ÊTRE PRÉPARÉ AUX RISQUES OU Y ÊTRE EXPOSÉ :

Le fossé de la cyber-résilience dans le secteur public

COHESITY

Les cyberattaques ne sont plus des événements isolés, mais une caractéristique inhérente à notre monde numérique. Chaque jour le confirme : à l'échelle mondiale, les entreprises du secteur public sont de plus en plus fréquemment prises pour cible. Aucune entreprise n'est à l'abri. La fréquence et la sophistication croissantes des menaces ont entraîné une augmentation du nombre de cyberattaques graves qui causent des dommages mesurables sur le plan financier, opérationnel et en termes de réputation.

UNE ENQUÊTE MONDIALE MENÉE AUPRÈS DE 399 DÉCIDEURS DANS LE DOMAINE DES OPÉRATIONS INFORMATIQUES D'ENTREPRISES DU SECTEUR PUBLIC RÉVÈLE LA RÉALITÉ.

67 %
des entreprises ont été victimes d'une cyberattaque significative

49 %
ont été touchés au cours des 12 derniers mois

1 SUR 4
1 entreprise sur 4 a été attaquée à plusieurs reprises

LES DOMMAGES SONT CONSIDÉRABLES ET **LES COÛTS S'ACCUMULENT RAPIDEMENT**

85 %
ont perdu des revenus

42 %
ont perdu des clients

61 %
des entreprises cotées en bourse ont dû revoir leurs prévisions financières

97 %
ont dû faire face à des conséquences réglementaires ou juridiques

92 %
ont payé une rançon au cours des 12 derniers mois

DE NOMBREUSES ENTREPRISES SURESTIMENT LEUR RÉSILIENCE BIEN QU'ELLES AIENT DES PREUVES ÉVIDENTES QUE CE N'EST PAS LE CAS.

54 %
ont totalement confiance en leur stratégie de cyber-résilience

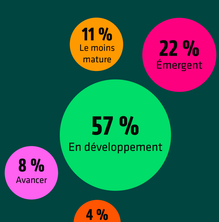
LA PLUPART D'ENTRE ELLES CONTINUENT DE PRIVILÉGIER LA PRÉVENTION ET LA DÉTECTION PLUTÔT QUE LA RÉPONSE ET LA RESTAURATION, QUI SONT TOUT AUSSI CRITIQUES.

Ordre basé sur le cadre de cybersécurité du NIST. La taille des cases indique la proportion des investissements en matière de cyber-résilience, de la plus élevée à la plus faible.

N°2	N°1	N°3	N°4	N°5
Identifier	Protéger	Détecter	Répondre	Restaurer

LA CONFIANCE ET LES HABITUDES DE CONSOMMATION **NE REFLÈTENT QU'UNE PARTIE DE LA RÉALITÉ**

La véritable résilience dépend des pratiques et des capacités qui la soutiennent. Si on l'évalue sur la base de critères de performance concrets, seules 4 % des entreprises font preuve de maturité dans cinq domaines essentiels : **la protection des données, la restauration des données, la détection et l'investigation des menaces, la résilience des applications et l'optimisation des risques liés aux données.**



La prochaine évolution nécessite de prendre conscience qu'il faut renforcer la résilience, et que celle-ci est alimentée par l'automatisation et l'IA. Les menaces sont de plus en plus rapides et complexes. L'automatisation est donc essentielle pour accélérer la détection, rationaliser la réponse et renforcer la restauration.

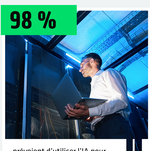
56 %

des personnes interrogées, être victime d'une cyberattaque leur a fait comprendre l'importance de mettre en place une meilleure automatisation de la détection, de la réponse et de la restauration

42 %

pensent que l'IA jouera un rôle central dans la manière dont elles détectent les menaces et y répondent, notamment en prenant certaines décisions de manière autonome

98 %



prévoient d'utiliser l'IA pour soutenir les opérations de sécurité des données d'ici 2026

ÊTES-VOUS PRÉPARÉ AUX RISQUES ?

Téléchargez le rapport sur la cyber-résilience dans le secteur public pour consulter les résultats détaillés.

Inscrivez-vous à un atelier consacré à la résilience face aux ransomwares.

Obtenez notre livre électronique **« Les 5 étapes de la cyber-résilience »** pour commencer dès aujourd'hui à améliorer votre maturité.

Vanson Bourne a interrogé 3 200 responsables informatiques et de la sécurité d'Amérique du Nord, d'Asie-Pacifique, d'Europe et d'Amérique latine, représentant des entreprises comptant 1 000 employés ou plus en 2025. Les répondants comprenaient 399 participants provenant d'entreprises du secteur public.

COHESITY VansonBourne

COHESITY
cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054
620003I-001-FR 6-2026