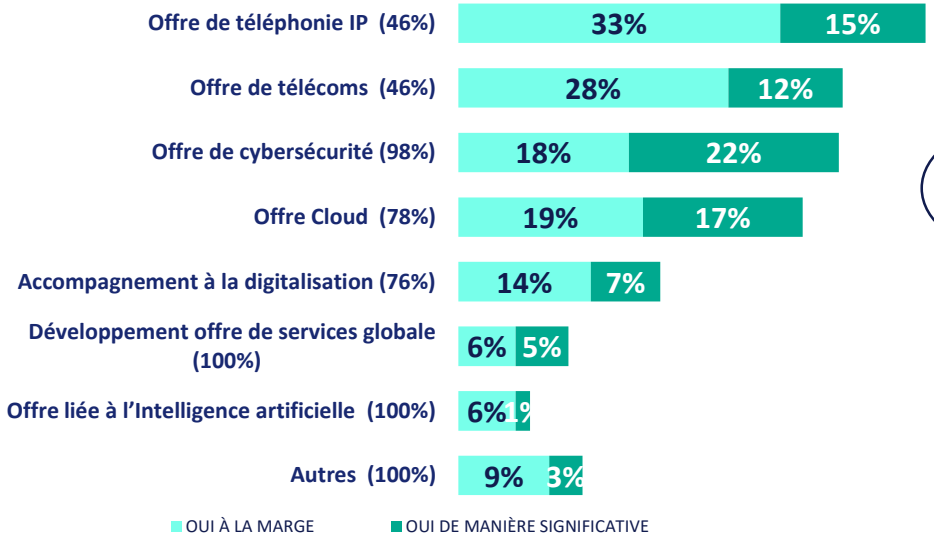
- Quasiment toutes les entreprises proposent a minina de la maintenance informatique ou de l'installation (8% ne font ni l'un ni l'autre).
- Près de la moitié proposent des services/solutions en rapports avec la cybersécurité.
- Parmi celles qui installent des serveurs, les solutions uniquement cloud ou physique deviennent marginales ; 76% proposent du Cloud (soit 61% de la totalité des entreprises répondantes).

Evolution de l'offre IT/cybersécurité et impacts sur les besoins en compétences

Evolution des offres commerciales en matière de services informatiques

Votre offre commerciale en matière de services informatiques a-t-elle évolué depuis ces 2 dernières années :

(xx%) entreprises concernées par la question

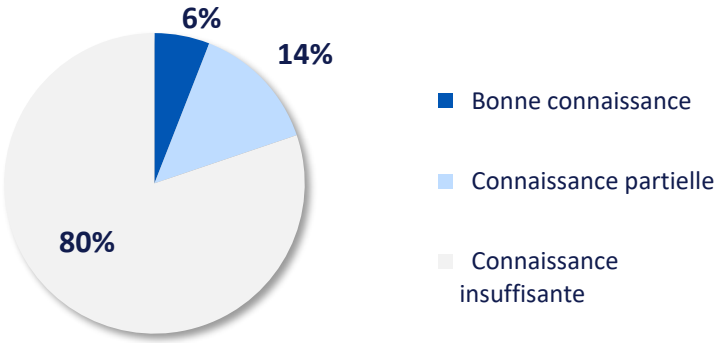


% Cumul	Contexte/Caractéristiques des évolutions
48%	Activité en développement du fait qu'elle s'apparente à de l'informatique ; augmentation de la demande (et contexte fibre)
40%	Vente d'antivirus/firewall ; sauvegarde ; sécurité réseaux ; protection boîtes emails ; Système d'authentification multi facteurs (MFA) ; service de test de fishing/intrusion ; conseil ; audit de sécurité ; formation
39%	
36%	Augmentation de la demande, moins de réticence au cloud
21%	Solutions d'archivage ; sensibilisation à la numérisation ; formation.
11%	Peu de commentaires
7%	COPILOT ; utilisation dans la vidéo protection ; quelques applications métiers (restaurant, laboratoires)
13%	Vidéos surveillance ; écrans interactifs ; impression 3D ;

- Au-delà de l'évolution de l'offre de téléphonie qui concerne moins de la moitié des entreprises répondantes, l'offre de cybersécurité (installation de logiciels de sécurité en majeur) et le cloud (plus de demandes) tendent à se développer pour plus d'un tiers des entreprises. L'intelligence artificielle reste très marginale à ce stade.

La NIS-2 et son impact

Comment évaluez-vous votre connaissance de la mise en application de la Directive NIS-2 ? (Question posée à 100% des entreprises répondantes)



Avez-vous prévu dans les mois à venir des adaptations de votre offre pour accompagner vos clients sur le sujet ? ➔10%

Variations selon les entreprises	Connaissance partielle	Bonne connaissance	Cumul connait
Connaissance selon la taille de l'entreprise			
- 11	**14%**	**6%**	20%
11 et +	**13%**	**6%**	19%
Connaissance selon l'offres de services			
DIAGNOSTIC SÉCURITÉ/CYBER	**20%**	**12%**	32%
SÉCURITÉ BIENS & PERSONNES	**0%**	**33%**	33%
Connaissance selon la taille des entreprises accompagnées			
<50	**14%**	**6%**	20%
50-200	**12%**	**6%**	18%
200-1000	**18%**	**3%**	21%
>1000	**15%**	**4%**	19%

- Seules 6% des entreprises estiment avoir une bonne connaissance de la directive NIS-2 et 14% une connaissance modérée.
- Un niveau de connaissance légèrement plus élevé (32%) parmi les entreprises qui accompagnent des entreprises sur la partie cybersécurité (on retiendra que cet accompagnement est souvent limité à l'installation de logiciels).
- Un enjeu d'adaptation de l'offre pour accompagner les clients qui reste très limité (10%) : *certaines entreprises témoignent de la réticence des entreprises à s'intéresser à ces enjeux (et/ou ne sont pas concernées), ce qui peut freiner le développement de ces activités dans les entreprises du secteur.*

Les compétences clés testées : rappel

Technicien de maintenance informatique/cybersécurité : Consigner les interventions réalisées en complétant et en transmettant les supports de suivi aux clients et à la hiérarchie, afin d'assurer une traçabilité et une communication claire des actions effectuées

Technicien de maintenance informatique/cybersécurité : Mettre en œuvre les procédures de travail établies pour les interventions et leur suivi afin de garantir la qualité de service et respecter les engagements contractuels.

Technicien de maintenance informatique/cybersécurité : Intervenir dans diverses situations et incidents en analysant les risques potentiels et en mobilisant des connaissances et compétences techniques et méthodologiques avancées en cybersécurité, afin de sécuriser les systèmes informatiques, protéger les données sensibles des clients, et permettre la continuité des activités.

Technico-commercial IT : Déterminer et prescrire des équipements, solutions et procédures adaptés aux besoins et spécificités des clients afin de garantir une efficacité optimale en matière de sécurité et répondre, le cas échéant, aux exigences de mise en conformité en matière de réglementation de cybersécurité.

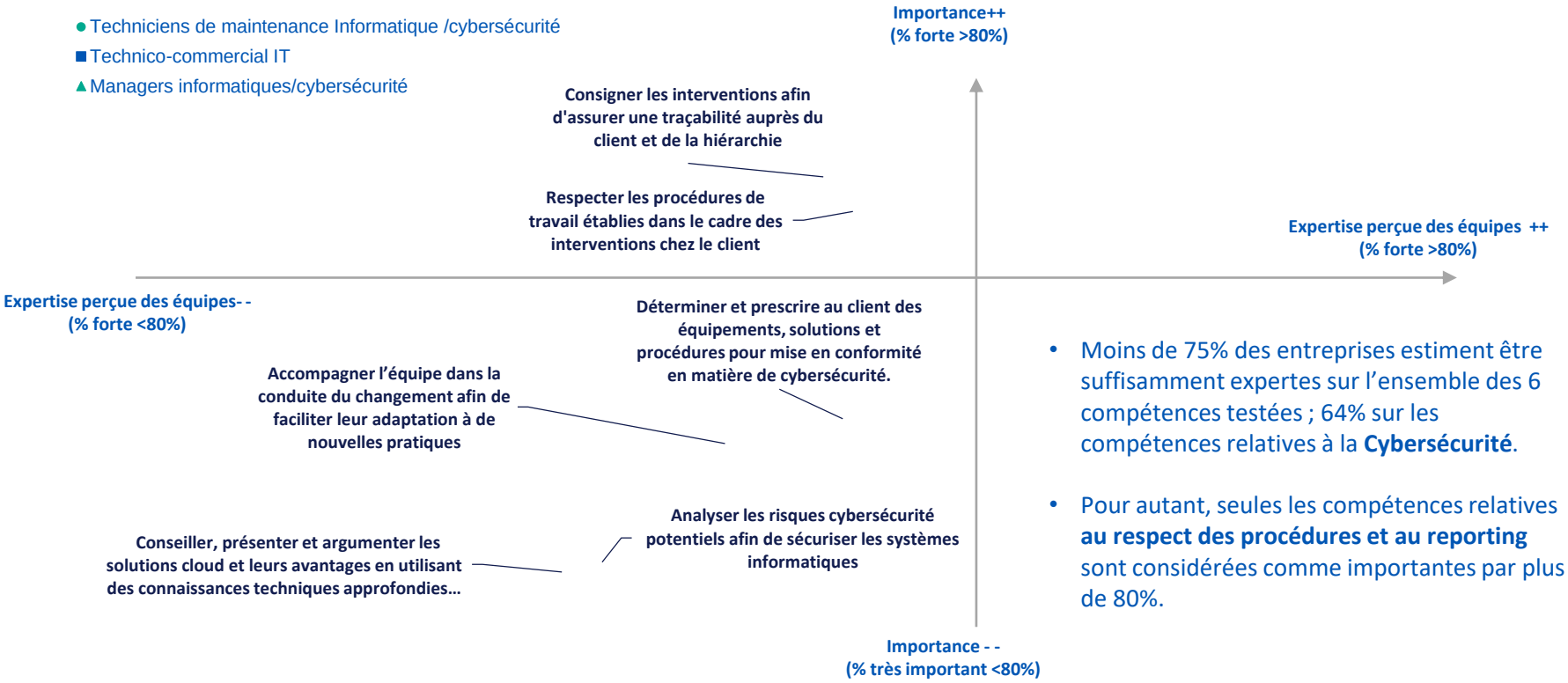
Technico-commercial IT : Conseiller, présenter et argumenter les solutions cloud et leurs avantages en utilisant des connaissances techniques approfondies aux technologies cloud afin de répondre aux besoins actuels du marché et des exigences des clients.

Manager : Accompagner les membres de son équipe dans les évolutions d'environnements techniques et les évolutions du marché en mettant en œuvre des méthodes et outils de conduite du changement afin de faciliter leur adaptation et permettre une transition vers de nouvelles pratiques.

- Pour rappel, 6 compétences clés identifiées en phase 1 ont été testées auprès du panel d'entreprises de la phase 2.
- Les entreprises devaient préciser si ces compétences étaient importantes dans l'exercice de leur activité (Pas du tout, plutôt pas ou plutôt, très important) et évaluer le niveau de maîtrise de leurs salariés sur le sujet (aucune ; moyenne/hétérogène ; forte).

Les compétences clés testées : une expertise perfectible

100% ont pu évaluer



- Moins de 75% des entreprises estiment être suffisamment expertes sur l'ensemble des 6 compétences testées ; 64% sur les compétences relatives à la **Cybersécurité**.
- Pour autant, seules les compétences relatives **au respect des procédures et au reporting** sont considérées comme importantes par plus de 80%.

Les compétences clés testées par typologie de services

	Importance					Expertise perçue			Installation et déploiement informatique		Service de sécurité des biens et des personnes		Service en matière de cybersécurité	
	Pas du tout	Plutôt pas	Plutôt	Très important	Cumul important	Aucune	Moyenne ou hétérogène	Forte	Importance	Maitrise %	Importance	Maitrise %	Importance	Maitrise %
Consigner les interventions afin d'assurer une traçabilité auprès du client et de la hiérarchie	6%	3%	21%	69%	90%	2%	24%	74%	94%	72%	93%	79%	93%	72%
Respecter les procédures de travail établies dans le cadre des interventions chez le client	10%	3%	26%	60%	86%	1%	24%	75%	91%	73%	87%	75%	88%	77%
Analyser les risques cybersécurité potentiels afin de sécuriser les systèmes informatiques	44%	4%	16%	35%	51%	2%	34%	64%	56%	62%	73%	82%	86%	68%
Déterminer et prescrire au client des équipements, solutions et procédures pour mise en conformité en matière de cybersécurité.	29%	5%	18%	48%	66%	2%	24%	74%	71%	72%	81%	92%	80%	74%
Argumenter les avantages des solutions cloud en utilisant des connaissances approfondies sur le sujet	36%	13%	27%	23%	50%	1%	36%	63%	60%	62%	80%	83%	65%	67%
Accompagner l'équipe dans la conduite du changement afin de faciliter leur adaptation à de nouvelles pratiques	21%	16%	31%	32%	63%	4%	27%	70%	66%	72%	67%	80%	71%	78%

- Parmi les entreprises qui proposent de l'installation informatique, le diagnostic de sécurité est jugé peu important, la vente des solutions davantage (ce qui tend à montrer que la cybersécurité est d'abord abordée sous l'angle de la fourniture de solutions/matériels plutôt qu'au travers d'une approche conseil).
- Si le sujet du diagnostic est jugé nettement plus important chez les entreprises qui proposent des services/produits en rapport avec la cybersécurité, seules 2/3 d'entre elles s'estiment pleinement compétentes.

Les compétences clés testées par taille et service Cloud

	Ensemble		Solution Cloud		Taille <11		Taille 11 et +	
	Importance	Maitrise %	Importance	Maitrise %	Importance	Maitrise %	Importance	Maitrise %
Consigner les interventions afin d'assurer une traçabilité auprès du client et de la hiérarchie	90%	74%	96%	71%	90%	74%	90%	70%
Respecter les procédures de travail établies dans le cadre des interventions chez le client	86%	75%	91%	73%	87%	76%	87%	65%
Analyser les risques cybersécurité potentiels afin de sécuriser les systèmes informatiques	51%	64%	61%	66%	50%	65%	63%	63%
Déterminer et prescrire au client des équipements, solutions et procédures pour mise en conformité en matière de cybersécurité.	66%	74%	71%	72%	67%	76%	60%	67%
Argumenter les avantages des solutions cloud en utilisant des connaissances approfondies sur le sujet	50%	63%	74%	61%	47%	62%	70%	67%
Accompagner l'équipe dans la conduite du changement afin de faciliter leur adaptation à de nouvelles pratiques	63%	70%	70%	74%	61%	71%	77%	61%

- Seules 61% des entreprises qui proposent des solutions cloud estiment être suffisamment compétentes pour en argumenter la vente.
- L'importance de l'accompagnement managérial semble minorée chez les TPE (les gérants s'estiment souvent compétents et/ou jugent que leurs équipes sont trop petites pour considérer le sujet) alors que chez les plus grandes, les déficits potentiels sont davantage conscientisés.

Les besoins en compétences exprimés à 2 ans

Avez-vous d'autres enjeux de développement de compétences dans les 2 ans à venir en lien avec vos services IT/cybersécurité ?

26% ont exprimé besoins (certaines entreprises considèrent qu'elles se forment en permanence avec des partenaires/fournisseurs ce qui limite leurs besoins)

Compétences techniques : 65%

- **33% en majeur, développer des compétences en cybersécurité** (certification, protection ses réseaux, test d'intrusion (CTPS), pare-feu, intégration de logiciel SIEM*)
- **12% développement de compétences en administration réseau/sécurité réseau** (NGFW PALOALTO ; NAS SYNOLOGY; certification CCNA (Cisco), certification Veeam (VMCA) ; EDR et XDR)
- **En mineur :** compétences cloud Microsoft 365 ; IA (développement logiciel métier médical notamment) ; réparation de matériel dont téléphone (microsoudure, changement composant/écran) ; infogérance ; téléphonie

Compétences commerciales : 44%

- **12% : technique de vente/négociation pour des profils techniques** dans une logique de polyvalence
- **8% : conseil et prévention/sensibilisation en matière de cybersécurité**
- **8% : recrutement de commerciaux** pour vendre les nouvelles solutions (cybersécurité, téléphonie)
- En mineur : développer une expertise technique en matière d'IA, de numérisation ; Cloud ; de téléphonique ; RGPD

Domaine management : 12%

- **10% : professionnaliser l'approche managériale :** animation du collectif ; gestion multigénérationnelle ; conduite du changement
- Autres : gestion d'entreprise ; pilotage de projet complexe

*logiciel de reporting des menaces de sécurité

Les enjeux à 2-5 ans : la cybersécurité

Quels seront les enjeux pour les entreprises en matière d'IT dans les prochaines années ?

51% des entreprises ont identifiés des enjeux

53% : développer l'activité de cybersécurité (proposer des packs simplifiés pour les PME/TPE ; acculturer le grand public et les entreprises aux enjeux de la cybersécurité ; mettre en place des formations/sensibilisations auprès utilisateurs)

24% : développement de l'IA, notamment dans les activités prédictives (maintenance, cybersécurité)

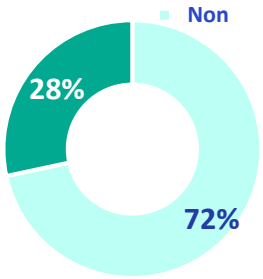
12% : sensibilisation et accompagnement des entreprises à aller plus loin en matière de digitalisation/dématérialisation (ex : factures électroniques)

En mineur (<10%) développement du Cloud + développement de solutions alternatives (satellite/hertzien) ; développement des pratiques numériques responsables (à faible énergie).

- Si la cybersécurité n'est pas un sujet encore d'actualité pour une moitié des entreprises, son importance et son développement dans les années à venir ne fait pas débat, notamment en matière de formation/sensibilisation des utilisateurs et entreprises.
- Au-delà de l'IA dont les contours semblent encore flous, la dématérialisation reste un enjeu.

Recrutements envisagés pour 2025/2026

Anticipez-vous des recrutements pour 2025/2026 en rapport avec vos activités IT ?



1,4 recrutement en moyenne par entreprise qui anticipe une action

- 28% des entreprises anticipent au moins un recrutement, 1,4 en moyenne.
- Les 2/3 des recrutements concerneront des profils techniques, en majorité des techniciens de maintenance de niveau 5, avec 2 ans d'expérience (certaines évoquent une spécialisation en Cybersécurité).

Répartition des recrutements envisagés par métier		Nb moyen	Diplôme souhaité en majorité	Expérience souhaitée
Technicien de maintenance Informatique	41%	1,1	5 (BTS)	>2ANS POSTE SIMILAIRE
Technico-commercial	22%	1,0	5 (BTS)	>2ANS POSTE SIMILAIRE
Administrateur de Réseaux Informatiques	13%	1,3	6 (LICENCE)	>2ANS POSTE SIMILAIRE >5ANS POSTE SIMILAIRE
Intégrateur informatique	6%	1	6 (LICENCE)	>5ANS POSTE SIMILAIRE
Ingénieur réseaux-sécurité	4%	1	6 et 7	>2ANS POSTE SIMILAIRE
Responsable technique	1%	1	NC	nc
Ingénieur Services Cloud	1%	1	6 (LICENCE)	>2ANS POSTE SIMILAIRE
Chargé d'affaires numérique /Ingénieur…	1%	1	NC	NC
Autre métier commercial	7%	1	NC	DÉBUTANT
Autre métier technique	1%	1	6 (LICENCE)	>2ANS POSTE SIMILAIRE

En synthèse

Caractéristiques des entreprises et évolutions de leur offre

- Les entreprises qui proposent des services informatiques (a priori 40% de la totalité des entreprises de la branche) proposent a minima de la maintenance informatique ou de l'installation.
- La moitié d'entre elles n'accompagne que des entreprises de moins de 50 salariés quand 18% proposent leur service à des entreprises de plus de 200 salariés.
- Près de la moitié propose des services en rapports avec la Cybersécurité ; 39% ont fait évoluer leur offre ces dernières années : en majorité de la vente de solutions d'antivirus/firewall/sécurité réseaux/protection boîtes emails/système de sauvegarde/système d'authentification. Le diagnostic de sécurité/conseil, les services de test de phishing/intrusion ou la formation semblent plus marginales.
- Dans ce contexte, seules 20% des entreprises estiment connaître la NIS-2 (dont 6% avec une bonne connaissance) ; 32% parmi les entreprises qui proposent des services en rapport avec la Cybersécurité. Un enjeu d'adaptation de l'offre limité (10%) dans un contexte où les entreprises clientes sont souvent réticences et pas toujours concernées.
- Par ailleurs, 61% des entreprises installent des serveurs en cloud, en complément de solutions physiques. Un développement de l'offre pour 36% des entreprises compte tenu de l'augmentation de la demande.

Besoins en compétences et enjeux à 5 ans

- Seules 64% des entreprises estiment posséder des compétences fortes en matière d'analyse de risque cybersécurité ; 68% parmi les entreprises qui proposent des services en la matière. En complément, on notera que la cybersécurité constitue le premier besoin en matière de compétence technique. Pour autant 50% des entreprises estiment que l'analyse de risque cybersécurité n'est pas importante dans le cadre de leur activité ➔un enjeu identifié comme majeur mais dans une perspective à 2-5 ans.
- Seules 61% des entreprises qui proposent des solutions cloud estiment être suffisamment compétentes pour en argumenter la vente. Au-delà de ce constat le sujet ressort peu en matière de besoins en compétences (offre de formation déjà complète) et n'est pas forcément envisagé comme une solution pérenne.
- Si l'IA est également identifiée comme un enjeu, les contours en restent flous au-delà de la maintenance prédictive ou pour servir la cybersécurité.

Approfondissements en lien avec le Cloud

Rappel hypothèse d'approfondissement Cloud

Les solutions cloud, en développement mais avec des besoins en compétences qui restent limités :

- 61% des entreprises installent des serveurs en cloud, en complément de solutions physiques.
- Un développement de l'offre pour 36% des entreprises compte tenu de l'augmentation de la demande.
- Seules 61% des entreprises qui proposent des solutions cloud estiment être suffisamment compétentes pour en argumenter la vente.
- Au-delà de ce constat le sujet ressort peu en matière de besoins en compétences (offre de formation déjà complète) et n'est pas forcément envisagé comme une solution pérenne.

➔Intérêt de proposer un module de formation sur le sujet pour des profils commerciaux ?

Dans ce cadre, il a été décidé de vérifier la consistance de l'offre de formation sur le sujet

Etude de l'offre de formation à l'usage de commerciaux pour le cloud

- Une offre de formation à l'usage des commerciaux pour valoriser et vendre des solutions cloud devraient intégrer :
  - Des compétences commerciales solides, incluant la capacité à structurer un argumentaire et à gérer des objections.
  - Une compréhension des bénéfices concrets et différenciés des solutions cloud (SaaS, PaaS, IaaS).
- La majorité des formations disponibles se concentre sur les aspects techniques du cloud computing : architecture, fonctionnement, et applications pratiques.
- Ces formations sont principalement adaptées aux professionnels techniques (architectes cloud, ingénieurs système, etc.) et moins aux profils technico-commerciaux.
  - 5 formations recensées au RNCP. Exemples : Expert cloud computing (MS) ; Coordinateur de projets informatiques (infrastructures cloud, applicatives ou data) ; Expert en systèmes d'information sécurisés (Cloud ou Big Data)
  - 22 formations recensées au Répertoire Spécifique : Le développement dans le cloud avec IBM Bluemix ; Administrer les services Cloud Microsoft Azure ; IBM Certified Integration Professional - MobileFirst Protect Cloud Extender and Enterprise Gateway ; Concepteur de Solution Cloud Computing
  - 267 formations recensées au Réseau des Carif-Oref (hors RS ou RNCP).. Exemples : Expert Cloud DevOps ; BUT spécialité réseaux & télécommunications parcours développement système et cloud ; Expert en architecture des systèmes d'information - mastère expert cloud, sécurité & infrastructure.
- L'offre de formation ciblant cette approche commerciale apparait restreinte, 6 formations ont été recensées :
  1. Formation : Cloud Computing, solutions techniques (ORSYS) : *découverte des principes clés et des principales offres cloud*
  2. Formation Vente du SaaS à l'international (Route To Business) : *méthodologie de différenciation dans un contexte international*
  3. Formation à la vente de solutions Cloud (cloud42) : *formation très opérationnelle vente/argumentation et devis/négociation*
  4. Cours de formation à la vente de SaaS (klozers) : *atelier d'une journée consacrée à la vente de Saas*
  5. Vendre le Cloud OUTSCALE (m2iformation) : *découvertes des solutions cloud Outscale de l'éditeur Dassault Systèmes*
  6. Décryptez le Cloud : marché, applications et cas d'usages (institut.capgemini) ; *découverte du cloud et clés pour construire une offre*

Etude de l'offre de formation à l'usage de commerciaux pour le cloud

Ainsi, il pourrait être pertinent de développer un module de formation (ou lancer un appel à projets pour intégrer 1 des 6 formations existantes sur Click&Form ?)

Public cible :

- Commerciaux en charge de la vente de solutions cloud, tous niveaux d'expérience.
- Responsables commerciaux et prescripteurs de solutions cloud.

Première hypothèse de modules de formation:

- Comprendre les fondamentaux du Cloud Computing : acquérir une vue d'ensemble des solutions cloud (SaaS, PaaS, IaaS) et des différents fournisseurs du marché (AWS, Microsoft Azure, Google Cloud, etc.). Positionner les solutions cloud dans différents contextes commerciaux.
- Argumentaire commercial : apprendre à structurer et à présenter un argumentaire commercial pour convaincre les clients des bénéfices des solutions cloud adaptées à leurs besoins.
- Identification des besoins clients : savoir identifier les besoins spécifiques des clients et leur proposer des solutions cloud sur mesure.
- Maîtriser les avantages du cloud : acquérir une compréhension des avantages concrets que le cloud peut apporter à l'entreprise : réduction de coûts, agilité, sécurité, etc.
- Techniques de négociation et de vente : intégrer les aspects commerciaux de la vente cloud : les techniques de négociation et de gestion des objections...

Approfondissements en lien avec la cybersécurité

Principaux enseignements et hypothèses d'approfondissement

Enseignements relatifs à la cybersécurité :

- **Les services en rapport avec la cybersécurité sont en développement mais plus sous forme de vente de solutions que de conseil.** Près de la moitié propose des services en rapports avec la Cybersécurité ; 39% ont fait évoluer leur offre ces dernières années : en majorité de la vente de solutions d'antivirus/firewall/sécurité réseaux/protection boîtes emails/système de sauvegarde/système d'authentification. Le diagnostic de sécurité/conseil, les services de test de phishing/intrusion ou la formation semblent plus marginales.
- **La NIS-2 est méconnue avec peu d'enjeux identifiés à ce stade en partie parce les entreprises clientes ne sont pas considérées comme suffisamment matures sur le sujet**. Seules 20% des entreprises estiment connaître la NIS-2 (dont 6% avec une bonne connaissance) ; 32% parmi les entreprises qui proposent des services en rapport avec la Cybersécurité. Un enjeu d'adaptation de l'offre limité (10%) dans un contexte où les entreprises clientes sont souvent réticences et pas toujours concernées.
- **Si des déficits de compétences sont ressentis en matière de cybersécurité, il s'agit plutôt d'un enjeu à 2-5 ans.** Seules 64% des entreprises estiment posséder des compétences fortes en matière d'analyse de risque cybersécurité ; 68% parmi les entreprises qui proposent des services en la matière. En complément, on notera que la cybersécurité constitue le premier besoin en matière de compétence technique. Pour autant 50% des entreprises estiment que l'analyse de risque cybersécurité n'est pas importante dans le cadre de leur activité ➔un enjeu identifié comme majeur mais dans une perspective à 2-5 ans.

L'enjeu à court terme pour les entreprises, est d'abord de pouvoir sensibiliser leurs clients sur le sujet avant de pouvoir leur proposer un diagnostic. Dans ce cadre, il a été décidé de mener des entretiens d'approfondissement avec des entreprises « les plus matures » qui réalisaient déjà ce travail pour identifier les bonnes pratiques ; les entreprises ciblées par ce type d'action et évaluer le ROI.
➔10 entretiens ont été réalisés auprès de répondants des 2 premières phases.

Les bonnes pratiques relevées

Les types d'actions de sensibilisation menées

- **Dans le cadre des interventions** techniques de maintenance, identification des failles de sécurité et sensibilisation du client ; sensibilisation des utilisateurs au quotidien.
- Dans le cadre des visites commerciales : organisation d'un pré-diagnostic rapide basés sur 8-10 questions pour fixer les priorités ; organisation de mini-formations de 15 minutes auprès des salariés.
- Organisation d'actions de sensibilisation dans le cadre des souscriptions aux assurances (partenariat).

- **Organisation d'évènements** autour de la cybersécurité : participation à des forums, à des salons, à des journées « portes ouvertes » ; organisation de petits déjeuners ; Escape-Game autour des enjeux de cybersécurité.

- **Diffusion de mailing/newsletters** ; communication sur les réseaux sociaux (ex : partage de bonnes pratiques sur LinkedIn) ➔peut représenter 50% des communications des entreprises.

Un niveau de résistance des clients tend à baisser compte tenu notamment du nombre d'attaques constatées dans leur environnement et de la maturité de certaines cibles (ex : institutions publiques type hôpitaux ; entreprises qui répondent à des appels d'offres où la sécurité informatique peut être un critère).

Une résistance qui est en partie liée :

- à l'aspect peu concret du sujet (un enjeu de comportement/process et pas uniquement un investissement matériel)
- au coût perçu/à la perte de productivité : temps passé à respecter les process (ex : identification de l'utilisateur, changements mot de passe)
- au sentiment de ne pas constituer une cible (en particulier chez les petites entreprises) ➔un travail de pédagogie de long terme ; également auprès des utilisateurs

Les bonnes pratiques relevées

Les bonnes pratiques en matière de sensibilisation

Dans le contenu :

- Description des risques (financiers, psychosociaux notamment pour les salariés responsables de l'intrusion) ;
- Explication des typologies d'attaques avec chiffres associés (ex : phishing =30%) ; explication des points d'entrée.
- Présentation d'études de cas anonymes par typologie d'entreprise (PME, TPE, …) auprès des entreprises de mêmes caractéristiques.
- Démonstration des attaques à partir d'outils élaborés par l'entreprise (ex : plateforme de phishing à partir d'un formulaire, ou d'un malware ; envoi d'un email pour récupérer les identifiants) ➔permet de mieux expliquer la mécanique d'une attaque, de faire la démonstration de l'impact concret à partir de sujets accessibles pour acculturer les entreprises et les utilisateurs au sujet.
- Relai des communications officielles « CYBERMOI » de l'ANSSI ; cybermalveillance.gouv ; document de la Confédération PME « Que faire en cas de cyberattaque » ; communication de EBEN ➔un point d'attention particulier à la qualité de l'information tant la communication en matière de cybersécurité peut être fournie et erronée.
- Actions de communication/sensibilisation « à chaud » juste après qu'une attaque ait été constatée ➔ relai auprès des clients sur le cas pratique, la vulnérabilité qui a été exploité, les moyens à mettre en œuvre pour l'éviter de manière très concrète.
- Présentation des risques concrets en lien avec l'activité de l'entreprise (explication de l'impact d'une attaque sur tous les outils digitaux ; sur l'éco système de l'entreprise dont ses clients).

Dans la différenciation selon les cibles :

- Actions de communication/sensibilisation ciblées sur des technologies/risques spécifiques avec un travail de ciblage auprès des clients concernés (via CRM)
- Approche différenciée entre salariés (centrée sur les bons usages ; ex : mots de passe) et chefs entreprises où la cybersécurité est abordée sous l'angle du « management de la sécurité » (dans ce cadre le travail du dirigeant est de mener fréquemment des actions de sensibilisation en interne, créer des chartes informatique/process, …)

Un travail de sensibilisation qui consiste à rendre le sujet le plus concret et le plus accessible possible ; d'autant qu'il constitue un sujet « à la mode » où les fausses informations/promesses peuvent être fréquentes. Dans ce cadre, la NIS-2 est jugée à ce stade trop complexe et pas assez stabilisée (attente décrets) ; une frange ne connait pas le sujet.

Les enjeux et les évolutions anticipées

Evolutions de l'offre en cours/anticipées

Un enjeu de « marketing » de l'offre :

- Développement de packages intégrés. Exemple : solution pour 10-20 postes avec coût mensuel où la cybersécurité est intégrée sans que cela soit particulièrement valorisée + scission du marché en 2 : offre simple et packagée d'un côté ; de l'autre, une offre sur mesure intégrant de la gestion de projet.
- Développement de diagnostics de 3 niveaux selon les enjeux de l'entreprise avec une articulation de différents partenaires en fonction de la profondeur de la demande.
- En cours de formalisation avec une articulation autour de l'assurance cybersécurité, la création de fiches produits.
- Passage de certification/label pour démontrer la capacité à faire

Une offre qui va évoluer en fonction des nouvelles technologies

- Attente d'évolutions technologiques assistées par l'IA pour faciliter l'usage de la sécurité par l'utilisateur (reconnaissance automatique) ; NPU (Neural Processing Unit)
- Evolution naturelle en fonction des évolutions technologiques.

La formation des équipes

Des formations surtout réalisées en interne

- Opération de test phishing auprès des collaborateurs avec formation automatique en cas de mauvaise réponse ➔ mais pas de suivi et pas formalisé, besoin éventuel ; via assureur.
- Formation RGPD/cyber réalisée par un membre de l'équipe et relayée en interne.
- Formation label Cyber (de l'ANSSI) pour être référencé « cybermalveillance.gouv »
- Création d'une école « cyber-univers-it » consacrée aux métiers de services numériques (alternance)

Quelques attentes exprimées en matière de formations

- Utilisation des formations cyber Click&Form mais l'attente de formations plus techniques.
- Formations bloquées en externe car les certifications les plus reconnues (américaines) ne sont pas prises en charge (ex : certification OSCP ; INE)
- Certains ont abandonné la formation de leur client car la certification Qualiopi implique trop d'administratif et n'est pas jugé rentable.

A ce stade, la NIS-2 apparait encore éloignée des préoccupations de la plupart des entreprises. 2 entreprises relèvent un enjeux business fort dans les années à venir (avec DORA : Digital Operational Resilience Act).

Bonnes pratiques et compétences mobilisées

Résumé des bonnes pratiques relevées

- Sensibiliser les clients et utilisateurs lors d'interventions ou d'évènements sur les types de risques (financiers, psychosociaux) ; les types d'attaques avec des chiffres associés ; les points de vulnérabilité, en particulier liés aux utilisateurs ; les conséquences d'une attaque sur son activité et son écosystème (dont ses propres clients).
- Créer des outils des sensibilisation ludiques et pédagogiques (ex : Escape-Game).
- Consolider et présenter des études de cas concrètes basées sur l'expérience de leur client, spécifiques au profil des clients et qui explique de manière pratiques, la vulnérabilité exploitée et les moyens à mettre en œuvre.
- Elaborer et présenter des outils de démonstration qui reproduisent des cas de cyber attaque de façon à mieux sensibiliser les entreprises et les utilisateurs.
- Consolider et relayer des communications fiables/officielles relatives à la Cybersécurité de façon à sensibiliser les clients et palier les communications erronées qui peuvent être diffusées.

Compétences mobilisées

- Identifier les besoins spécifiques en sensibilisation selon les profils clients (grands comptes, TPE…).
- Analyser les différents types d'attaques numériques (phishing, ransomware…) et les risques associés (fraudes, pertes financières, atteinte à l'image) ainsi que les points de vulnérabilité des systèmes et des utilisateurs.
- Assurer une veille sur les statistiques actualisées des cybermenaces et leur impact sur les entreprises, ainsi que sur les communications fiables et officielles en cybersécurité, et sélectionner les informations pertinentes à diffuser.
- Collecter et analyser les retours d'expérience clients pour identifier des cas de cyberattaque pertinents.
- Concevoir des supports de sensibilisation adaptés et ludiques, comprenant des présentations pratiques basées sur des scénarios réels de cyberattaques.
- Animer des interventions pédagogiques et vulgarisées de sensibilisation auprès de différents profils d'audience.
- Élaborer des outils de démonstration en sélectionnant les scénarios d'attaque et en utilisant des outils de simulation et de présentation adaptés.
- Présenter les mécanismes d'attaque et les solutions de protection associées en les illustrant par des démonstrations pratiques.