AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

ÉTUDE SUR LA CYBERSÉCURITÉ DES ÉTABLISSEMENTS DE SANTÉ

12 mars 2026

Etude réalisée par le cabinet occurrence , groupe IFOP

Dans ce rapport d’étude

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

MÉTHODOLOGIE DE L'ÉTUDE ET PROFIL DES RÉPONDANTS

1

Méthodologie de l'étude

Étude quantitative online : terrain réalisé du 16 mai au 30 juin 2025

Échantillon : 719 répondants (directeurs d'établissements de santé)

Le questionnaire : 33 questions dont 12 numériques

Marge d'erreur pour un échantillon de 719 répondants : ± 4 points

Différences significatives : Les différences statistiquement significatives selon le profil (âge, sexe, CSP, taille d'agglo) des répondants sont présentées tout au long du rapport, de la manière suivante :

- xx% (significativement supérieures aux autres)
- xx% (significativement inférieures)

Des tris croisés ont été effectués selon les critères suivant : public/privé, lucratif/non lucratif, ainsi que la capacité d'accueil lorsque cela s'avérait pertinent.

Les tris statistiquement significatifs sont présentés dans le rapport.

Profil des 719 répondants

TYPE D'ETABLISSEMENT

Privé à but lucratif : **33%**

Privé à but non lucratif : **26%**

Public : **41%**

Privé : **59%** / Public : **41%**

Lucratif : **33%** / Non lucratif : **67%**

CAPACITE D'ACCUEIL

Inférieure à 100 lits : **30%**

De 100 à 300 lits : **41%**

De 300 à 1 000 lits : **23%**

Supérieure à 1 000 lits : **6%**

CONNAISSANCE DU PLAN DE PREVENTION

Oui : **87%**

Non : **13%**

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

ENSEIGNEMENTS DE L'ÉTUDE

Près d'1/4 des établissements naviguent à vue en cas de cyberattaque

Prévalence des incidents cyber

- **15 % des établissements de santé** ont été confrontés à un **incident cyber ayant entraîné des perturbations**.
  - Les petits établissements (<100 lits) sont un peu moins touchés : **12 %** déclarent un incident.
  - Pas de différence significative observée selon le type d'établissement (public/privé ; but lucratif/non lucratif).
  - Parmi ces 15% d'établissements de santé ayant subi un incident cyber, **seuls 15 %** estiment avoir été **« bien préparés »** (contre 53% « assez bien préparés », et 32% « insuffisamment préparés »).

Niveau de préparation

- **Parmi les établissements de santé n'ayant pas subi d'incident cyber** dans les 3 dernières années (85% des établissements), **13% seulement estiment être « bien préparés »** (contre 66% « assez bien préparés », et 21% « insuffisamment préparés »).
- **Dans l'ensemble, les établissements de santé privés ou à but lucratif ont tendance à se sentir mieux préparés** que les établissements publics ou à but non lucratif, sans pour autant que l'on constate de différences significatives entre les différents types établissements dans les incidents cyber déclarés plus haut.

Des directeurs d'établissement personnellement impliqués dans la cybersécurité

Gouvernance et implication

- **2/3 des directeurs d'établissement ont eu une réunion récente (<3 mois) avec leur équipe SSI.**
- **87 % ont connaissance du plan de prévention cybersécurité**, et jusqu'à 97% parmi les établissements privés.
- **72 % déclarent intervenir personnellement dans l'élaboration du plan de prévention des risques**, jusqu'à 78% dans les établissements privés.
- **La direction générale** est quasiment systématiquement **impliquée dans les exercices de crise cyber réalisé en 2023/2024 (86%)** ce qui souligne une prise de conscience stratégique de l'enjeu cyber.
- **Près des 2/3 des directeurs d'établissement (63%) considèrent leurs équipes SSI compétentes et autonomes en matière de prévention des risques cyber**, et jusqu'à 75% parmi les établissements de santé à but lucratif.

Continuité et sécurité en ligne de mire

Impacts perçus d'un incident cyber

- **Les directeurs d'établissements estiment que les impacts potentiels sont multiples et significatifs,** de plus fort au plus faible :
  - **Continuité des soins : 4,1/5**
  - **Coût financier : 3,9/5**
  - **Qualité de vie au travail du personnel : 3,8/5**
  - Sécurité des patients : 3,6/5
  - Commande et relations fournisseurs : 3,3/5
  - Réputation : 2,8/5
  - Contentieux et réclamations : 2,6/5

- **86 % des établissements déclarent travailler les impacts identifiés.**
  - Les actions perçues comme les plus accessibles financièrement sont :
    - Formation/sensibilisation du personnel
    - Exercices de crise
    - Actualisation des documents

Des budgets qui peinent à suivre les ambitions

Priorités

- **Loin devant les autres leviers, les directeurs d'établissement priorisent le renforcement technique de la sécurité des SI** (2,1/5 pour ordonnancement de priorité de 1 à 5 ; plus la note est basse, plus l'action est prioritaire).
  - **Les autres leviers proposés suscitent un niveau d'intérêt semblable :**
    - Exercices de crise : 3/5
    - Analyse de risques, plan de continuité et reprise d'activité : 3,2/5
    - Formation / Sensibilisation du personnel : 3,3/5
    - Audits : 3,5/5

Allocations budgétaires

- **La prévention cyber reste cependant marginale dans les budgets informatiques des établissements de santé** :
  - 60% des établissements y consacrent moins de 5% de leur budget d'investissement informatique (CAPEX),
  - 53% des établissements y consacrent moins de 5% de leur budget de fonctionnement informatique annuel (OPEX).

- **42% des directeurs d'établissements déclarent que le budget et les ressources dont ils disposent ne permettent pas d'élaborer un plan de prévention des risques cyber au bon niveau**, c'est davantage le cas parmi les établissements de 300 à 1000 lits (55%), publics (53%) et à but non lucratif (49%).

Face au risque, deux réflexes : l'expert et le matériel

Ressources disponibles

- Les deux **ressources jugées prioritaires en cas d'incident cyber** sont (2 choix maximum) :
  - **L'identification d'experts techniques mobilisables 7j/7 (84%)**
  - **La mise à disposition de matériel informatique et téléphonique pour reprendre l'activité (73%)**
- Loin devant
  - Le recours à une expertise en matière de gestion de crise pour communiquer à bon escient en interne et en externe (31%)
  - Un contact avec un directeur d'établissement ayant connu une cyber attaque (5%)

Partenaires d'appui

- **Les GRADeS / CRRC en tête sur l'accompagnement et la prévention des risques cyber** (61% des directeurs d'établissement déclarent un accompagnement régulier)
  - Suivi par les ARS (55%), l'ANSSI (54%), la CERT Santé (47%)
  - Avec seulement 21 %, les fédérations hospitalières ferment la marche, en particulier dans le public (16 %).
  - Le public est beaucoup plus accompagné par l'ANSSI (+13 pts) et les GRADeS (+11 pts).

La cybersécurité se joue en collectif local

Coopération territoriale

- En termes de coopération territoriale, la **mutualisation des expertises entre établissements d'un même territoire** est **plébiscitée par 9 directeurs sur 10**.
  - Encore plus fortement par les établissements publics (92%) et non lucratifs (94%).
  - La mise à disposition de solutions communes portée par un acteur local souverain et la convergence de solutions informatiques communes à moyen terme sont des pistes retenues par une majorité des directeurs d'établissements (respectivement 58% et 57%).

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

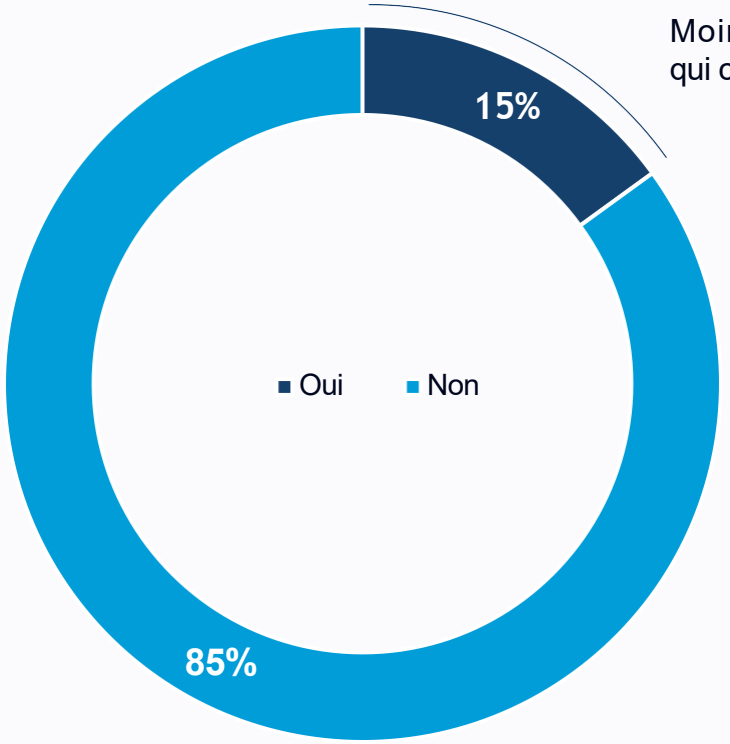
RÉSULTATS DÉTAILLÉS

3

15% des établissements ont rencontré un incident cyber qui a entrainé des perturbations de fonctionnement

Q3. Votre établissement a-t-il fait l'objet d'une perturbation dans son fonctionnement à la suite d'un incident cyber depuis 2022 ?

QCU |Base : 719 répondants



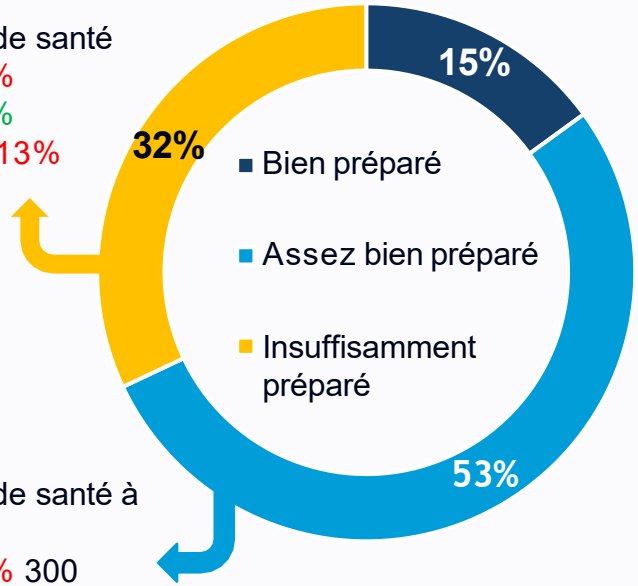
Moins courant dans les établissements qui comptent moins de 100 lits : 12%

Parmi eux, 15% seulement se sentaient « bien préparés » ; et seulement 13% parmi les établissements n'ayant pas rencontré d'incidents

Q4. Si oui, jugiez-vous, avant cet incident cyber, que votre établissement était :

QCU |Base : 111 répondants

Etablissements de santé à but lucratif : 16% / non lucratif : 38%
300 à 1000 lits : 13%

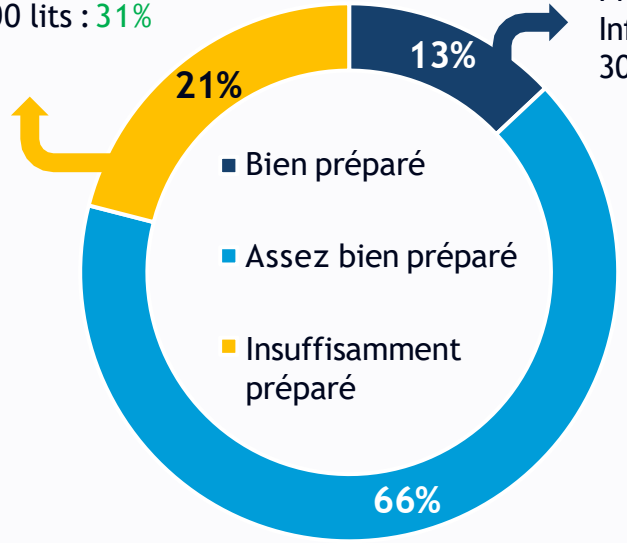


Etablissements de santé à but lucratif : 75% / non lucratif : 44% 300 à 1000 lits : 78%

Q5. Si non, estimez-vous que votre établissement est aujourd'hui :

QCU |Base : 609 répondants

But lucratif : 9% / non lucratif : 27%
Privé : 14% / public : 32%
Inférieur à 100 lits : 13% / 300 à 1000 lits : 31%

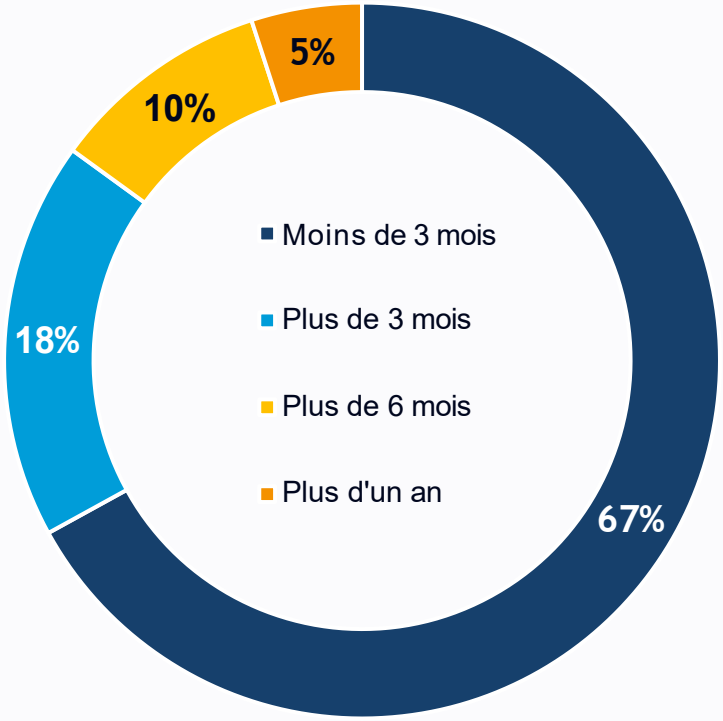


But lucratif : 23% / non lucratif : 8%
Privé : 17% / public : 7%
Inférieur à 100 lits : 20% / 300 à 1000 lits : 7%

Pour 2 chefs d'établissement sur 3 la dernière réunion de travail avec leur équipe SSI remonté à moins de 3 mois

Q6. Votre dernière réunion de travail avec votre équipe SSI (sécurité des systèmes d'information) / référent SSI sur la prévention des risques cyber remonte à :

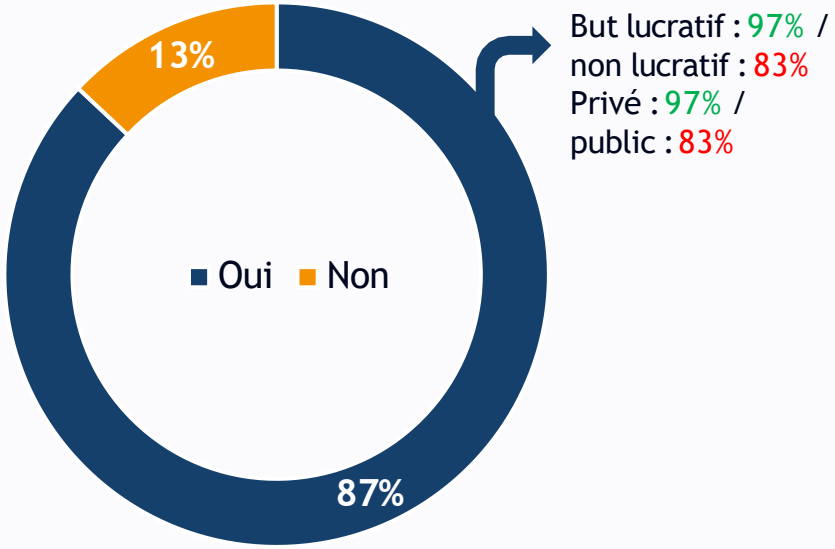
QCU |Base : 719 répondants



87% des directeurs d'établissement ont connaissance du plan de prévention Les ¾ interviennent personnellement dans l'élaboration du plan

Q7. En tant que directeur d'établissement, avez-vous connaissance du plan de prévention des risques cyber de votre établissement ?

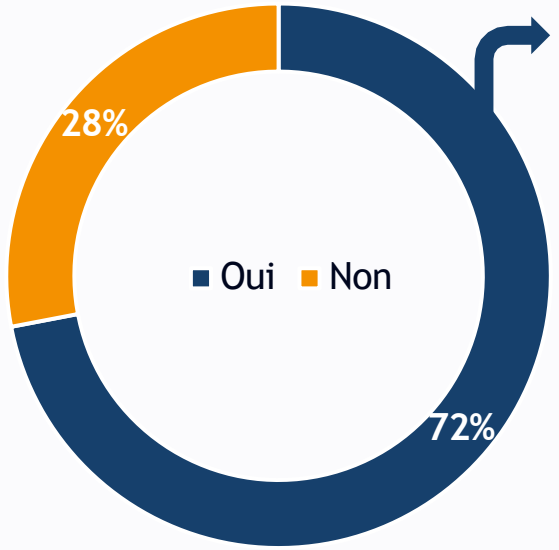
QCU |Base : 719 répondants



But lucratif : 97% / non lucratif : 83%
Privé : 97% / public : 83%

Q8. Si oui, intervenez-vous personnellement dans l'élaboration de ce plan de prévention des risques, notamment dans le volet cyber ?

QCU |Base : 629 répondants

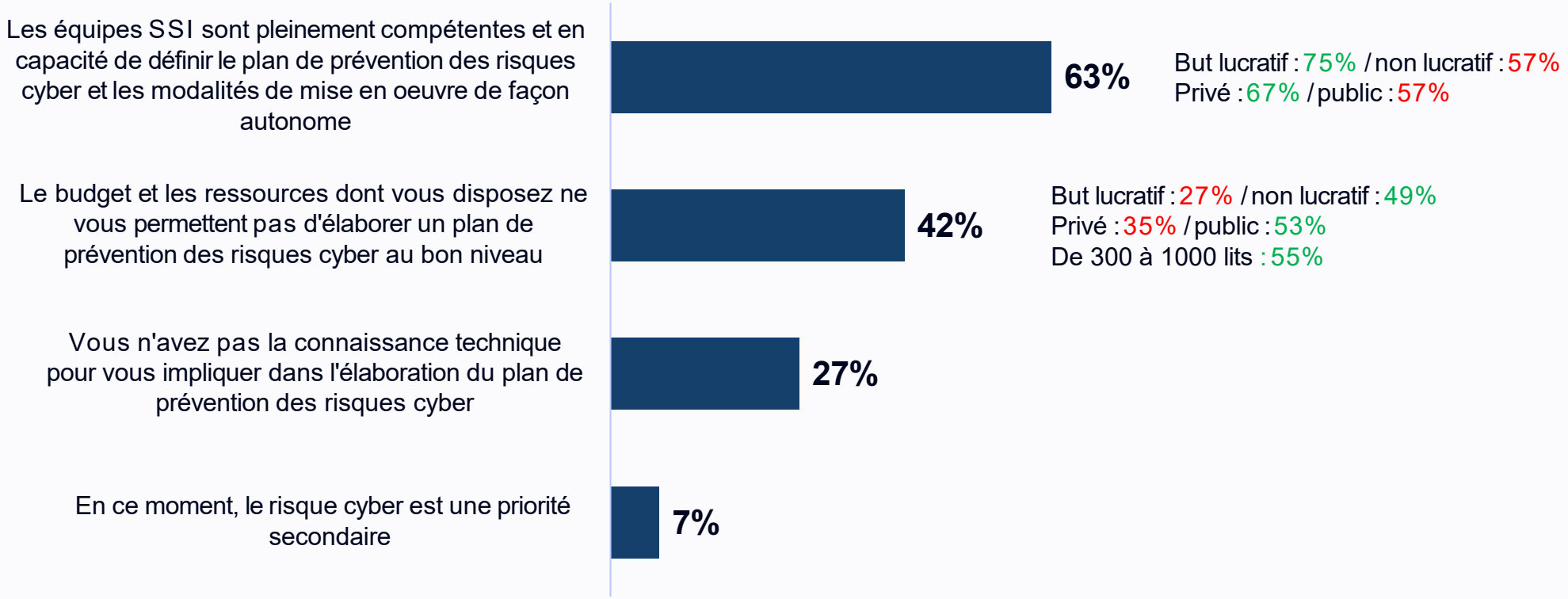


Privé : 78% / public : 62%
Inférieur à 100 lits : 78%

2/3 des directeurs d'établissement considèrent leurs équipes SSI compétentes et autonomes sur le sujet de la prévention des risques

Q9. Considérez-vous principalement que :

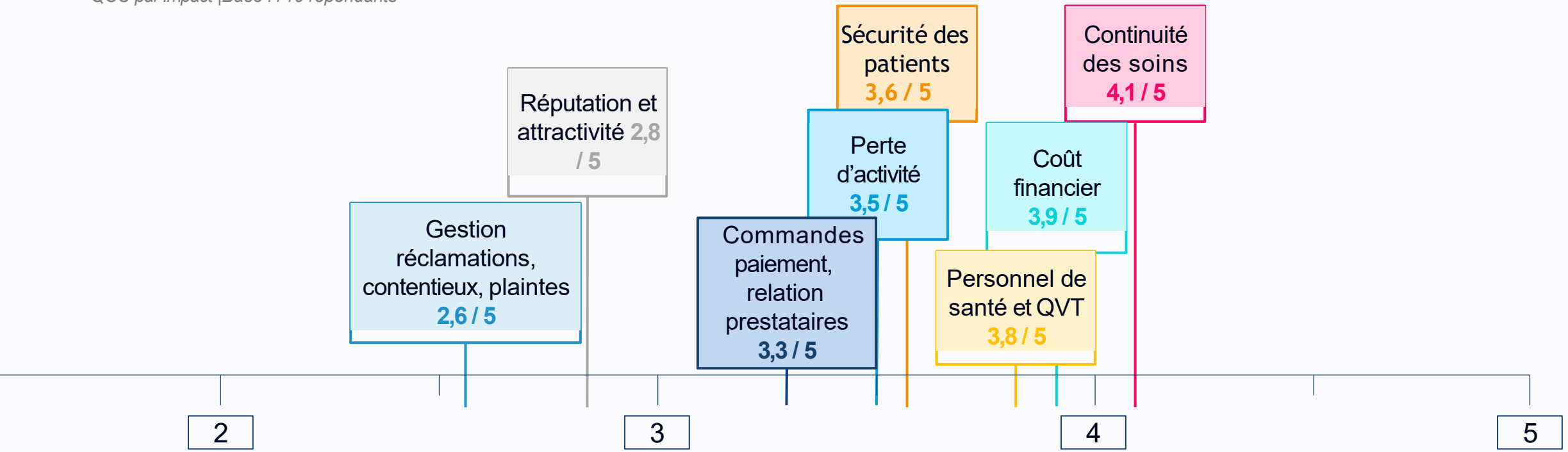
QCM | Base : 719 répondants | 1,4 réponse en moyenne



En cas d'incident cyber, les principaux impacts perçus portent sur la continuité des soins, le coût financier et le personnel de santé

Q10-17. Selon vous, dans le cadre d'un incident cyber, quels seraient les impacts les plus importants pour votre établissement ? Notez l'importance de chacun des impacts suivants sur une échelle de 0 à 5, 5 correspondant à un très fort impact.

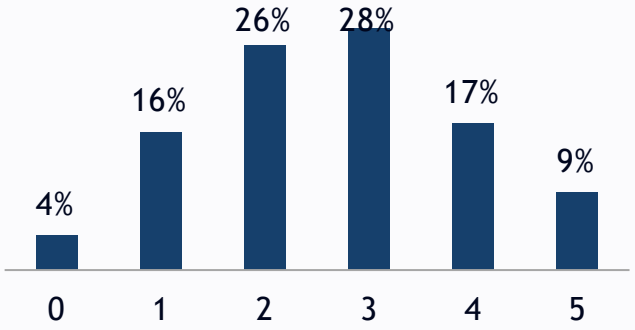
QCU par impact |Base : 719 répondants



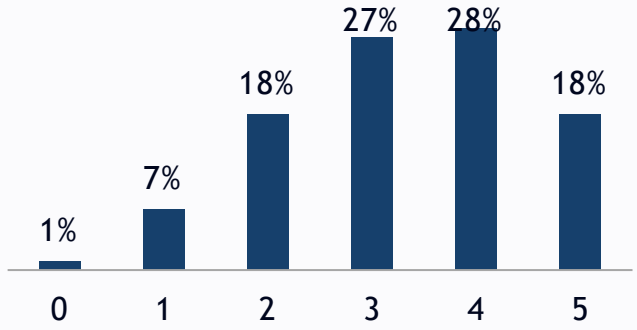
Les impacts perçus d'un incident cyber [1/2]

Q10-17. Selon vous, dans le cadre d'un incident cyber, quels seraient les impacts les plus importants pour votre établissement ? Notez l'importance de chacun des impacts suivants sur une échelle de 0 à 5, 5 correspondant à un très fort impact.

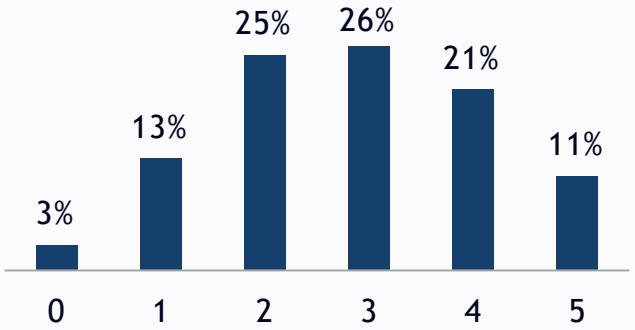
QCU par impact |Base : 719 répondants



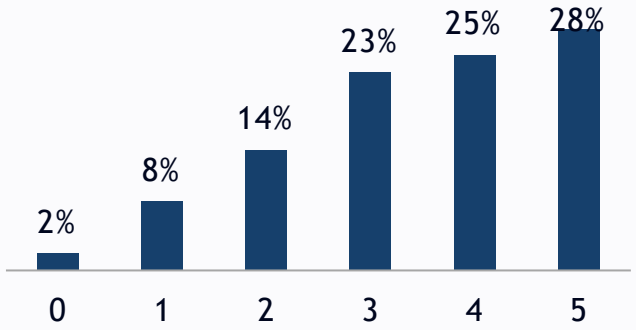
Gestion réclamations, contentieux, plaintes. Moy. **2,6 / 5**



Commande, paiement, relation prestataires. Moy. **3,3 / 5**



Réputation et attractivité. Moy **2,8 / 5**

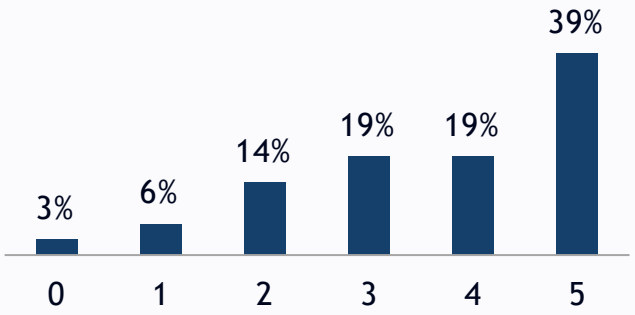


Perte d'activité. Moy. **3,5 / 5**

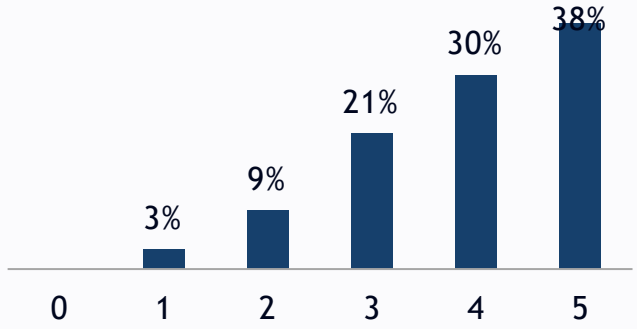
Les impacts perçus d'un incident cyber [2/2]

Q10-17. Selon vous, dans le cadre d'un incident cyber, quels seraient les impacts les plus importants pour votre établissement ? Notez l'importance de chacun des impacts suivants sur une échelle de 0 à 5, 5 correspondant à un très fort impact.

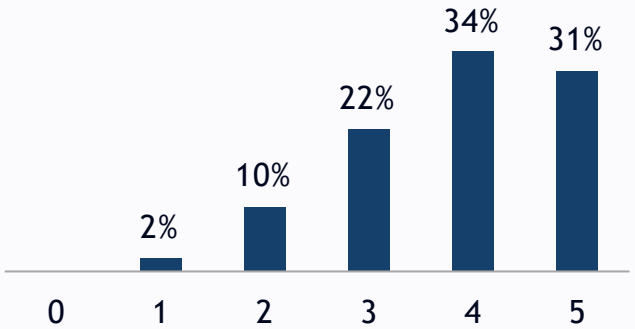
QCU par impact | Base : 719 répondants



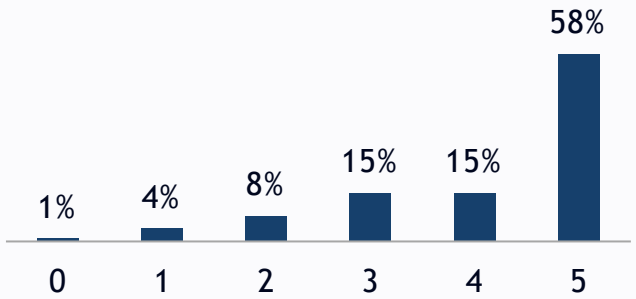
Sécurité des patients. Moy. 3,6 / 5



Coût financier. Moy. 3,9 / 5



Personnel de santé et QVT. Moy. 3,8 / 5

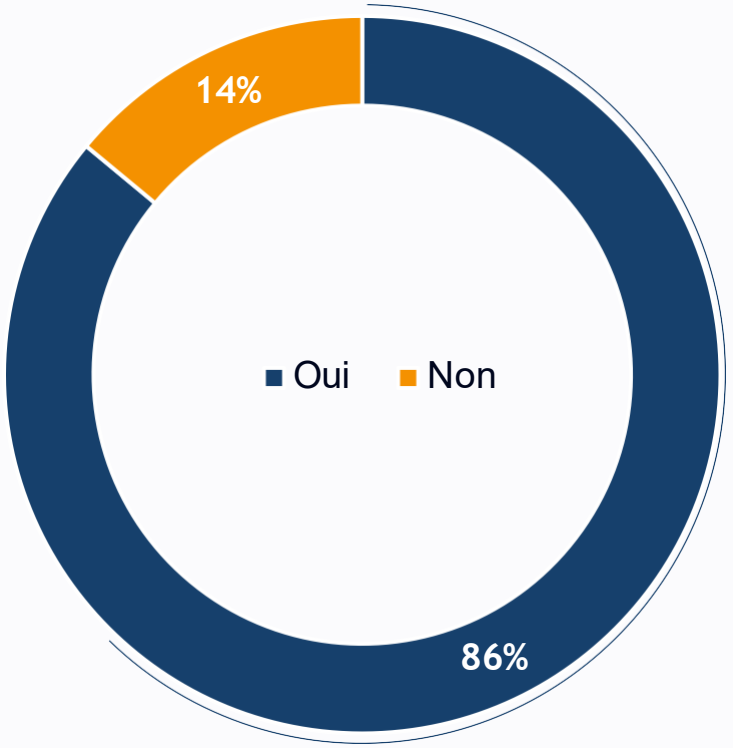


Continuité des soins. Moy. 4,1 / 5

Globalement les impacts identifiés sont travaillés au sein des établissements

QSUP. Est-ce que les impacts identifiés dans la question précédente sont déjà travaillés et pris en compte dans le plan de continuité et de reprise de l'activité de l'établissement ?

QCU |Base : 719 répondants



86% oui

Faible part budgétaire dédiée

Q18.Quelle part la prévention des risques cyber représente-t-elle dans les dépenses d'investissement annuelles (CAPEX) du budget consacré par votre établissement à l'informatique en 2024 ?

QCU |Base : 719 répondants

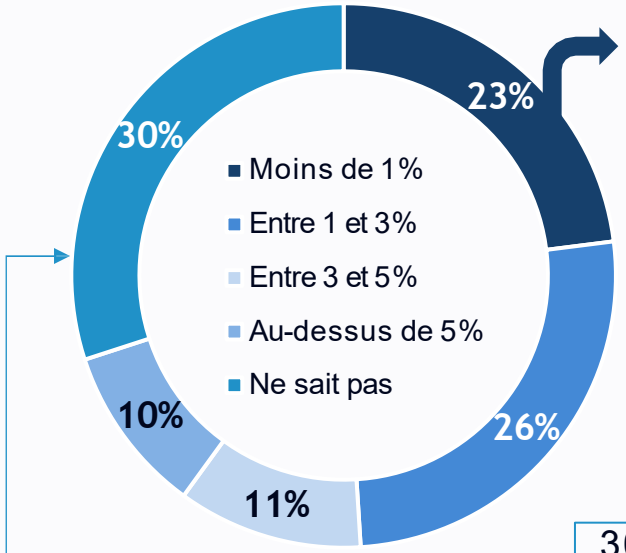
Q19. Quelle part la prévention des risques cyber représente-t-elle dans les dépenses de fonctionnement annuelles (OPEX) du budget consacré par votre établissement à l'informatique en 2024 ?

QCU |Base : 719 répondants

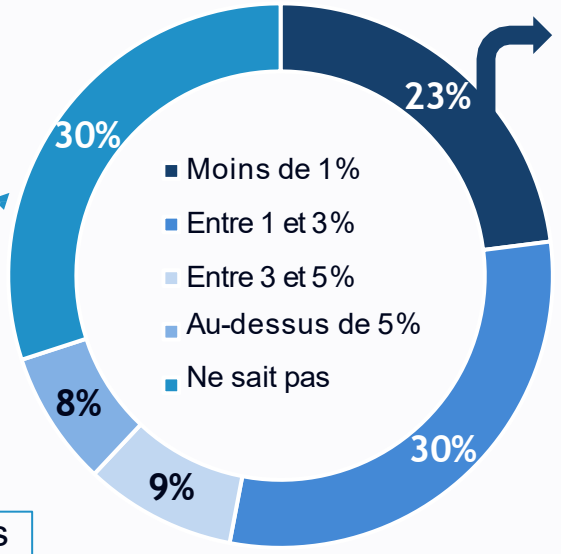
23%
moins de 1%

17% des répondants ont sélectionnés « Moins de 1% » aux deux questions

23%
moins de 1%



But lucratif : 18% / non lucratif : 25%
Privé : 18% / public : 30%



Privé : 19% / public : 29%

30% des répondants ont sélectionnés « Ne sait pas » aux deux questions

La priorité budgétaire est -de loin- au renforcement technique de la sécurité des SI

Q20-24. Le montant financier, que vous allouez à la prévention des risques cyber en 2024/2025, se porte-t-il prioritairement sur ? Classez de 1 à 5.

QCU par impact |Base : 719 répondants

[1 étant le plus prioritaire – 5 étant le moins prioritaire]

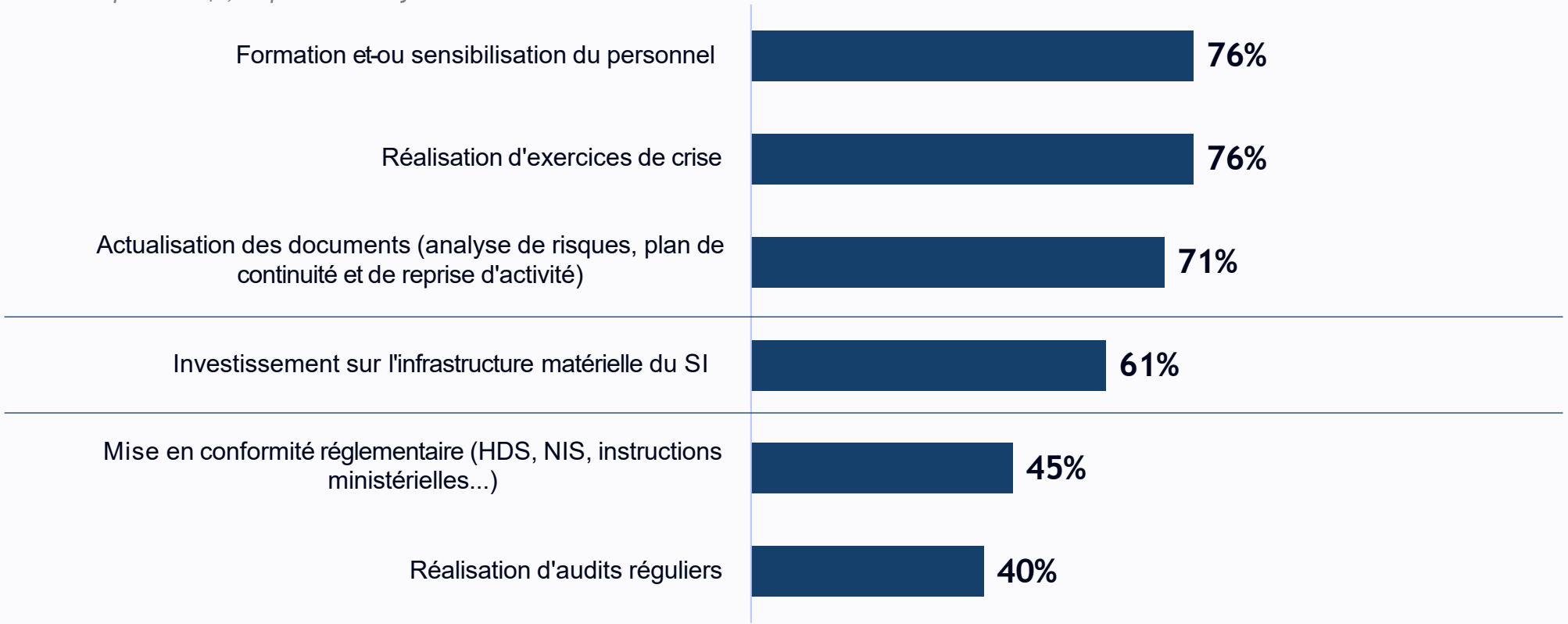
Ordre de priorité (+ / -)

Renforcement technique de la sécurité des SI	2,1 /5	54% 14% 10% 10% 13%
Réalisation d'exercices de crise	3 /5	15% 24% 26% 21% 15%
Analyse de risques, plan de continuité et de reprise d'activité	3,2 /5	10% 22% 23% 25% 19%
Formation et/ou sensibilisation du personnel	3,3 /5	6% 23% 25% 29% 16%
Audits	3,5 /5	15% 17% 16% 16% 37%

Les actions les plus accessibles sont : la formation et sensibilisation du personnel, la réalisation d'exercices de crise, l'actualisation des documents

Q25. Parmi les actions ci-dessous, quelles sont celles que votre établissement sera en mesure d'engager financièrement en 2025 ?

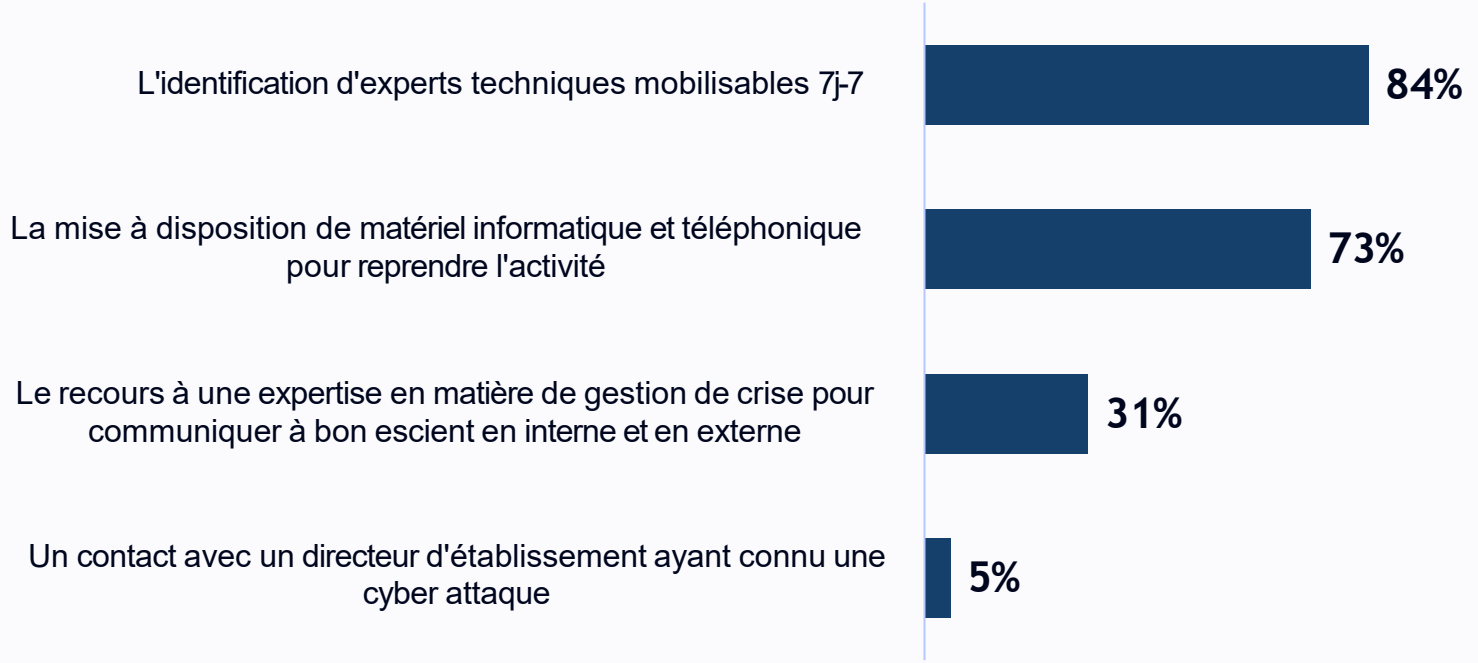
QCM | Base : 719 répondants | 3,7 réponses en moyenne



Les 2 ressources prioritaires sont de loin l'identification d'experts techniques mobilisables 7j-7 et la mise à disposition de matériel informatique et téléphonique pour reprendre l'activité

Q26. Sélectionnez les 2 ressources que vous jugez prioritaires dans le contexte d'une attaque cyber de votre établissement.

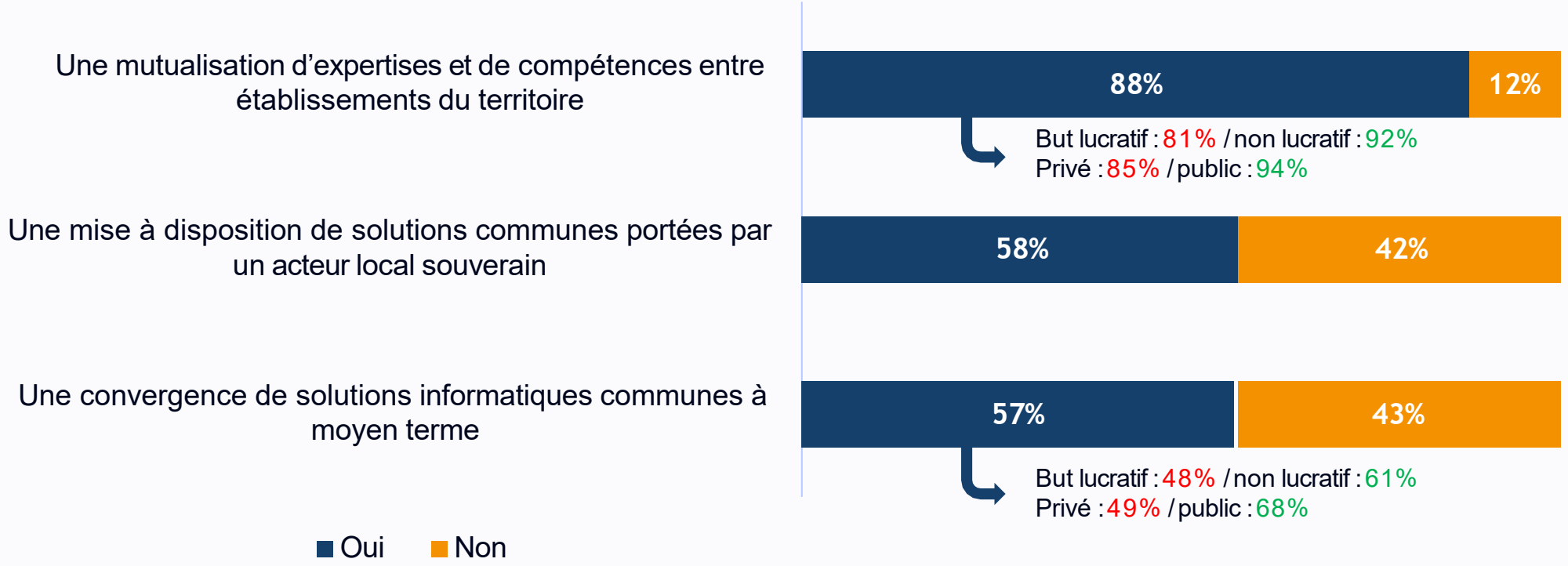
QCM |Base : 719 répondants | 1,9 réponse en moyenne



La mutualisation d'expertises et de compétences entre établissements du territoire est plébiscitée par 9 directeurs d'établissement sur 10 ce qui en fait une priorité

Q27-29. Pour renforcer la prévention et la gestion des attaques cyber et répondre aux contraintes financières des établissements de santé, vous diriez qu'il faut mettre en place sur les territoires :

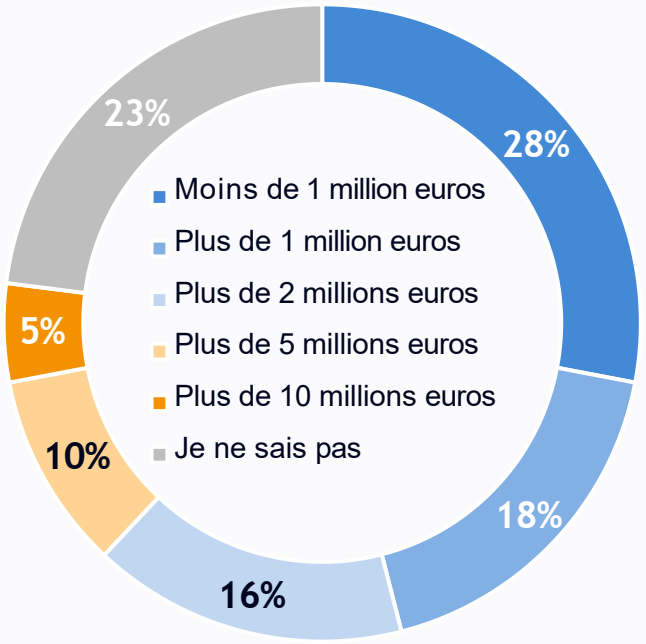
QCU par ligne |Base : 719 répondants



Perception variable du risque économique selon les typologies d'établissement

Q30. Selon vous, le coût global d'une cyber-attaque, qui immobiliserait votre établissement de santé, pendant une durée d'un mois s'élèverait à :

QCU |Base :719 répondants



Coût médian : 1 500 000€

Base répondants : 550 répondants

Conditions de recodage :
Moins de 1 millions d'euros = 500 000€
Plus de 1 millions d'euros = 1 500 000€
Plus de 2 millions d'euros = 3 500 000€
Plus de 5 millions d'euros = 7 500 000€
Plus de 10 millions d'euros = 12 000 000€

	Total	Privé	Public	But lucratif	But non lucratif	Inférieure à 100 lits	De 100 à 300 lits	De 300 à 1 000 lits	Supérieure à 1 000 lits
Moins de 5 millions euros	**62%**	**65%**	56%	**69%**	58%	**73%**	64%	54%	**22%**
Plus de 5 millions euros	**15%**	10%	**22%**	10%	**17%**	1%	11%	**28%**	59%

Taux de participation des différentes directions d'établissement aux exercices de crise

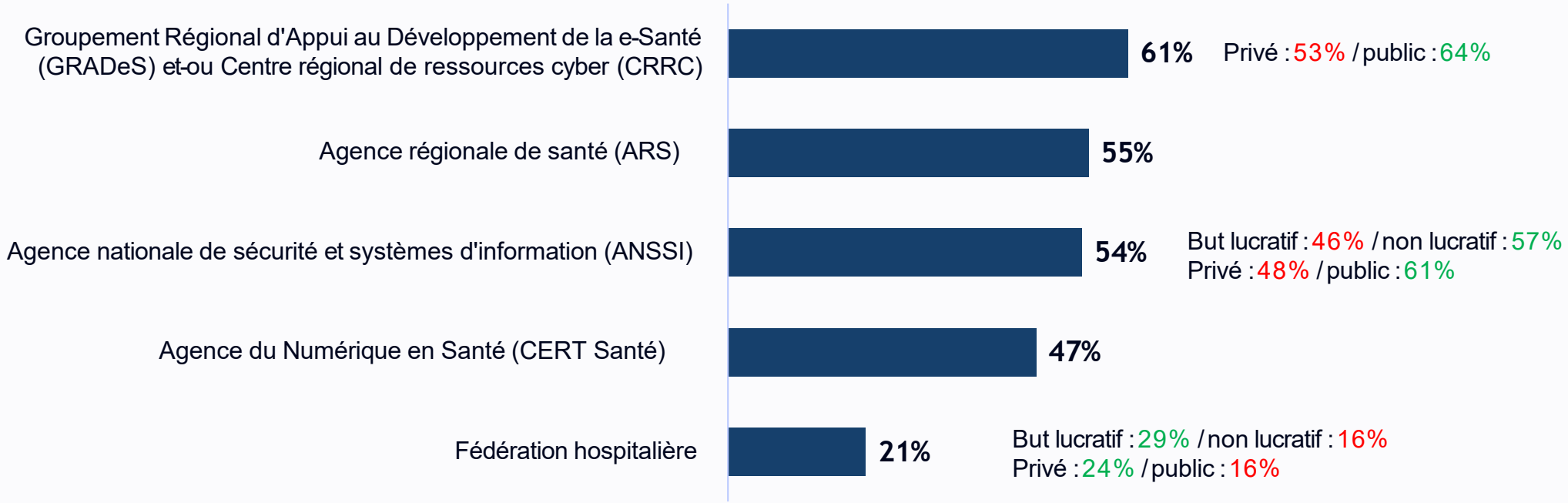
Q31. Quelles sont les directions de votre établissement qui ont participé à l'exercice de crise cyber que vous avez réalisé en 2023/2024 ?

QCM |Base : 719 répondants |6,3 réponses en moyenne

Les GRADeS / CRRC en tête sur l'accompagnement et la prévention des risques cyber

Q32. Pour conclure, parmi les parties prenantes ci-dessous, quelles sont celles qui vous apportent un accompagnement régulier (hors financement) dans le domaine de la prévention des risques cyber et de la gestion des crises cyber ?

QCM | Base : 719 répondants | 2,4 réponses en moyenne



AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

GRANDS ENSEIGNEMENTS

Grands enseignements (1/2)

1. **Un sentiment de vulnérabilité latent :**

Seuls 15 % des établissements ont connu un incident cyber perturbateur ces 3 dernières années, mais moins d'1 sur 6 se sentait réellement bien préparé au moment des faits. Et même sans incident subi, la majorité des directeurs restent lucides sur leur niveau de préparation (seuls 13% se déclarent « bien préparés »).

2. **Une gouvernance globalement mobilisée, mais des moyens encore trop limités :**

Si la cybersécurité est bien inscrite à l'agenda des directions générales (exercices de crise, réunions SSI, implication directe), 42% des directeurs estiment ne pas avoir les moyens nécessaires pour un plan de prévention adapté. Ce constat est accentué dans les établissements publics et non lucratifs.

3. **Un arbitrage budgétaire défavorable à la cybersécurité :**

60% des établissements consacrent moins de 5% de leur CAPEX informatique à la cybersécurité, et plus d'un sur quatre moins de 1%. Dans ce contexte, les actions perçues comme les plus accessibles sont la sensibilisation du personnel, les exercices de crise et l'actualisation documentaire.

4. **Des réflexes bien identifiés face à la crise :**

En cas d'attaque, les directeurs privilégient deux réponses : la mobilisation rapide d'experts techniques (84%) et la mise à disposition de matériel pour assurer la continuité (73%). En revanche, la communication de crise ou l'appui d'un pair expérimenté restent très secondaires.

Grands enseignements (2/2)

5. **Un appel à la mutualisation territoriale :**

9 directeurs sur 10 plébiscitent la coopération locale entre établissements. Cette attente est particulièrement forte dans le public (94%) et dans le non lucratif (92%). Des solutions partagées, portées par des acteurs souverains à l'échelle des territoires, sont largement soutenues.

6. **Des différences nettes entre petits et grands établissements :**

Les petits établissements (<100 lits) sont un peu moins exposés aux incidents (12%), mais plus souvent démunis en moyens et ressources humaines. À l'inverse, les établissements de 300 à 1000 lits sont plus souvent victimes (21%) mais également mieux structurés (78% d'équipes jugées compétentes et autonomes).

7. **Privé/lucratif versus public/non lucratif : une ligne de fracture sur les moyens :**

Les établissements privés à but lucratif se sentent plus préparés, sont plus nombreux à connaître leur plan de prévention, et consacrent des moyens plus importants. À l'opposé, les publics/non lucratifs cumulent plus souvent manque de ressources, retard budgétaire et moindre accompagnement par les fédérations professionnelles.

AGENCE DU NUMÉRIQUE EN SANTÉ
La transformation commence ici

MERCI DE VOTRE ATTENTION