BAROMÈTRE
DE LA SOUVERAINETÉ NUMÉRIQUE 2025

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

EY

L'ÉDITO

Jean-Noël de Galzain
Président Hexatrust
CEO Wallix Group

Les résultats de ce baromètre de la souveraineté numérique soulignent l'importance cruciale de renforcer nos efforts en matière de pédagogie et de visibilité des solutions souveraines. Ce baromètre témoigne d'un engagement constant depuis plus de dix ans d'Hexatrust, qui travaille au quotidien à fédérer les entreprises françaises et européennes les plus dynamiques dans les domaines du cloud de confiance et de la cybersécurité. Notre mission est de continuer à jouer ce rôle essentiel, en multipliant les initiatives qui mettent en lumière l'excellence de nos solutions.

Cette année, avec le lancement de l'HexaDiag et de l'HexaSearch, nous avons équipé les organisations d'outils puissants pour agir concrètement et bâtir la souveraineté numérique de demain. Ces initiatives ne sont que le début d'un mouvement plus large visant à structurer notre filière, à renforcer le dialogue avec les institutions et à stimuler des dynamiques collectives.

Hexatrust s'engage à bâtir une véritable filière d'excellence du numérique souverain, capable de répondre aux enjeux stratégiques de résilience et d'autonomie pour l'Europe. En travaillant ensemble, nous pouvons créer un écosystème robuste et innovant, prêt à relever les défis de demain et à garantir notre indépendance technologique. C'est en unissant nos forces que nous pourrons véritablement construire un avenir numérique souverain et sécurisé pour tous.

LA SOUVERAINETÉ COMME CRITÈRE STRATÉGIQUE : CAP OU PAS CAP ?

"Choisir une solution souveraine est encore trop souvent vu comme un acte militant, plutôt que comme un acte stratégique." Alain GARNIER, CEO Jamespot.

La souveraineté doit accélérer pour s'imposer dans le paysage de la cybersécurité en France.

Bien que la majorité des organisations, publiques comme privées, aient engagé une démarche globale de sécurisation de leurs systèmes d'information, l'adoption de solutions souveraines reste encore marginale. Ce besoin est encore moins identifié lorsque l'organisation n'a pas été identifiée de prime abord comme Entité Essentielle ou Importante. Plusieurs facteurs peuvent expliquer cette situation :

Un cadre réglementaire en évolution, notamment avec la directive NIS2, qui devrait nous inciter à recourir à des solutions souveraines. Pourtant,

49%

des organisations interrogées n'ont pas encore défini de plan d'action pour s'y conformer.

Une méconnaissance des acteurs souverains, souvent associée à des doutes sur leur maturité technologique, leur couverture fonctionnelle, leur fiabilité ou leur coût. Ainsi,

40%

des répondants déclarent ne pas effectuer de veille sur ces solutions.

Un manque de perception du besoin de souveraineté, particulièrement dans le secteur privé, même lorsque le siège est situé en France. Ce besoin est encore moins identifié lorsque la directive NIS2 ne s'applique pas directement.

Ces constats soulignent l'importance d'une meilleure sensibilisation aux enjeux de souveraineté numérique et d'un accompagnement renforcé pour intégrer ces solutions dans les stratégies de cybersécurité.

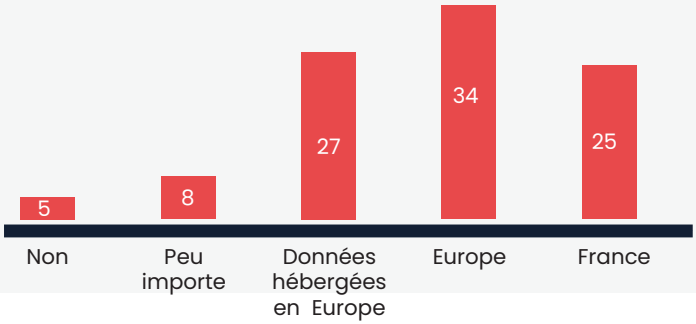
MÉCONNAISSANCE
DE L'ÉCOSYSTÈME SOUVERAIN

Connaissez vous l'association Hexatrust ?

Les principaux labels et associations en charge de la promotion de l'écosystème souverain sont connus d'une grande partie des organisations sollicitées (plus des 3/4) mais ne sont pas encore suffisamment mobilisés dans le cadre du référencement des solutions de cybersécurité ou en amont des appels d'offres.

En effet, près de **40%** des organisations ne font pas de veille sur les solutions souveraines, et **42%** le font au mieux 1 fois par an.

Privilégiez-vous l'achat de solutions françaises ou européennes dans les domaines de la cybersécurité et du Cloud, incluant une préférence pour des solutions souveraines ?



MALGRÉ UNE PRISE DE CONSCIENCE DE PLUS EN PLUS IMPORTANTE DE LA PART DES ACTEURS

Le contexte géopolitique actuel contribue à faire évoluer les priorités, notamment au sein des structures nationales et, plus encore, des organisations publiques, avec la nécessité de maîtriser son patrimoine informationnel. En revanche, les entreprises internationales restent davantage guidées par des critères de performance, de fiabilité et d'adéquation aux risques identifiés, que par des considérations de souveraineté, d'autant plus qu'elles ont besoin d'être rassurées par une présence en dehors des frontières.

" Oui, nous avons des dépendances. Mais arrêtons de nous auto-censurer. La France a des atouts considérables qu'il faut mettre en avant." Clara Chappaz, Ministre déléguée, chargée de l'intelligence artificielle*

Cette exigence de résultats est d'autant plus marquée que le marché des solutions souveraines demeure encore peu connu, ou perçu comme n'offrant pas toujours des alternatives équivalentes aux solutions globalement établies, malgré les progrès réalisés ces dernières années.

L'intensification des réglementations européennes et nationales pousse néanmoins les organisations à s'intéresser de plus près à l'offre souveraine. Pour répondre à cette attente croissante, les acteurs du marché devront relever plusieurs défis majeurs :

- Assurer une capacité d'opération à l'échelle mondiale ;
- Maintenir une compétitivité économique ;
- Proposer des solutions techniquement robustes, ergonomiques et capables de passer à l'échelle ;
- Renforcer leur maturité, leur fiabilité et atteindre une taille critique.

50%

1 organisation sur 2 a déjà écarté une solution IT en raison de préoccupations liées à la souveraineté

79%

Près de 4 organisations sur 5 pensent que la souveraineté est un critère de choix qui prendra de plus en plus d'importance à l'avenir.

Le contexte géopolitique, les guerres, la situation économique, etc. sont autant de facteurs « facilitant ».

C'est à cette condition que les solutions souveraines pourront s'imposer comme de véritables alternatives dans les stratégies de cybersécurité des organisations.

*Source : Discours Clara Chappaz, Ministre déléguée, chargée de l'intelligence artificielle et du numérique prononcé le 14 avril 2025 lors de la soirée de la Souveraineté du numérique

3 QUESTIONS À

Simon UZENAT
Sénateur du Morbihan
Président de la Commission d'enquête sur les coûts et les modalités effectifs de la commande publique et la mesure de leur effet d'entraînement sur l'économie française

Aujourd'hui, une organisation sur deux affirme avoir déjà écarté une solution IT pour des raisons de souveraineté. Selon vous, le critère de souveraineté est-il suffisamment pris en compte aujourd'hui dans les choix des acheteurs publics ?

Clairement non ! Le rapport de la commission d'enquête souligne à plusieurs reprises les incohérences caractérisées entre les discours et les actes. Les exemples du marché de l'Éducation nationale ou encore de la Plateforme des données de Santé (Health Data Hub), confiés à Microsoft malgré l'existence d'alternatives françaises et en contradiction avec la doctrine « cloud au centre », témoignent de l'inconséquence gouvernementale depuis de trop longues années.

Face à la méconnaissance persistante de l'offre souveraine en cybersécurité - 53 % des répondants ne la jugent pas différenciante et 40 % n'effectuent aucune veille dédiée, comment mobiliser les entreprises et renforcer la visibilité et l'attractivité des solutions souveraines ?

Jusqu'à très récemment, la souveraineté numérique et ses conséquences en matière d'innovation, d'emploi et de protection des données, n'ont pas été identifiées comme des enjeux prioritaires par les acteurs publics comme privés. Attirés par des prix d'entrée plus bas, nombre d'entre eux n'ont pas, encore maintenant, pris la pleine mesure des risques auxquels ils s'exposent, a fortiori dans le contexte de guerre commerciale : hausses brutales des coûts, ruptures de services, soumission aux législations extraterritoriales au détriment de la sécurité des données, comme l'a d'ailleurs reconnu le Directeur des affaires publiques et juridiques de Microsoft France.

Pour renforcer l'attractivité des solutions souveraines, il faut d'abord un effort massif de sensibilisation afin de démontrer concrètement les risques liés à nos dépendances aux solutions non-européennes, en particulier aux GAFAM. **Ensuite, la puissance publique doit assumer son rôle de prescripteur : en donnant de la visibilité par la commande publique aux opérateurs français et européens de solutions adaptées aux attentes des différents utilisateurs, en structurant des réseaux mixtes publics/privés, et en renforçant la formation des acheteurs pour qu'ils soient capables d'identifier et de valoriser l'offre nationale**. Nous appelons aussi les acteurs publics et privés à faire preuve de la plus grande vigilance en cas de recours à des cabinets de conseil car ces derniers peuvent, eux aussi, être soumis à l'application de législations extraterritoriales.

Face à l'intensification des tensions géopolitiques, à la montée des cybermenaces et à la dépendance accrue envers des solutions non-européennes, quelles responsabilités et leviers d'action reviennent aux politiques publiques pour consolider notre autonomie stratégique numérique ?

Le rapport de la commission est clair : **la commande publique constitue un levier stratégique majeur pour réduire notre dépendance et soutenir l'émergence de champions européens.**

L'exemple américain est éclairant : c'est un marché public passé par la CIA en 2013, pour un montant de 600 millions de dollars, qui a permis à Amazon Web Services de devenir un acteur mondial du cloud. La France et l'Union européenne doivent adopter la même logique en passant des contrats massifs et de long terme avec des fournisseurs souverains, afin de leur garantir des débouchés et de leur permettre d'investir pour répondre aux besoins.

Cela implique de mettre en oeuvre une véritable préférence européenne, sur le modèle du Buy American Act. Notre rapport recommande ainsi d'instaurer un principe général de préférence européenne dans les achats des personnes publiques. **Nous demandons également à rendre obligatoire l'insertion d'une clause de non-soumission aux lois extraterritoriales étrangères dans tous les marchés publics comportant des prestations d'hébergement et de traitement de données publiques en cloud.** Enfin, parmi les solutions qualifiées SecNumCloud, nous appelons à privilégier le recours à celles qui reposent sur des technologies intégralement souveraines.

Ce volontarisme doit aller de pair avec un Small Business Act européen, réservant une part des marchés aux PME innovantes, et avec l'application stricte de la doctrine « cloud au centre » pour toutes les données publiques. En somme, il s'agit de **transformer la commande publique en outil assumé de souveraineté numérique et de résilience économique.**

Vous avez porté une réflexion d'ampleur au Sénat sur la commande publique aux côtés de votre collègue sénateur Dany Wattebled. Quelles seront, selon vous, les priorités à inscrire dans les chantiers prioritaires à venir pour faire évoluer durablement la commande publique au service de la souveraineté numérique ?

La priorité est d'instaurer un principe de préférence européenne dans le cadre du processus de révision des directives sur les marchés publics. À l'échelle de notre pays, nous recommandons de rationaliser le pilotage de la politique numérique de l'État en réaffirmant le rôle de pilote de la direction interministérielle du numérique, sous l'autorité du Premier ministre, et en rappelant aux administrations de l'État le caractère obligatoire de la doctrine « cloud au centre ».

Nous demandons aussi à l'État de faire preuve de cohérence en garantissant des moyens budgétaires adaptés pour les différents acheteurs publics, en particulier les collectivités locales et les hôpitaux. Nous souhaitons par ailleurs faire de l'Ugap un outil de souveraineté économique en confiant sa tutelle au seul ministère chargé de la souveraineté industrielle et numérique et en lui assignant un objectif d'appui à la structuration de la filière française et européenne du numérique, avec la diffusion de solutions souveraines en matière de logiciels et d'hébergement en nuage.

DÉTAILS DE L'ÉTUDE
ÉLÉMENTS CLÉS DU BAROMÈTRE

96

DSI et RSSI interrogés

79%

Dans le secteur public et **21%** dans le secteur privé

37

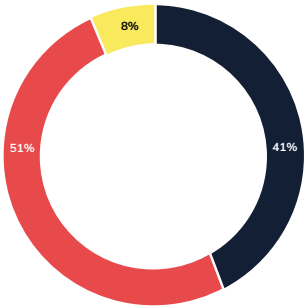
Questions posées dont 10 directement liées à la souveraineté

GOUVERNANCE
SÉCURITÉ DES SI

Toutes les organisations interrogées ont défini un budget pour la gestion de la cybersécurité (incluant la séparation des coûts associés aux ressources des dépenses relatives aux solutions de sécurité).
Mais **23%** des organisations le font dans un budget commun avec la Direction des Systèmes d'Information.

74%

Les organisations ont majoritairement intégré une démarche globale pour la Sécurité des SI **(95%)**, incluant un engagement de l'exécutif pour les 3/4 d'entre elles.



Une majorité des organisations interrogées s'appuie sur une connaissance au moins partielle des risques liés au numérique.

Crédit photo : VideoFlow - #1507111403 - stock.adobe.com

Crédit photo : Spirit - #1423594318 - stock.adobe.com

RÉGLEMENTATION & CONFORMITÉ

Les organisations publiques et privées évoluent dans un environnement réglementaire de plus en plus complexe et structurant.
2025 et 2026 apporteront des nouveautés non négligeables (CRA, NIS2, etc.) pour lesquelles les organisations sont en train de se mettre en ordre de marche, malgré les discussions encore en cours au niveau étatique.

49%

ne sont pas prêtes et n'ont pas défini de plan d'action pour se mettre en conformité avec NIS2

16%

savent déjà que NIS2 ne s'applique pas pour elles

SENSIBILISATION
À LA CYBERSÉCURITÉ

Les organisations réalisent de plus en plus d'actions de formation et de sensibilisation auprès de leurs employés, même si la fréquence de ces actions peut fortement varier, les programmes de sensibilisation et de formation ne sont pas toujours sur mesure ni adaptés aux différentes populations au sein de l'organisation. 44% seulement des organisations dispensent des formations cybersécurité adaptées à leurs équipes opérationnelles (IT, cyber, etc.).

46%

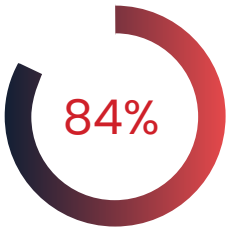
connaissent les principaux éditeurs de solution de sensibilisation souverains : Conscio Technologies, SoSafe, etc.

32%

connaissent les principaux organismes de formation spécialisés dans la cybersécurité : HS2, SecureSphere by EPITA, etc.

DÉTECTION
& RÉPONSE À INCIDENT

Les SOC sont de plus en plus déployés au sein des organisations interrogées, en 24x7 ou en HO. Contrairement à ce qu'on pourrait penser, le SOC est même plus répandu que des services de détection de type MDR (Managed Detection and Response).



En complément du SOC, **34%** des organisations sollicitées ont souscrit à un service d'Incident Retainer et 32% ont souscrit à une assurance cybersécurité.

En revanche, parmi les organisations, il est à noter que seuls :
24% des prestataires de confiance pour le SOC sont PDIS (qualification de l'ANSSI pour les Prestataires de Détection des Incidents de Sécurité).
33% des prestataires de confiance pour la Réponse à Incident sont PRIS (qualification de l'ANSSI pour les Prestataires de Réponse à Incident de Sécurité)

RÉSILIENCE CYBER :
GESTION DE CRISE & RECONSTRUCTION SI

62%

considèrent leur gestion de crise et leur dispositif de reconstruction opérationnel.

64%

des acteurs testent leur PCA/PRA au moins une fois par an, le reste ne le testant jamais, voire n'ont pas défini leurs procédures de reconstruction.

73%

des acteurs réalisent au moins un exercice de crise cyber par an pour sensibiliser leurs dirigeants.

32%

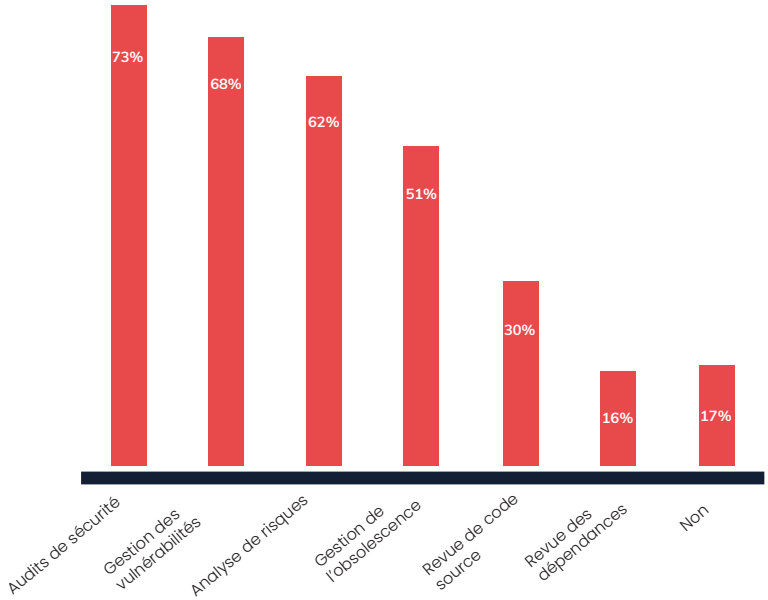
seulement des acteurs déclarent tester la restauration de leurs sauvegardes et seulement 35% considèrent leurs procédures de reconstruction bien formalisées.

INTÉGRATION DE LA SÉCURITÉ
DANS LES PROJETS LIÉS AUX TIERS

Si les acteurs en grande majorité déclarent mettre en œuvre une démarche d'intégration de la sécurité dans les projets, certaines activités sont plus répandues que d'autres.

L'identification des risques cyber induits par les projets est réalisée par **62%** des acteurs, bien que la méthodologie varie : au sein des organisations publiques c'est la méthodologie EBIOS RM qui prime, tandis que les entreprises privées ont souvent leur propre méthode.
La gestion des vulnérabilités **(68%)** et les audits de sécurité techniques **(73%)** sont les activités les plus répandues, En revanche, l'analyse automatisée des dépendances ou la revue du code source sont moins fréquentes.

Enfin, seule la moitié des organisations sollicitées met en place une gestion de l'obsolescence. Lorsque les organisations font appel à des tiers pour le développement ou l'intégration, le principal garde-fou mis en place est la gestion contractuelle, au détriment de l'analyse de la maturité cybersécurité du tiers, de ses certifications, ou même d'un suivi des exigences de sécurité tout au long de la relation contractuelle.



Intégrez-vous une démarche dite de « sécurité dès la conception (Security by design) » lors du développement ou de l'acquisition d'un système d'information au travers d'analyses de risques et de tests de sécurité ?

Crédit photo : InfiniteFlow - #1532854040 - stock.adobe.com

RISQUES LIÉS
AUX NOUVELLES TECHNOLOGIES

Une maturité encore très faible sur les risques cyber liés aux nouvelles technologies ou aux futurs usages :

- **Intelligence Artificielle** : manque de recul et de cadre de gouvernance adapté
- **Prestataire Cloud** : risques de fuite ou de perte de données non couverts contractuellement
- **Informatique quantique** : menace future sur la cryptographie actuelle
- **Interopérabilité des systèmes dans les territoires connectés** : multiplication des points d'entrée vulnérables
- **Véhicules autonomes** : nouveaux enjeux de sécurité des systèmes embarqués

22%

L'IA est encore peu intégrée, et son impact en matière de cybersécurité reste peu analysé.
22% des acteurs déclarent avoir une vision claire des risques cyber liés à l'IA

41%

Forte dépendance aux prestataires, avec une faible appropriation des responsabilités de sécurité.
41% des répondants estiment que leurs exécutifs n'ont pas connaissance des risques liés au Cloud et que ces risques sont mal maîtrisés

HEXATRUST
CLOUD CONFIDENCE & CYBERSECURITY

EY

EY s'engage à bâtir un monde meilleur, en créant de la valeur sur le long terme pour nos clients et nos collaborateurs aussi bien que pour la société et la planète dans leur ensemble, tout en renforçant la confiance dans les marchés financiers.
En s'appuyant sur le traitement des données, l'IA et les nouvelles technologies, les équipes EY contribuent à créer la confiance nécessaire à nos clients pour façonner un futur à l'épreuve des défis les plus pressants d'aujourd'hui et demain.
À travers tout un éventail de services allant de l'audit au consulting en passant par la fiscalité, la stratégie et les transactions, les équipes d'EY sont en mesure de déployer leur expertise dans plus de 150 pays et territoires. Une connaissance approfondie du secteur, un réseau international et pluridisciplinaire ainsi qu'un écosystème de partenaires aussi vaste que diversifié sont autant d'atouts qui permettront à EY de participer à la construction d'un monde plus équilibré. Ensemble pour créer un futur riche d'opportunités. EY désigne l'organisation mondiale et peut faire référence à l'un ou plusieurs des membres d'Ernst & Young Global Limited, dont chacun représente une entité juridique distincte. Ernst & Young Global Limited, société britannique à responsabilité limitée par garantie, ne fournit pas de prestations aux clients. Les informations sur la manière dont EY collecte et utilise les données personnelles, ainsi que sur les droits des personnes concernées au titre de la législation en matière de protection des données sont disponibles sur ey.com/privacy. Les cabinets membres d'EY ne pratiquent pas d'activité juridique lorsque les lois locales l'interdisent.
Pour plus d'informations sur notre organisation, veuillez-vous rendre sur notre site ey.com.

SCORE N°2025-076
ED None.
Crédit photo : EY, Adobe Stock, Hexatrust

CAMPUS CYBER - HEXATRUST
5-7 rue Bellini - 92800 Puteaux
hexatrust.com - contact@hexatrust.com