Etude de cas n°3

L'entreprise 3 a pour activité le conseil aux entreprises et la formation. L'effectif est de 200 personnes. Son activité est lié au numérique, tout le personnel a un poste informatique, le réseau internet est accessible au publique extérieur librement. Ils disposent d'un site interne hébergé chez un prestataire informatique.

L'entreprise souhaite manager la protection du risque numérique et pour ce faire elle met en œuvre la démarche de prévention et d'anticipation du risque numérique. Le dirigeant a dans un premier temps situé le niveau de maîtrise du risque numérique de l'entreprise. Dans un second temps il a invité les salariés à situer à leur tour leur niveau de maîtrise.

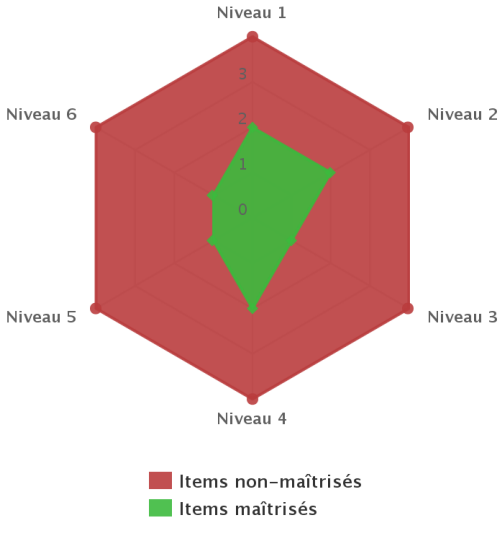
Le dirigeant s'est fixé pour objectifs :

- d'améliorer la préoccupation de l'entreprise pour la protection du risque numérique (niveau 1),
- de faire en sorte que les actions de protection ne restent pas le fruit d'initiatives individuelles (niveau 2),
- de décider avec la direction générale de mettre en place une démarche de protection du système numérique (niveau 3),
- d'impliquer toutes les composantes de l'entreprise dans la maîtrise du risque numérique (niveau 4).

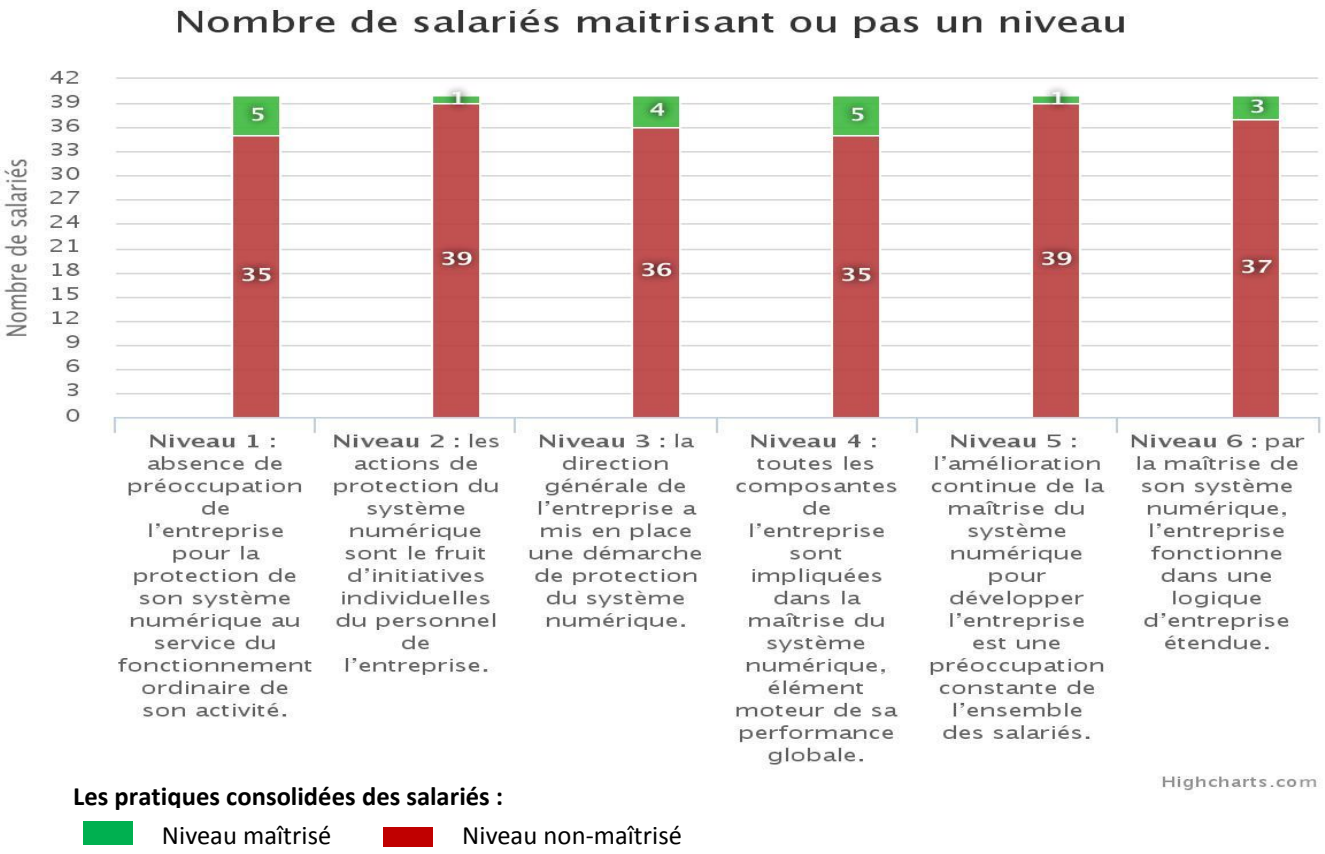
Son but final est que l'amélioration continue de la maîtrise du risque numérique fasse l'objet d'une préoccupation constante de l'ensemble des salariés. (Niveau 5)

Partie I : les résultats :

1- **Les résultats d'ensemble sur chacuns des niveaux du dirigeant et des salariés :**
   a. **Dirigeant :**



b. Salariés :



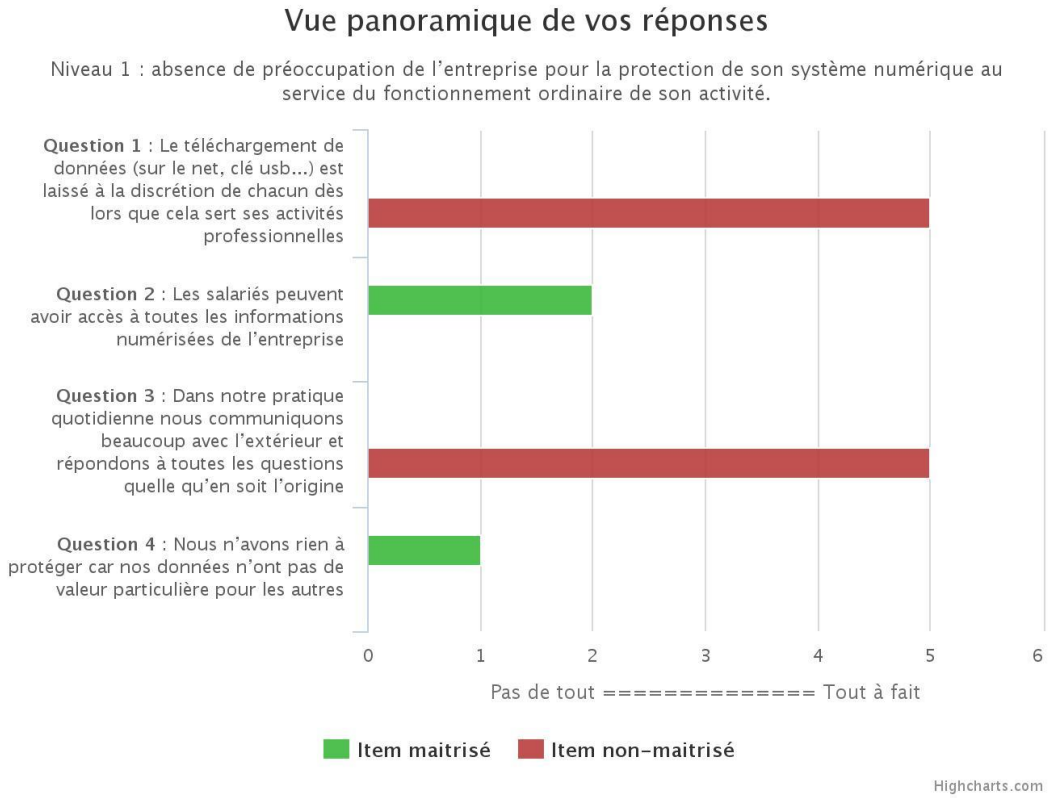
Les pratiques consolidées des salariés :

Niveau maîtrisé Niveau non-maîtrisé

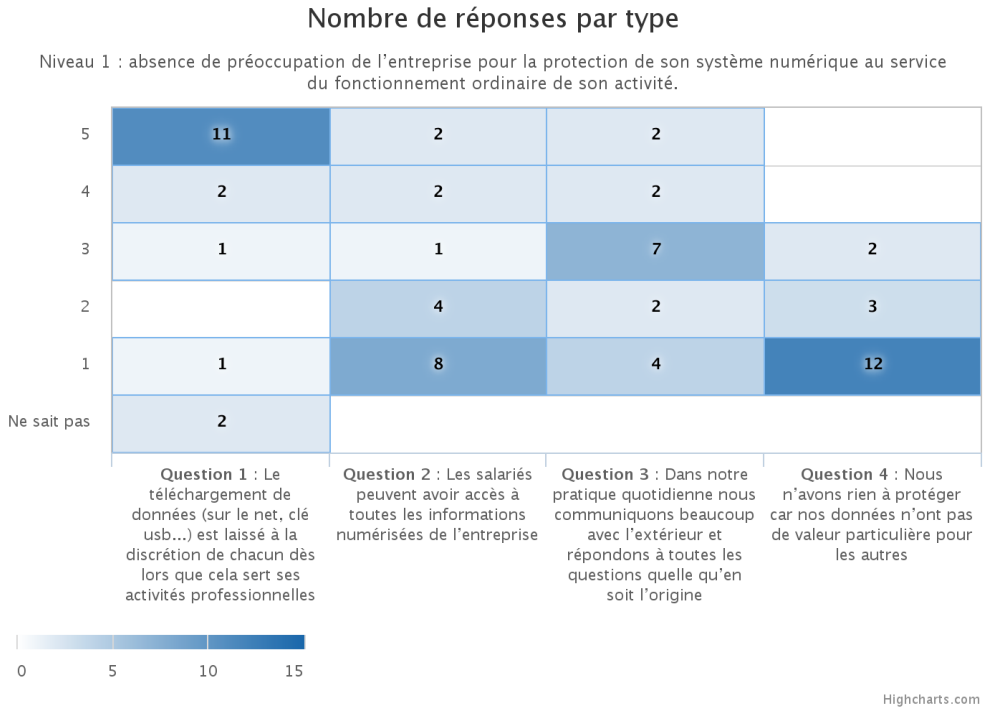
2- Résultats des salariés par niveaux de maîtrise :

a. Niveau 1 : absence de préoccupation de l'entreprise pour la protection de son système numérique au service du fonctionnement ordinaire de son activité

Dirigeant :

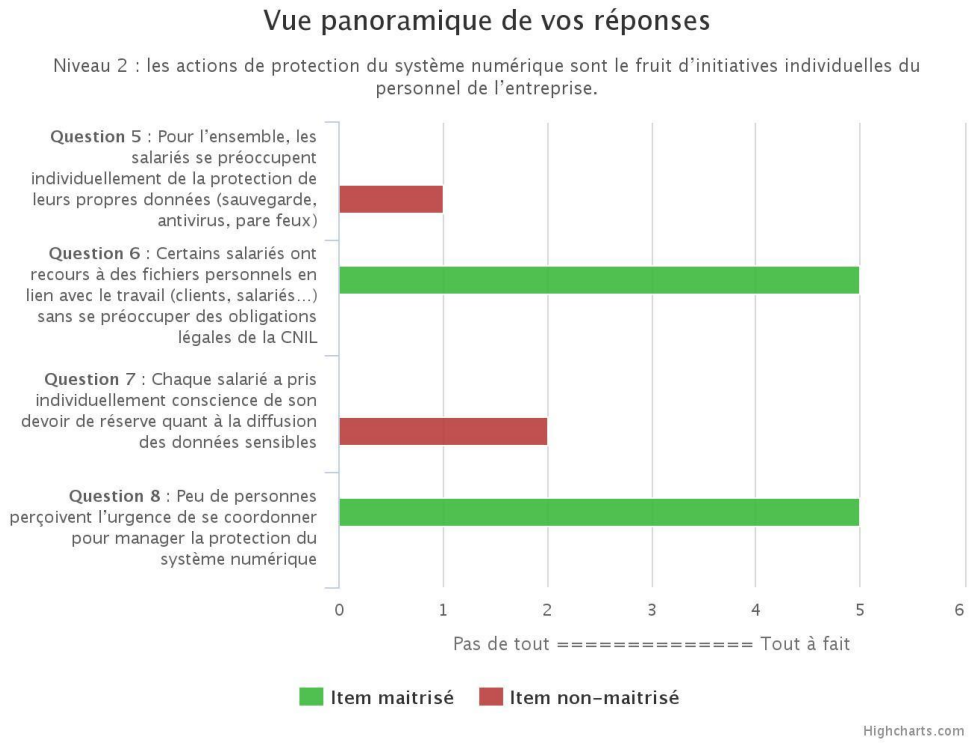


Salariés :

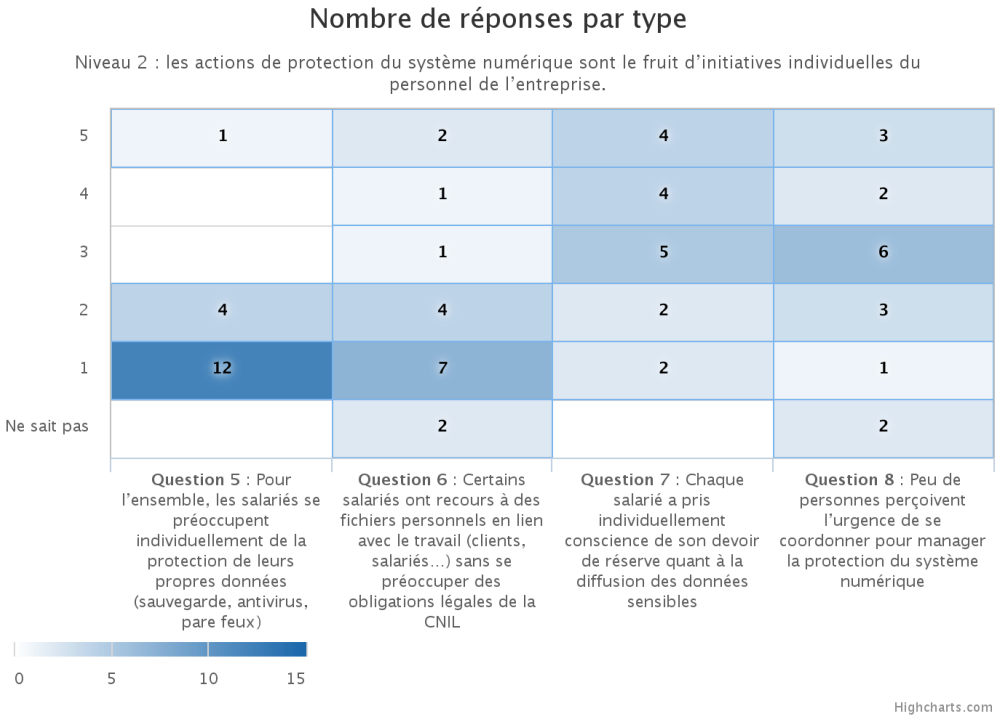


b. Niveau 2 : les actions de protection du système numérique sont le fruit d'initiatives individuelles du personnel de l'entreprise

Dirigeant :

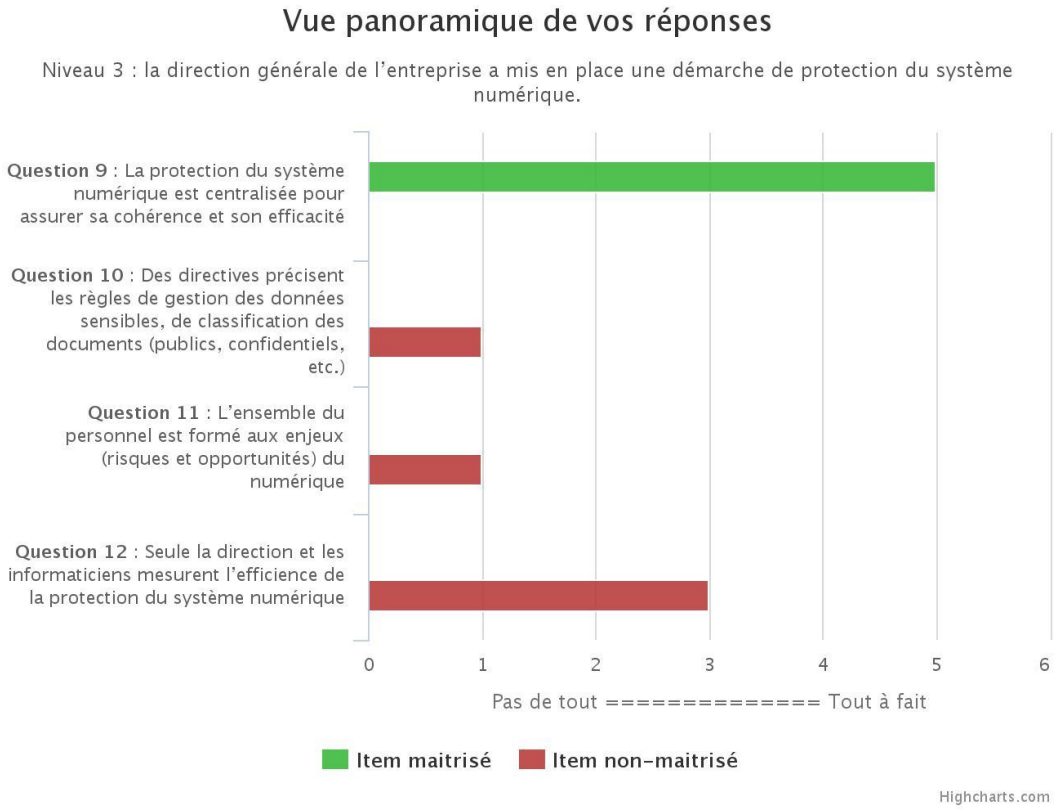


Salariés :

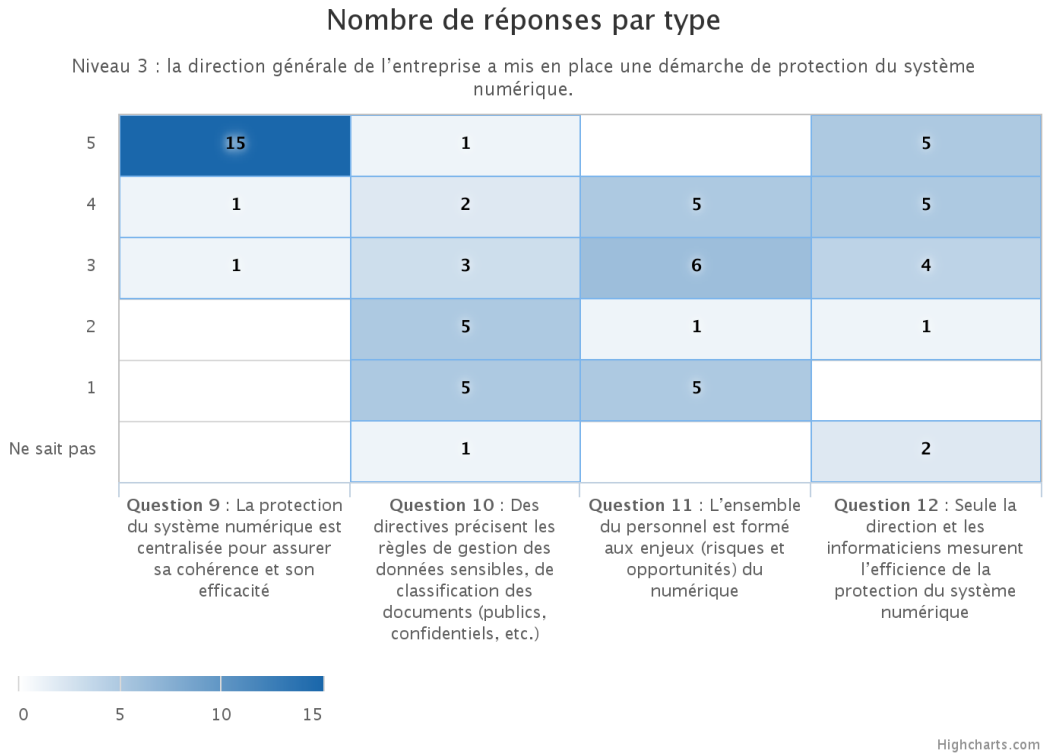


c. Niveau 3 : la direction générale de l'entreprise a mis en place une démarche de protection du système numérique

Dirigeant :

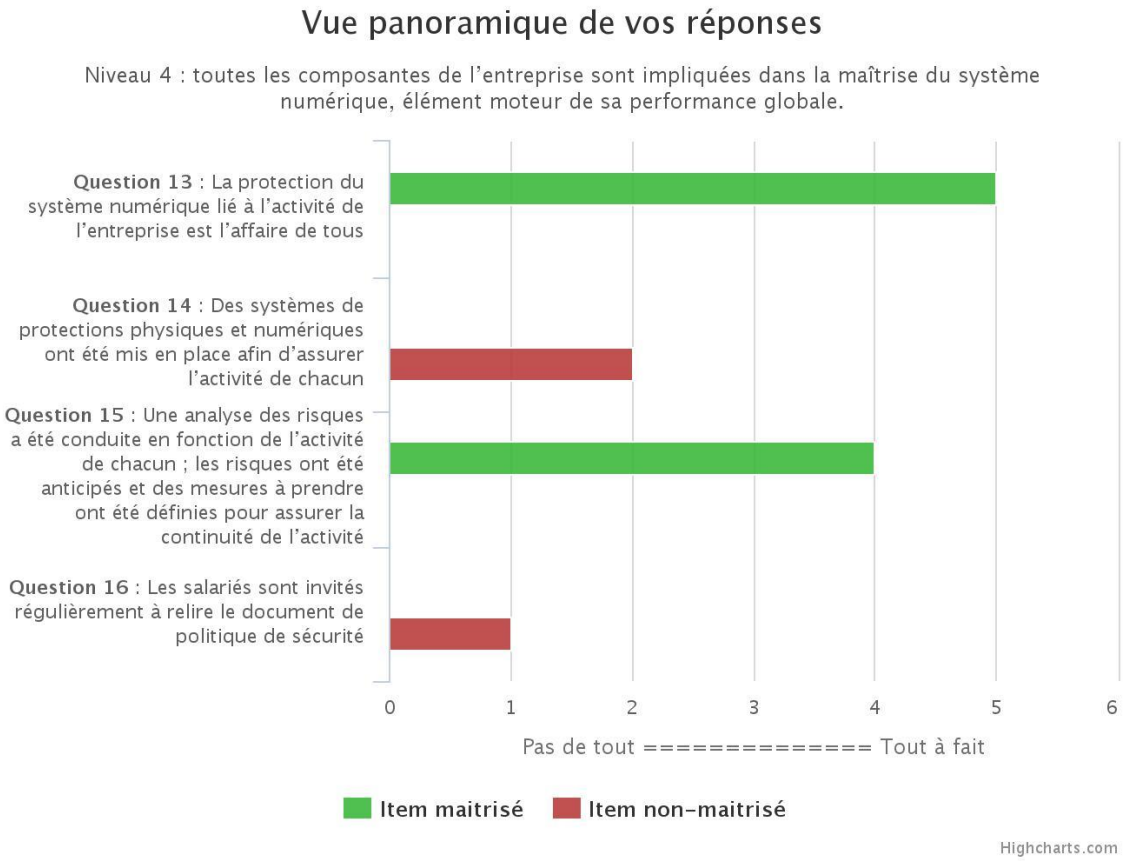


Salariés :

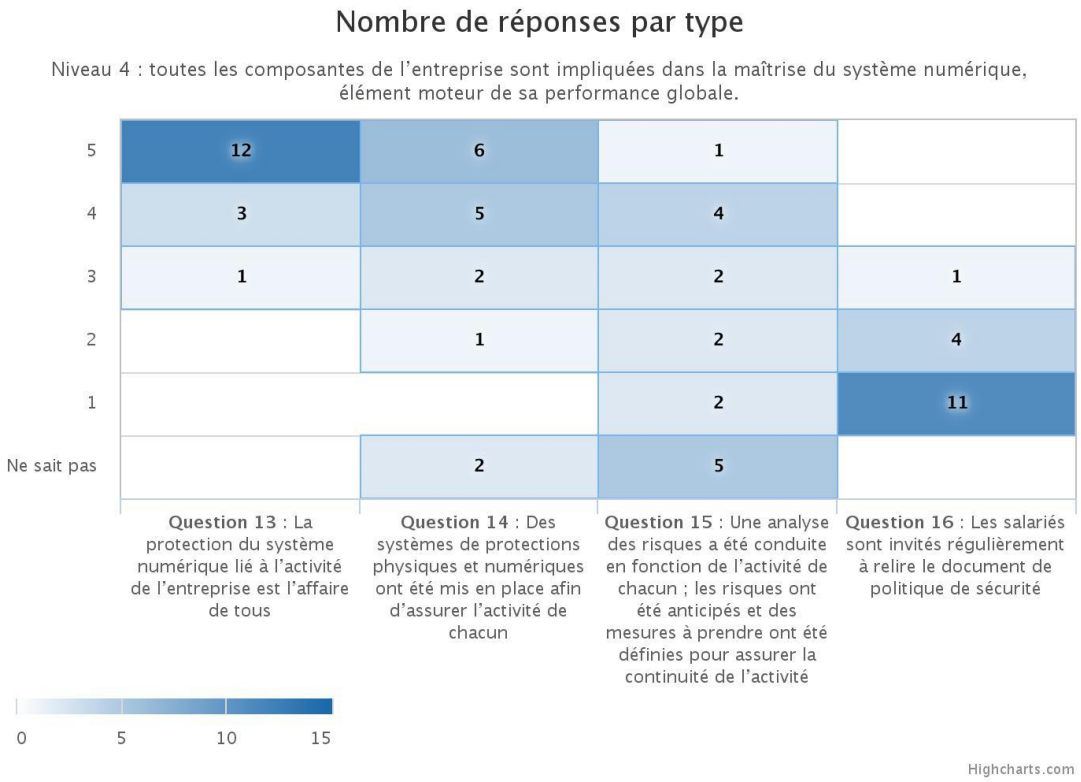


d. Niveau 4 : toutes les composantes de l'entreprise sont impliquées dans la maîtrise du système numérique, élément moteur de sa performance globale

Dirigeant :

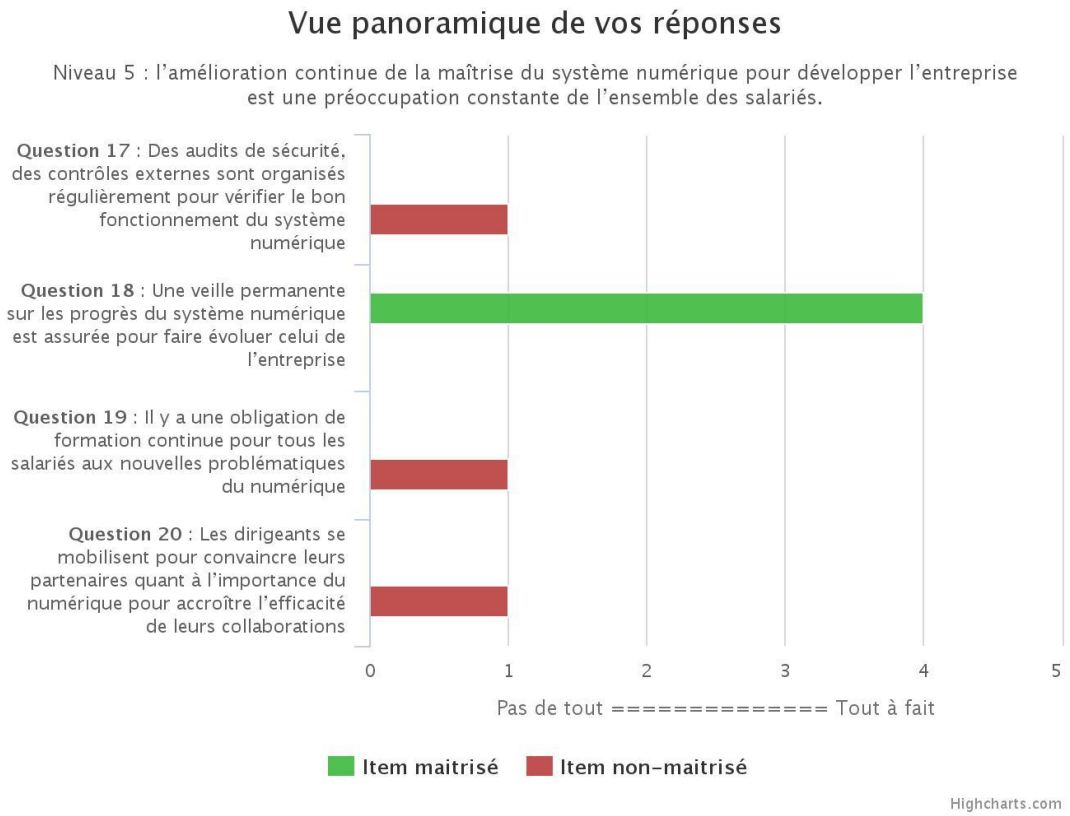


Salariés :

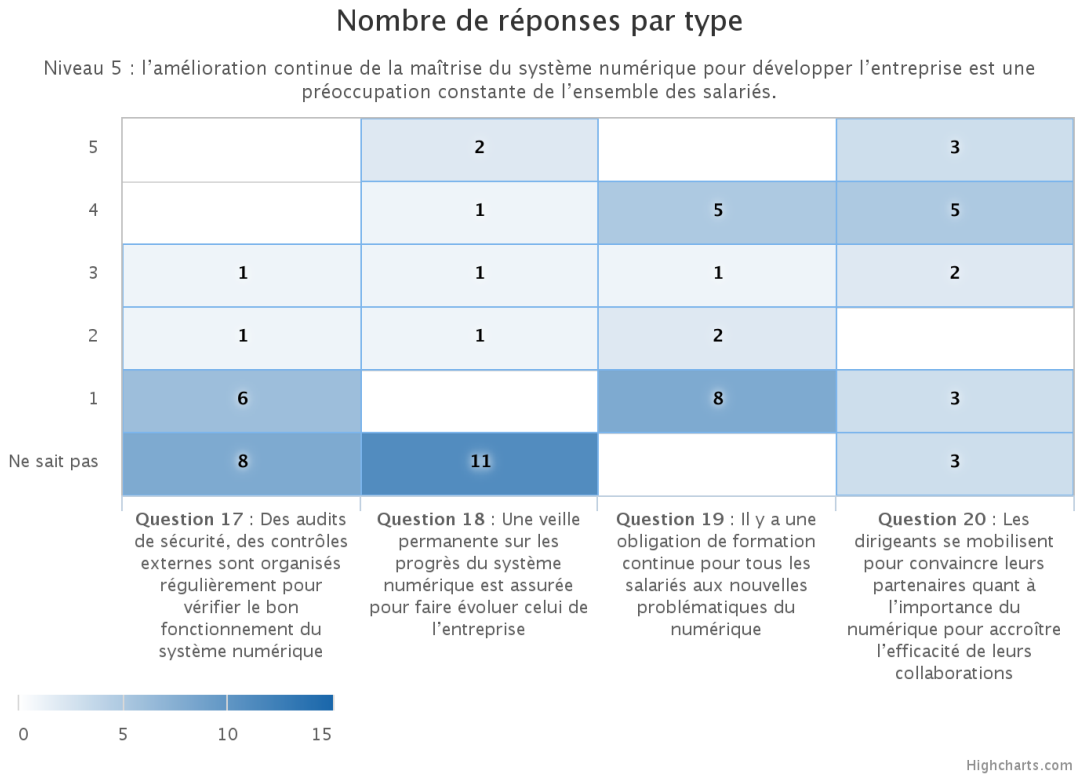


e. Niveau 5 : l'amélioration continue de la maîtrise du système numérique pour développer l'entreprise est une préoccupation constante de l'ensemble des salariés

Dirigeant :

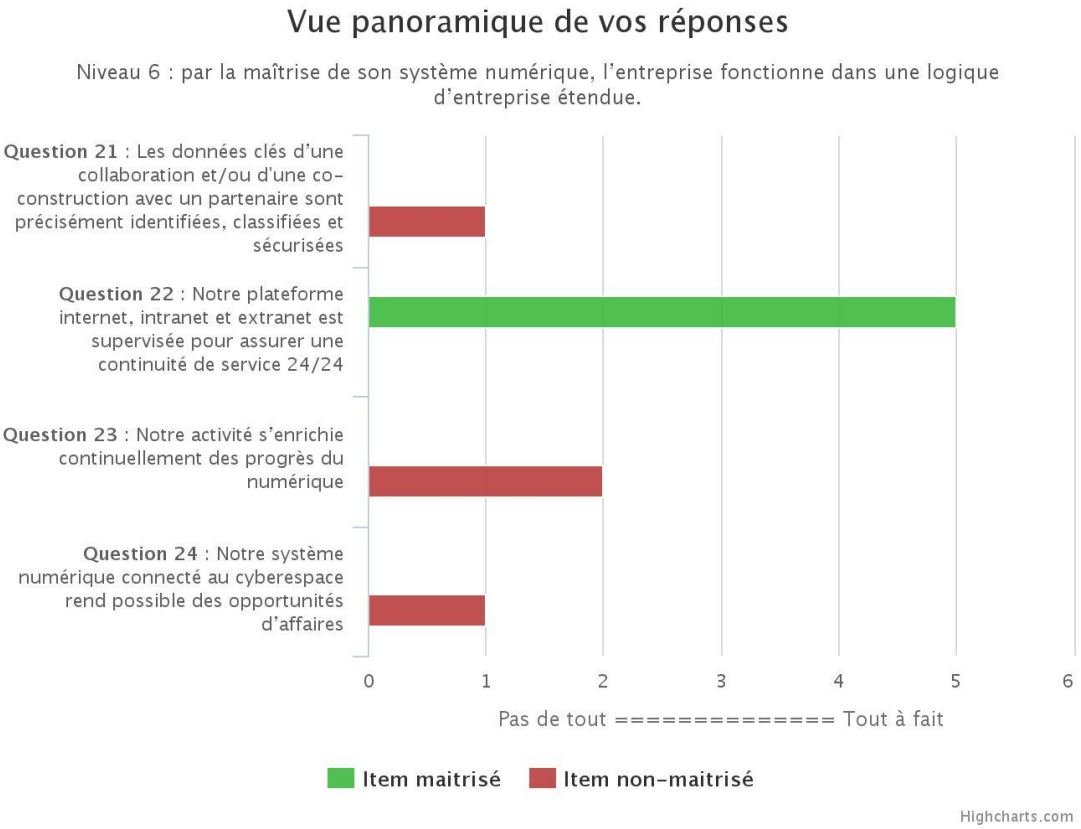


Salariés :

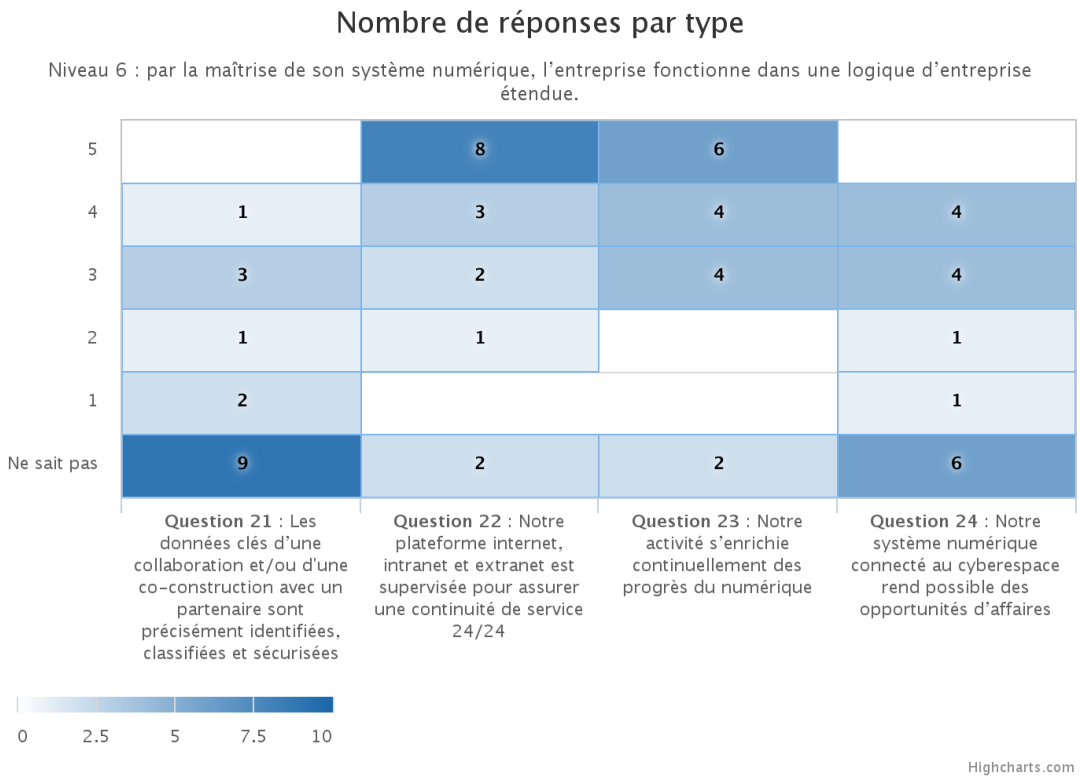


f. Niveau 6 : par la maîtrise de son système numérique, l'entreprise fonctionne dans une logique d'entreprise étendue

Dirigeant :



Salariés :


Nombre de réponses par type
Niveau 6 : par la maîtrise de son système numérique, l'entreprise fonctionne dans une logique d'entreprise étendue.
5
4
3
2
1
Ne sait pas
8
6
1
3
4
4
3
2
4
4
1
1
1
2
1
9
2
2
6
Question 21 : Les données clés d'une collaboration et/ou d'une co-construction avec un partenaire sont précisément identifiées, classifiées et sécurisées
Question 22 : Notre plateforme internet, intranet et extranet est supervisée pour assurer une continuité de service 24/24
Question 23 : Notre activité s'enrichie continuellement des progrès du numérique
Question 24 : Notre système numérique connecté au cyberespace rend possible des opportunités d'affaires
0
2.5
5
7.5
10
Highcharts.com

Partie II : Les conseils d'engagement:

Niveau 1 : Des conseils pour sensibiliser l'entreprise aux enjeux de la sécurité numérique

Pour ne pas rentrer dans le niveau :

- Le management devrait prendre conscience de l'intérêt de sécuriser le système numérique de l'entreprise.

A faire dans 3 mois

- Un/plusieurs responsables en charge de coordonner la politique sécuritaire devrait être désignés et la fonction intégrée dans sa/leur fiche de poste.

A faire dans 3 mois

- Une action de communication sur le lancement de la démarche de sensibilisation devrait être effectuée.

A faire dans 3 mois

- Des priorités d'action avec un planning d'atteinte de chacun des niveaux devraient être établies.

A faire dans 3 mois

Pour dépasser le niveau 1 : Partager l'enjeu de la protection du système numérique au sein de l'entreprise est un premier pas.

- Il faudrait animer avec un expert, une ou plusieurs séance(s) de travail avec l'équipe dirigeante.

A faire dans 3 mois

- Il faudrait préfigurer un plan d'action pour initier une démarche de protection du système numérique.

A faire dans 3 mois

- Il faudrait identifier deux actions spécifiques à mettre en œuvre immédiatement.

A faire dans 3 mois

Niveau 2 : Des conseils pour obtenir une implication individuelle des salariés.

Pour ne pas rentrer dans le niveau:

- L'organisme devrait disposer d'un inventaire exhaustif des comptes internet sensibles et le maintenir à jour.

A faire dans 6 mois

- Les mises à jour des logiciels devraient être effectuées régulièrement mais uniquement à partir des sites de confiance (site de l'éditeur).

A faire dans 3 mois

- L'organisation devrait s'assurer que l'accès au système d'information s'effectue à partir d'un mot de passe unique et robuste propre à chaque utilisateur.

A faire dans 3 mois

- Un pare-feu personnel sur chaque poste client devrait être installé et utilisé.

A faire dans 3 mois

- Il devrait y avoir un anti-virus mis à jour sur chaque poste.

Fait

- Les données sensibles de l'entreprise devraient être sauvegardées périodiquement.

A faire dans 3 mois

- Il faudrait sensibiliser en permanence les utilisateurs aux règles d'hygiène informatique élémentaires.

A faire dans 3 mois

- Chaque nouvel arrivant devrait être informé des règles de sécurité numérique relatives au fonctionnement de l'entreprise.

A faire dans 3 mois

Pour dépasser le niveau 2 : Passer de l'implication individuelle à la prise de conscience collective soutenue par le dirigeant.

- Il faudrait organiser une réunion entre les salariés et l'équipe dirigeante pour partager un état des lieux des incidents rencontrés par le passé et au quotidien.

A faire dans 3 mois

- Il faudrait imaginer des solutions adaptées pour éviter les problèmes les plus fréquents.

A faire dans 3 mois

- Il faudrait mettre en œuvre deux ou trois solutions concrètes.

A faire dans 3 mois

Niveau 3 : Des conseils pour accompagner le dirigeant à s'engager dans une politique de sécurité numérique.

Pour progresser dans le niveau :

- Les procédures d'arrivée et de départ des utilisateurs devraient être écrites et appliquées.

A faire dans 3 mois

- Les utilisateurs devraient être sensibilisés aux bonnes pratiques de stockage et ne pas utiliser les mécanismes automatiques de sauvegarde.

A faire dans 6 mois

- Les services qui ne participent pas directement à la réalisation de l'activité professionnelle devraient être désactivés.

A faire dans 6 mois

- L'exécution automatique des logiciels stockés sur les supports amovibles (clé USB, …) devrait être désactivée.

A faire dans 9 mois

- Les passerelles d'interconnexions avec internet devraient être spécifiées en fonction du niveau d'exigence de l'entreprise.

A faire dans 3 mois

- Il devrait y avoir des procédures claires de destruction ou de recyclage des supports informatiques en fin de vie.
- La sauvegarde des données sensibles devrait être spécifié et automatisé (et ne repose pas sur la bonne volonté des utilisateurs).

A faire dans 6 mois

- Les sauvegardes devraient être vérifiées périodiquement.

A faire dans 3 mois

- Il devrait y avoir des audits de sécurité périodique (minimum annuel).

Pour dépasser le niveau 3 : De la prise de décision du dirigeant à la mise en place d'une démarche engageante de l'ensemble des parties prenantes de l'entreprise.

- Il faudrait associer l'ensemble du personnel pour que la démarche de protection du système numérique soit portée par le collectif à partir de retours d'expérience.

A faire dans 3 mois

- Il faudrait créer une cellule d'animation pour la maîtrise du système numérique.

A faire dans 3 mois

- Il faudrait conduire trois ou quatre chantiers prioritaires et transversaux sur les pratiques de sécurité numérique.

A faire dans 6 mois

- Sur la base de l'expérience il faudrait que l'entreprise rédige et mette à jour périodiquement une charte de sécurité numérique.

A faire dans 9 mois

Niveau 4 : Des conseils pour engager le collectif dans la politique de sécurité numérique.

Pour progresser dans le niveau :

- L'entreprise devrait disposer d'un inventaire qualifié de ses ressources matérielles et logicielles.

A faire dans 3 mois

- La connexion d'équipements personnels au système numérique de l'entreprise devrait faire l'objet de consignes de la part de la direction.

A faire dans 3 mois

- Le BIOS des machines devrait être inaccessible.

A faire dans 6 mois

- Le réseau Wifi devrait être séparé du réseau interne normal d'utilisation courante.

A faire dans 3 mois

- Il ne devrait pas y avoir de possibilité d'accès d'administration sur les systèmes autorisés depuis internet ou sinon via des moyens sécurisés (tunnel, VPN, cryptage).

A faire dans 3 mois

- Il devrait y avoir un cloisonnement physique des réseaux numériques de l'entreprise : ceux connecter sur internet, ceux qui sont indépendants et renfermant des données sensibles.

A faire dans 3 mois

- Une analyse des risques numériques devrait permettre d'établir un plan de continuité de l'activité.

A faire dans 3 mois

- Il devrait y avoir des procédures d'urgence strictement respectées

A faire dans 3 mois

Pour dépasser le niveau 4 : Vers un processus d'amélioration continue du système numérique.

- Il faudrait positionner la politique de maîtrise du système numérique au cœur de la prise de décision de l'entreprise.

A faire dans 9 mois

- Il faudrait décliner, animer et partager la politique de maîtrise du système numérique à tous les niveaux hiérarchiques de l'entreprise.

A faire dans 9 mois

- Il faudrait déployer un plan de formation récurrent pour piloter la sécurité numérique.

A faire dans 9 mois

- Il faudrait identifier des experts externes pour mesurer l'efficience de cette politique d'amélioration continue au service du développement de l'entreprise.

A faire dans 9 mois

Niveau 5 : Des conseils pour organiser le processus d'amélioration continue de la sécurité numérique.

Pour progresser dans le niveau :

- Les points névralgiques de l'architecture réseau devraient être identifiés.

A faire dans 6 mois

- Une supervision des systèmes et réseaux, avec alerte, devrait être mise en place.
- Il faudrait gérer de façon centralisée les obsolescences (les matériels et applications ayant dates de fin de support constructeur et éditeur).

A faire dans 6 mois

- Les authentifications par défaut existant dans les applications, les systèmes d'exploitation et les matériels, à l'origine de leur installation devraient être renouvelées systématiquement.

A faire dans 6 mois

- Les risques de sécurité numérique devraient participer au développement des applications métiers.

A faire dans 9 mois

- Il devrait exister des tableaux de bord pour piloter et communiquer les résultats de la politique de sécurité numérique auprès de l'ensemble des salariés.

Pour dépasser le niveau 5 : De l'amélioration continue du système de sécurité numérique à un fonctionnement en entreprise étendue.

- Il faudrait organiser le pilotage en continue de la protection du système numérique.
- Il faudrait former en continue dans l'action l'ensemble des salariés aux apports du numérique.
- Il faudrait réfléchir à l'activité et la faire évoluer en fonction des apports des technologies numériques notamment en matière de dématérialisation.

- Il faudrait développer des partenariats externes de tous ordres à partir de méthodes collaboratives éprouvées et codifiées, de bases de données multimédias…

Niveau 6 : Des conseils pour fonctionner en entreprises étendue.

Pour progresser dans le niveau :

- Le nomadisme devrait être encouragé et pratiqué au quotidien.
- Travailler en entreprise étendue devrait conduire à la mise en place d'un système d'authentification adapté (carte à puce, PDV, BIO)..
- Travailler en entreprise étendue devrait conduire à durcir (par ajout de composants optionnels de sécurité) la protection des systèmes d'exploitation et de restauration des postes utilisateurs.
- Il faudrait encourager une pratique de travail en dehors de l'entreprise (VPN…)