



Communiqué de presse

AL'X COMMUNICATION - Véronique Loquet
+33 668 427 968 vloquet@alx-communication.com

IA, réglementation, dépendances, les RSSI doivent arbitrer sur tous les fronts

21 mini-sondages menés auprès des membres du CESIN au premier semestre 2026, éclairent les tendances, les priorités et les arbitrages des RSSI.

Paris, 16 septembre 2026 – Au premier semestre 2026, les RSSI ont dû composer avec une accélération simultanée des usages technologiques, des exigences réglementaires et des risques liés aux dépendances numériques. Dans ce contexte, leur enjeu n'est plus seulement de renforcer la protection des organisations, mais de hiérarchiser des priorités toujours plus nombreuses, et d'arbitrer entre des chantiers qui deviennent tous stratégiques.

C'est le principal enseignement des Instantanés du CESIN au premier semestre 2026. À travers 21 mini-sondages hebdomadaires, les membres du CESIN témoignent d'une fonction cyber en pleine transformation.

La cybersécurité ne repose plus seulement sur la protection du système d'information. Elle engage désormais les métiers, les fournisseurs et les directions, et place l'arbitrage au cœur de la fonction RSSI.

Fabrice Bru, Président du CESIN, déclare : « *La mission du RSSI est en plein chamboulement. Les repères évoluent, les priorités aussi, et les réponses d'hier ne suffisent plus toujours. Les RSSI doivent aujourd'hui trouver leur propre voie pour accompagner cette transformation.* »

L'IA avance, et sa gouvernance se construit

L'IA générative s'installe dans les organisations. Or, les règles ne progressent pas toujours au même rythme, de nombreuses organisations, plutôt de taille intermédiaire (27% des répondants), n'ont encore défini aucune politique concernant son utilisation.

Les environnements de développement enrichis à l'IA illustrent cette situation. Seuls 18% des répondants ont mis en place une politique spécifique pour les développeurs. 34% autorisent leur installation de manière générale. 34% l'autorisent par exception.

Les outils de transcription et de synthèse des réunions posent les mêmes questions. Qui accède aux données ? Où sont-elles stockées ? Combien de temps sont-elles conservées ?

L'IA entre aussi dans les outils de cybersécurité. Les organisations expérimentent, et la majorité se situe encore au stade du pilote ou du test. Trois préoccupations dominent, la fiabilité, la confidentialité et la souveraineté.

Cette accélération concerne aussi les usages malveillants de l'IA. 54% des grandes entreprises interrogées déclarent avoir déjà subi une attaque de type deepfake, ainsi que 19% des ETI et 5% des TPE/PME. L'exposition progresse donc nettement avec la taille de l'organisation.

Le post-quantique reste largement à ouvrir

La migration vers la cryptographie post-quantique reste encore peu engagée. 69% des répondants n'ont pas encore commencé à s'en préoccuper. 20% évaluent les impacts et les besoins, 3% ont engagé des pilotes ou des tests, et seul 1% a commencé une migration opérationnelle.

Le chantier dépasse la seule technologie. Il suppose d'identifier les usages cryptographiques et les données critiques, mais aussi d'inscrire le sujet dans une gouvernance plus transverse.

La conformité s'impose davantage dans les plus petites organisations

La conformité réglementaire arrive en tête des priorités cyber pour 2026. 46% des grandes entreprises la placent parmi leurs trois chantiers prioritaires. Ce taux atteint 61% dans les ETI et 72% dans les TPE/PME.

Les grandes entreprises répartissent davantage leurs priorités. Elles travaillent aussi sur l'IA, les tiers et la gouvernance. Les structures plus petites concentrent davantage leurs efforts sur la conformité.

Le risque cyber se joue aussi chez les fournisseurs

Les dépendances technologiques occupent une place croissante dans les préoccupations des RSSI. Le Cyber Resilience Act en donne une illustration. 52% des ETI interrogées ne sont pas directement concernées par le règlement, mais elles sont toutes clientes de fournisseurs qui le sont.

Les rachats dans le secteur cyber produisent également des effets très concrets. 69% des grandes entreprises déclarent avoir constaté une explosion des coûts après le rachat d'un fournisseur ; ce score grimpe à 74% chez les ETI, et 38% des TPE/PME constatent le même phénomène. En outre, 41% des répondants soulignent un enfermement technologique.

Le risque ne s'arrête plus aux frontières du système d'information. Il se prolonge dans les chaînes de fournisseurs et dans les choix technologiques.

La transformation du métier se lit aussi dans les carrières

L'évolution de la fonction se lit aussi dans les perspectives de carrière des RSSI. Interrogés à nouveau deux ans après un premier sondage sur le sujet, seuls 24% des 162 répondants estiment que les opportunités de postes de RSSI sont aussi nombreuses que par le passé, soit 17 points de moins qu'en 2024. Dans le même temps, 31% envisagent de basculer vers le conseil faute de capacité à agir dans les organisations, une proportion en hausse de 16 points. Au-delà du marché de l'emploi, ces résultats traduisent aussi une interrogation sur les conditions dans lesquelles les RSSI peuvent aujourd'hui exercer pleinement leur fonction.

La maturité cyber change de nature

Ces Instantanés ne dessinent pas une cybersécurité moins mature. Ils montrent une cybersécurité plus complexe. Les RSSI doivent désormais conjuguer protection, anticipation et arbitrage, tout en inscrivant leurs décisions dans une gouvernance plus large, associant métiers et directions.

La maturité cyber ne se mesure donc plus seulement aux dispositifs déployés, mais aussi à la capacité de l'organisation à faire des choix éclairés face au risque.

À propos des Instantanés du CESIN

Les Instantanés du CESIN du premier semestre 2026 s'appuient sur 21 mini-sondages hebdomadaires réalisés auprès des membres du CESIN. Les panels comptent entre 84 et 160 répondants selon les questions, avec une moyenne de 116 répondants.

A propos du CESIN

Le CESIN (Club des Experts de la Sécurité de l'Information et du Numérique) est une association loi 1901, créée en juillet 2012, avec des objectifs de professionnalisation, de promotion et de partage autour de la cybersécurité.

Lieu d'échange, de partage de connaissances et d'expériences, le CESIN permet la coopération entre experts de la sécurité de l'information et du numérique et entre ces experts et les pouvoirs publics. Il participe à des démarches nationales et est force de proposition sur des textes réglementaires, guides et autres référentiels. Le CESIN compte parmi ses membres plusieurs organismes et institutions, comme l'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI), Gendarmerie Nationale, Commandement Cyber Gendarmerie, Commission Nationale de l'Informatique et des Libertés (CNIL), Gimelec, Préfecture de Police, Police Judiciaire, Cybermalveillance.gouv.fr, Ministère de la Justice, Ministère de l'Intérieur.

Le CESIN rassemble plus de 1 300 membres issus de tous secteurs d'activité, industries, Ministères et entreprises, dont CAC40 et SBF120. Pour en savoir plus www.cesin.fr