CSC

We are the business behind business®

Perspectives RSSI 2025

Faire face à l'évolution des menaces utilisant des noms de domaine à l'ère de l'IA et du renforcement de la réglementation cyber

Sous l'impulsion notamment de l'essor rapide de l'intelligence artificielle (IA), la diversité et l'intensité des menaces cyber qui pèsent sur les organisations continuent de s'accroître.

Les acteurs malveillants d'aujourd'hui ont accès à des méthodes de plus en plus sophistiquées, notamment les deepfakes et les algorithmes de génération de noms de domaine (DGA - Domain Generation Algorithms), ce qui représente un défi croissant pour les entreprises qui doivent les anticiper et s'en protéger. Dans le même temps, les responsables de la sécurité des systèmes d'information (RSSI) et leurs équipes doivent continuer à se prémunir contre des menaces de sécurité plus établies, telles que les attaques par déni de service distribué (DDoS). Ces incidents continuent de mettre les entreprises en danger, malgré les mesures et les efforts déployés depuis des années pour en limiter l'impact.

Au premier trimestre 2025, CSC a commandé une étude indépendante auprès de RSSI, de directeurs des systèmes d'information (DSI) et d'autres professionnels de l'informatique de haut niveau afin de mieux comprendre leurs préoccupations actuelles. Nous avons cherché à comprendre l'évolution des cybermenaces, l'état actuel des budgets consacrés à la sécurité informatique, la manière dont les professionnels de la cybersécurité font face au renforcement et à l'évolution des réglementations, et comment les équipes utilisent les politiques et les technologies de sécurité pour assurer la sécurité des organisations.

Notre étude a révélé que près des trois quarts (70%) des personnes interrogées pensent que les menaces de sécurité vont augmenter au cours de l'année à venir ; presque toutes (98%) prévoient une augmentation au cours des trois prochaines années. Près de neuf personnes sur dix (87%) estiment que les DGA basés sur l'IA constituent une menace.

Il ne fait aucun doute que les RSSI continueront à être mis au défi par les menaces de sécurité. Notre travail consiste à continuer à développer de meilleurs moyens de contrôler à la fois les risques résiduels et les nouveaux vecteurs de menaces.

NOS EXPERTS

Ihab Shraim
CTO, CSC Digital Brand Services

Nina Hrichak
Vice-Présidente Account Management EMEA, CSC Digital Brand Services

Mark Flegg
Directeur Produit Cybersécurité, CSC Digital Brand Services

Mark Eggleston
CISO, CSC

Ce que disent les RSSI: un aperçu

Nous avons interrogé 300 RSSI, DSI et responsables informatiques au premier trimestre 2025 et avons constaté que les menaces cyber constituent des risques importants qui deviennent de plus en plus difficiles à gérer.

67%

des personnes interrogées ont déclaré que les menaces liées à la cybersécurité étaient critiques ou importantes en 2024.

70%

s'attendent à une augmentation des menaces en 2025.

98%

estiment que les risques augmenteront au cours des trois prochaines années.

Les noms de domaine et le DNS domineront le paysage des menaces

Les trois principales menaces pour la sécurité en 2024 ont été citées comme suit :

1. Cybersquatting
2. Piratage de noms de domaine et de DNS
3. Attaques DDoS

4. *Rançongiciels et logiciels malveillants*
5. *Cyberattaques et diffamation sur les réseaux sociaux*
6. *Hameçonnage et ingénierie sociale*
7. *Autres*

Les trois principales menaces attendues au cours des trois prochaines années sont les suivantes :

1. Cybersquatting
2. Piratage de noms de domaine et de DNS
3. Rançongiciels et logiciels malveillants

4. *Attaques DDoS*
5. *Cyberattaques et diffamation sur les réseaux sociaux*
6. *Hameçonnage et ingénierie sociale*
7. *Autres*

Le recours à des services externalisés pour la cybersécurité est répandu mais inégal

Près de la moitié des personnes ayant répondu ont déclaré utiliser principalement des systèmes, des processus et du personnel internes, mais faire appel à des spécialistes dans une mesure limitée.

Un peu moins d'un cinquième (18%) ont recours exclusivement à des ressources internes.

18%

Près d'un tiers (30%) font appel à des spécialistes, mais utilisent également des ressources internes.

30%

L'IA aura un impact significatif sur la cybersécurité

Près de neuf personnes sur dix (87%) estiment que les DGA basés sur l'IA constituent une menace

87%

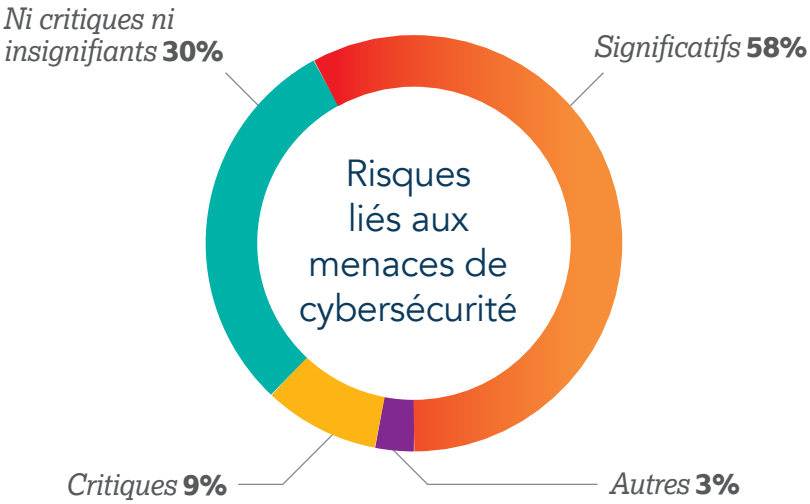
La grande majorité (97%) se dit préoccupée par le fait de donner à des systèmes tiers basés sur l'IA l'accès aux données de l'entreprise.

97%

Les cybermenaces évoluent et ne cessent de se complexifier.

Les RSSI sont confrontés à une vague croissante de cybermenaces toujours plus sophistiquées. Pire encore, ils prévoient que les défis en matière de sécurité auxquels ils sont confrontés ne feront que s'intensifier.

Près d'un répondant sur dix (9%) a déclaré que les risques liés aux menaces de cybersécurité étaient « critiques » en 2024. Les trois cinquièmes (58%) les ont jugés importants, ce qui signifie que les deux tiers (67%) ont estimé que les risques étaient importants. En outre, 30% ont déclaré que les risques n'étaient ni critiques ni insignifiants.



***"Les RSSI ont dû faire face à de longues périodes de transition, il est donc compréhensible qu'ils considèrent les risques comme très sérieux"*, explique Mark Flegg, Directeur Produit Cybersécurité, CSC Digital Brand Services.**

"Lorsque les entreprises ont commencé à migrer leurs systèmes centraux depuis leur infrastructure interne vers le cloud, elles ont exposé leurs environnements informatiques à de nouvelles menaces. Le détournement de sous-domaines, ou prise de contrôle de sous-domaines, en est un parfait exemple. Il y a 20 ans, lorsque les entreprises géraient leurs propres datacenters et confiaient rarement l'adressage IP ou le contrôle du DNS à des tiers, ce problème n'était pas aussi préoccupant. Aujourd'hui, les systèmes informatiques sont plus faciles à pénétrer et les acteurs malveillants sont à l'affût du moindre trou dans la raquette."

Les risques liés aux cybermenaces vont s'aggraver dans les mois et les années à venir, selon les personnes interrogées. Près des trois quarts (70%) s'attendent à une augmentation en 2025, 5% estimant que cette augmentation sera "significative" ; 98% s'attendent à une augmentation au cours des trois prochaines années, les deux tiers (66%) estimant qu'elle sera également significative.

L'essor des capacités de l'IA signifie que certaines menaces liées à certains noms de domaine deviennent plus importantes.

Par exemple, les cybercriminels peuvent utiliser l'IA pour rechercher à grande échelle des sous-domaines abandonnés ou mal configurés, ce qui leur permet de les pirater.

Parallèlement, les RSSI sont confrontés à un défi de taille: la plupart des menaces auxquelles ils ont toujours été confrontés continuent de poser problème, tandis que la liste des nouvelles attaques et méthodes potentielles ne cesse de s'allonger et de se complexifier.

Les cybermenaces sont de plus en plus sophistiquées et combinent souvent plusieurs techniques pour augmenter leurs chances de réussite. Beaucoup commencent par une forme d'ingénierie sociale, parfois associée à une tactique telle que les domaines similaires, comme le typosquatting, afin d'accroître leur crédibilité.

Ces attaques servent de catalyseurs, préparant le terrain pour de futures menaces.

D'autres exemples incluent le tunneling DNS pour contourner les mesures de sécurité et transmettre des logiciels malveillants à travers un réseau, ou compromettre le système d'un fournisseur tiers et utiliser cet accès pour voler des données à une entreprise.

"Nous constatons que les attaques telles que les rançongiciel(s) ne se produisent pas de manière isolée et que les acteurs malveillants peuvent ensuite voler des informations dans le cadre d'attaques hybrides ou combinées, qui peuvent s'avérer véritablement dévastatrices."

Mark Eggleston
CISO, CSC

Les menaces liées aux noms de domaine

sont au coeur des préoccupations des RSSI.

Les trois principales menaces de sécurité de l'année dernière ont été désignées par les personnes interrogées comme étant le cybersquatting, le piratage de noms de domaine et de DNS, et les attaques DDoS.

Seuls 22% ont déclaré disposer d' « outils adéquats ». Il est clair que les RSSI estiment qu'ils pourraient faire davantage pour contrer les menaces liées aux noms de domaine, et la nécessité de renforcer les ressources devient de plus en plus cruciale.

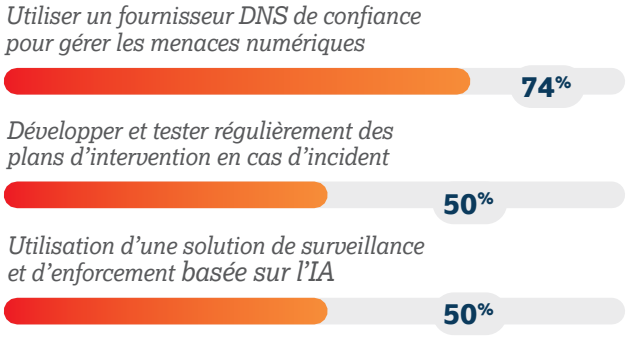
76% Les trois quarts se disent "plutôt confiants" quant à la capacité de leur entreprise à atténuer les attaques de domaine ; seuls 7% se disent "très confiants."

99% En outre, presque tous (99%) admettent être plutôt ou très préoccupés par le fait que leurs bureau d'enregistrement de noms de domaine ne respectent pas les politiques "Know Your Customer" (KYC) visant à vérifier l'identité des clients et des fournisseurs.

59% Près des trois cinquièmes (59%) ont déclaré que lorsque leur entreprise détecte des cybermenaces liées aux noms de domaine, elle dispose d'outils et de processus pour les atténuer, mais que le processus de neutralisation des menaces est complexe et prend beaucoup de temps.

Les trois quarts des personnes interrogées dans le cadre de Perspectives RSSI 2025 ont recours à un fournisseur DNS de confiance pour gérer les menaces numériques qui ciblent leur surface d'attaque externe et leurs actifs numériques.

50% ont élaboré et testent régulièrement des plans d'intervention en cas d'incident, et 50% utilisent une solution de surveillance et d'enforcement basée sur l'IA.



"L'élément humain reste à l'origine des plus grands risques de sécurité, et le maillon faible de toute entreprise est le manque de formation au sein des équipes. Le piratage de DNS et la prise de contrôle de sous-domaines sont des risques dont certaines personnes commencent seulement à prendre conscience."

Nina Hrichak
Vice-présidente Account Management EMEA, CSC Digital Brand Services

L'IA joue un rôle dans la lutte contre les cybermenaces, mais son utilisation généralisée reste préoccupante.

Il ne fait aucun doute que l'IA crée de la valeur pour les organisations du monde entier. Les RSSI et autres cadres supérieurs que nous avons interrogés ont déclaré que le retour sur investissement (ROI) le plus important de l'intégration de l'IA était l'automatisation des processus, suivie par la formation interne et l'analyse des données:

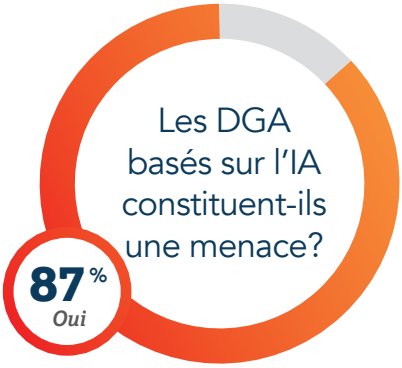
1. AUTOMATISATION DES PROCESSUS
2. FORMATION INTERNE ET FORMATION DU PERSONNEL
3. CYBERSÉCURITÉ
4. DÉTECTION DES FRAUDES
5. ANALYSE DES DONNÉES
6. RÉPONSE AUX REQUÊTES

Cependant, l'IA est clairement considérée comme une arme à double tranchant dans le monde de la sécurité, notamment parce qu'elle introduit le risque que des employés et des fournisseurs téléchargent des données sensibles vers de grands modèles linguistiques (LLM) tels que ChatGPT, et que des cybercriminels utilisent l'IA pour améliorer des outils tels que les DGA.

"L'IA peut être utilisée à bon escient, car elle nous aide à mener nos recherches plus rapidement. Elle constitue par exemple un excellent moyen d'effectuer des travaux de fond, même si personne ne devrait transmettre des documents générés par l'IA sans les faire valider par un humain en raison du risque d'erreur", explique Mark E. *"Cependant, il est également important de reconnaître que l'IA peut être utilisée pour générer de nouvelles menaces, telles que les deepfakes utilisés pour le phishing."*

Les personnes intérrogées étaient presque unanimes dans leur inquiétude quant aux risques liés à l'accès de systèmes tiers basés sur l'IA aux données de leur entreprise.

La majorité (87%) ont déclaré que les DGA alimentés par l'IA constituent une menace pour leur organisation. Les acteurs malveillants peuvent générer de grands volumes de nouveaux noms de domaine qui enfreignent la propriété intellectuelle, vendent des articles contrefaits ou soutiennent des campagnes de phishing. Les combinaisons possibles de mots-clés utilisés dans les noms de domaine sont presque infinies.



L'utilisation de l'IA aide également les criminels à élaborer et à lancer des campagnes complètes, avec des messages persuasifs, de faux sites web et des outils d'automatisation, afin d'attaquer des organisations, prévient Ihab Shraim.

"Il existe diverses plateformes basées sur l'IA qui permettent aux acteurs malveillants de lancer des campagnes ciblées contre des secteurs spécifiques, tels que les services financiers », explique Ihab Shraim. « Ces kits sont conçus pour être complets, ce qui rend les attaques plus convaincantes. Les fautes d'orthographe et de grammaire que nous voyions auparavant ont largement disparu, car l'IA est capable de produire des messages très précis et soignés."

Les organisations doivent disposer d'une politique de gouvernance claire concernant l'accès aux LLM au sein de l'organisation et les informations qui sont partagées. Cela implique notamment d'être conscient de la menace croissante que représente l'IA fantôme, c'est-à-dire l'utilisation non autorisée d'outils ou d'applications d'IA par des employés ou des fournisseurs.

AVIS D'EXPERT D'IHAB SHRAIM, CTO, CSC DIGITAL BRAND SERVICES

Pourquoi les menaces liées aux noms de domaine constituent un défi croissant ?

"Le DNS et les infrastructures liées aux noms de domaine sont des cibles faciles pour les cybercriminels, qui utilisent des vecteurs de menace spécifiques tels que le détournement de DNS ou l'usurpation de noms de domaine pour attaquer les systèmes exposés.

"Les acteurs malveillants mènent des reconnaissances approfondies, en analysant tout, des réseaux sociaux aux sites d'offres d'emploi, afin d'identifier les vulnérabilités potentielles, y compris les employés mécontents qui pourraient être susceptibles de se faire piéger par du phishing.

"Ils se concentrent sur les actifs que les organisations doivent garder accessibles au public, tels que le DNS, les sites web ou les passerelles de messagerie, ce qui facilite le lancement d'attaques précises comme le cybersquatting ou l'empoisonnement du cache DNS.

"Nous constatons déjà un volume élevé de ces attaques et nous nous attendons à ce qu'elles augmentent considérablement en 2025, à mesure que de nouveaux outils et kits d'attaque prêts à l'emploi se généralisent. "

Les cinq mesures principales d'Ihab Shraim pour établir une politique de gouvernance de l'IA

1 **Établir une politique claire en matière d'IA.** La priorité absolue pour toute organisation qui adopte l'IA est de créer une politique formelle qui soit communiquée à l'ensemble de l'entreprise.

2 **Définissez des règles explicites en matière de partage des données.** Définissez clairement les types de données que les employés peuvent et ne peuvent pas saisir dans les LLM afin de minimiser le risque d'exposition.

3 **Utilisez des environnements isolés pour les tests.** Lorsque vous testez des modèles d'IA, exécutez-les dans des environnements sécurisés et privés gérés par l'organisation, plutôt que dans le cloud, afin de garder le contrôle et de réduire les risques.

4 **Définissez des cas d'utilisation spécifiques.** Les modèles d'IA doivent être conçus avec des objectifs clairs, tels que l'automatisation d'une fonction particulière, afin d'éviter toute contamination involontaire des données.

5 **Validez les résultats de l'IA.** Aucun utilisateur de l'IA ne doit partir du principe que les données générées par l'IA sont universellement exactes : la supervision humaine reste essentielle.

"Vous pouvez contaminer tout un segment d'Internet avec des données erronées, car les informations sont répétées et renforcées par des modèles d'IA interconnectés," explique Ihab. "À l'avenir, il sera encore plus difficile pour les technologues d'effectuer des vérifications fondamentales sur les données utilisées."

Ihab Shraim
CTO, CSC Digital Brand Services

Focus sur **l'IA fantôme**

D'une certaine manière, l'IA fantôme peut être considérée comme la dernière d'une longue série de menaces de sécurité auxquelles les RSSI sont confrontés lorsque les utilisateurs finaux contournent la gouvernance informatique, comme lorsque les employés ont adopté pour la première fois des outils tels que Dropbox ou ont apporté leurs propres appareils mobiles sur leur lieu de travail sans surveillance.

D'un autre côté, elle est beaucoup plus complexe et insidieuse. Comme de nombreux outils d'IA sont basés sur le cloud et hébergés en externe, les acteurs malveillants peuvent les exploiter pour découvrir des vulnérabilités ou utiliser à mauvais escient des données utilisées involontairement par les employés. Les risques comprennent les violations de données et les manquements à la conformité si des informations sensibles sur l'entreprise ou les clients sont exposées à la suite d'une utilisation non autorisée.

Selon Mark E., la solution au problème de l'IA fantôme consiste à utiliser des agents logiciels qui suivent tous les LLM utilisés dans une organisation. *"Cela signifie que nous pouvons voir qui télécharge et transfère des informations à partir d'outils d'IA, et nous pouvons bloquer ceux qui présentent trop de risques. Vous appliquez ensuite politique de type « zéro trust », qui valide les utilisateurs et applique des contrôles, afin de vous assurer que tout le monde respecte la politique de gouvernance de l'IA de l'organisation."*

Les budgets cyber ne suivent peut-être pas le rythme de l'évolution des cybermenaces.

Bien que la cybersécurité soit considérée comme une priorité absolue par les grandes organisations, il peut encore être difficile d'obtenir les budgets nécessaires pour se protéger contre la gamme croissante de menaces et la quantité de données que les organisations doivent gérer.

"Le problème est que les dépenses en cybersécurité n'offrent pas un retour sur investissement spectaculaire," explique Mark F.

"C'est comme souscrire une assurance : tout le monde déteste payer, mais quand vient le moment de faire une déclaration, cette police est la meilleure chose qui soit. Les entreprises soucieuses de leur budget continuent de se demander si le coût de la protection est vraiment justifié."

"Il faut toujours prévoir un budget plus élevé d'une année sur l'autre," ajoute Mark F. *"Les menaces que vous gérez déjà ne disparaissent pas, vous devez donc continuer à les financer, en plus de toute nouvelle menace qui apparaît. Les RSSI ont passé beaucoup de temps à construire des pare-feu, à relever le pont-levis du château, et ils se rendent maintenant compte que des gens creusent des tunnels sous les douves."*

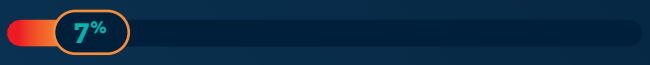
L'une des raisons de ce décalage entre les priorités du conseil d'administration en matière de cybersécurité et le financement alloué est que les décisions relatives aux risques liés à la sécurité des domaines ne sont pas toujours prises par ceux qui comprennent le mieux leur impact potentiel.

Les RSSI prennent des mesures pour combler cet écart en discutant de l'impact réel que peuvent avoir les menaces liées aux domaines, et beaucoup d'entre eux collaborent avec leurs collègues plus expérimentés afin de mieux comprendre ces menaces.

Budget global consacré à la cybersécurité et à la sécurité et la gestion des informations connexes.

Seuls 7% des répondants ont déclaré que leur budget global pour la cybersécurité et la sécurité et la gestion des informations connexes avait augmenté de manière significative entre 2024 et 2025, tandis que la majorité (80%) ont déclaré que leur budget avait augmenté modérément.

Augmentation significative entre 2024 et 2025



Augmentation modérée

Qui est responsable de la répartition des budgets consacrés à la cybersécurité?

La répartition est le plus souvent décidée par le directeur des risques (CRO) ou les équipes de gestion des risques (23%), le directeur financier (CFO) ou l'équipe financière (21%), ou par le RSSI ou l'équipe informatique (18%).

Les cinq principaux sujets abordés par les RSSI avec les autres divisions en matière de risques numériques sont classés comme suit :

1. RÉPUTATION ET PERTES FINANCIÈRES
2. CYBERSÉCURITÉ ET PROTECTION DES DONNÉES
3. PLANIFICATION STRATÉGIQUE ET OBJECTIFS COMMERCIAUX
4. BUDGÉTISATION ET ALLOCATION DES RESSOURCES
5. CONFORMITÉ ET GESTION DES RISQUES

"Il est bon de voir les RSSI se concentrer sur la réputation et les risques financiers plutôt que la conformité, qui est généralement la partie la plus facile de votre stratégie de cybersécurité", explique **Mark E.** *"La plupart des RSSI savent comment gérer la conformité, mais c'est l'atteinte à la réputation qui nous empêche de dormir la nuit."*

Pourquoi les budgets consacrés à la sécurité des noms de domaine sont parfois négligés ?

***"De nombreuses entreprises considèrent encore les noms de domaine comme un simple poste budgétaire lié à la marque, et cette mentalité doit évoluer vers la sécurité"*, explique *Nina*.**

"Il y a deux choses à garder à l'esprit lorsqu'il s'agit du portefeuille de noms de domaine d'une entreprise", observe-t-elle. *"Premièrement, l'enregistrement d'un nom de domaine est relativement peu coûteux. Deuxièmement, dans de nombreuses juridictions, il existe peu ou pas de règles relatives à l'enregistrement. Il est donc extrêmement important de sécuriser votre marque par l'enregistrement de noms de domaine, non seulement sur vos marchés principaux, mais aussi dans les extensions de noms de domaine à haut risque.*

"C'est pourquoi il convient de consacrer un budget plus important à la sécurité des noms de domaine. Dans les entreprises où les RSSI n'ont pas une vision claire de la manière dont les actifs numériques sont gérés, et où la responsabilité incombe à une personne moins sensibilisée à la sécurité, des mesures critiques et rentables telles que le Registry Lock peuvent être négligées.

"Il n'existe pas d'approche universelle. Les entreprises peuvent adopter une stratégie défensive en enregistrant un large éventail de noms de domaine, ou une approche plus légère en surveillant les violations et en prenant des mesures si nécessaire."

La conformité à la directive NIS2 reste **un travail en cours pour de nombreuses organisations**

La conformité réglementaire est un défi permanent pour les RSSI. La non-conformité à des initiatives telles que la directive NIS2 et le RGPD entraîne de lourdes amendes et un risque d'atteinte à la réputation.

Malgré cela, les entreprises ont peut-être mis la NIS2 en veilleuse, estimant qu'elle ne s'applique pas à elles ou parce que différents pays de l'Union européenne (UE) ont tardé à mettre en œuvre leur variante régionale de la nouvelle loi.

Ce retard pourrait expliquer pourquoi les personnes interrogées ont classé les cadres réglementaires suivants en fonction du niveau de difficulté qu'ils présentent pour traiter des risques spécifiques en matière de cybersécurité et de sécurité de l'information:

1. NIS2 ***(Europe)***

2. RGPD ***(Europe)***

3. Cybersecurity Maturity Model Certification ***(États-Unis)***

4. Organisation internationale de normalisation, Commission électrotechnique internationale (ISO/IEC) 27001/2 ***(Global)***

5. Payment Card Industry Data Security Standard ***(États-Unis)***

6. Protection des infrastructures critiques (CIP) Normes ***(États-Unis)***

7. Digital Operational Resilience Act (DORA) ***(Europe)***

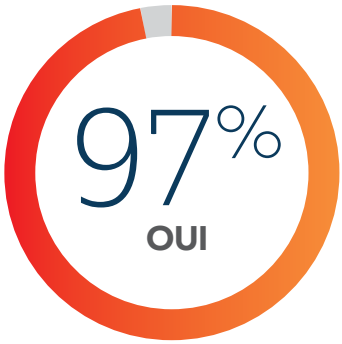
"Certains pays suivront la directive à la lettre, tandis que d'autres l'adapteront comme ils le jugent bon", explique **Mark F.** *"Pour l'instant, tout ce que nous pouvons faire, c'est trouver les points communs entre les différentes manières dont les pays ont mis en œuvre la NIS2 jusqu'à présent."*

Seuls 9% déclarent que leur organisation est entièrement conforme à la directive NIS2. Les principaux défis sont considérés comme étant la garantie de la conformité des partenaires externes (cité par 73%) et la difficulté à comprendre et à mettre en œuvre correctement les réglementations complexes (64%).

Cela fait écho aux conclusions précédentes de ce rapport, selon lesquelles les personnes interrogées s'inquiètent du fait que leurs partenaires ne procèdent pas à des vérifications KYC auprès des fournisseurs et autres tiers, une pratique qui pourrait avoir un impact sur la sécurité de la chaîne d'approvisionnement d'une organisation.

"À notre avis, la raison pour laquelle la NIS2 arrive en tête est qu'il s'agit de la norme la plus urgente à mettre en œuvre à l'heure actuelle", explique Nina. *"Nous traversons une période similaire à celle de la mise en œuvre du RGPD, où tout le monde sait qu'il faut agir, mais personne ne sait vraiment par où commencer. Par ailleurs, la norme ISO/IEC 27001/2 existe depuis beaucoup plus longtemps, et le processus de certification est très intense."*

Pensez-vous que le volume des audits de sécurité et des exigences réglementaires et de conformité auxquels votre entreprise sera confrontée au cours des trois prochaines années va augmenter ?



Se préparer à une augmentation des audits de sécurité

Mark E. note que l'augmentation des exigences réglementaires auxquelles les entreprises sont désormais confrontées est en partie due au fait que les juridictions affichent la même tendance en matière de réglementation de l'IA qu'elles avaient auparavant avec les lois sur la confidentialité des données, ce qui favorise le développement de leurs propres cadres.

La manière de gérer cela consiste à cartographier toutes les données relatives à la réglementation, qu'il s'agisse de confidentialité, d'IA ou autre, dans un cadre de contrôle". **Mark** explique que *"lorsque les RSSI procèdent à un audit, ils peuvent certifier la conformité à toutes les normes ; s'ils « auditent une fois et certifient plusieurs fois », cela réduit considérablement l'effort requis.*

"Les RSSI doivent s'assurer qu'ils disposent d'un programme efficace de gouvernance, de gestion des risques et de conformité, et que celui-ci applique toutes ces exigences à un cadre commun et qu'ils utilisent l'automatisation pour auditer et maintenir le contrôle".

L'externalisation stratégique aide les RSSI à gérer la complexité à grande échelle.

La plupart des RSSI et des organisations pour lesquelles ils travaillent reconnaissent la valeur de l'externalisation pour détecter, gérer et prévenir les cyberattaques.

48%

ont déclaré utiliser principalement des systèmes, des processus et du personnel internes

30%

ont principalement recours à l'externalisation auprès de spécialistes

Tout garder en interne

18%

Tout externaliser

4%

La réalité est que la plupart des équipes informatiques et cyber ne peuvent pas tout maîtriser. L'externalisation permet de combler des lacunes critiques, en particulier dans les domaines qui nécessitent une surveillance constante, une expertise approfondie ou une échelle dépassant les capacités internes

La détection et la réponse aux enregistrements de noms de domaine faits par des tiers sont un exemple où les partenaires externes peuvent apporter une réelle valeur ajoutée. De nouveaux noms de domaine sont enregistrés en permanence, et ce avec une relative facilité, ce qui rend la tâche presque impossible pour les équipes internes seules. Les pics d'enregistrements surviennent souvent en réponse à des événements réels, lancements de produits ou annonces publiques, et le suivi de ces tendances peut révéler des menaces émergentes ou des signaux du marché qui vont au-delà de la surveillance traditionnelle de la marque. Un fournisseur expérimenté peut fournir une surveillance automatisée pour analyser à grande échelle et identifier les tendances qui offrent une veille stratégique plus large, et pas seulement les violations potentielles.

Cependant, la surveillance automatisée n'est qu'un début. Les experts humains sont essentiels pour interpréter les résultats et orienter les décisions, par exemple pour déterminer s'il convient d'enregistrer un nom de domaine à titre préventif ou d'engager une procédure de takedown. Toutes les organisations ne disposent pas de personnel ayant une connaissance approfondie des activités liées aux noms de domaine ou du contexte dans lequel ils s'inscrivent. Le fait de pouvoir compter sur un partenaire qui suit de près l'évolution de la situation apporte donc un éclairage et une agilité essentiels.

> *"Un partenaire expérimenté peut vous accompagner tout au long de l'évolution des différents risques liés à la cybersécurité. Ce que nous observons aujourd'hui ne signifie pas que nous verrons les mêmes tendances dans quelques mois. Il se peut que quelque chose de nouveau apparaisse, et vous devez simplement garder une longueur d'avance."*
>
> **Nina Hrichak**
> *Vice-présidente Account Management EMEA, CSC Digital Brand Services*

Plus d'informations de nos experts

Un partenariat pour plus de simplicité : Gérer la sécurité des noms de domaine et du DNS en un seul endroit

"Lorsque l'on envisage de travailler avec un partenaire d'externalisation pour la sécurité des noms de domaine et des DNS, il est important d'établir une stratégie en fonction du secteur d'activité de l'organisation, de la structure de son portefeuille d'actifs numériques, de son budget et de sa tolérance au risque", explique ***Nina***.

"Cela implique de choisir le bon fournisseur, un seul, et non plusieurs, car le fait d'avoir de nombreux interlocuteurs différents peut entraîner des risques. Les entreprises doivent rationaliser leur stratégie afin de savoir à qui s'adresser en cas d'urgence, et ne pas avoir 10 fournisseurs différents, surtout dans une situation critique.

"Il faut également établir un partenariat de confiance et savoir que le fournisseur adoptera la même approche que l'entreprise en interne.

"Pour en revenir à l'évolution du secteur et aux vecteurs de menaces émergents, les entreprises doivent constamment repenser leur stratégie, car aucune entreprise ne peut rester immobile, sans que son domaine et son portefeuille de marques changent.

"Dans le même temps, les entreprises doivent se tenir informées de l'évolution du secteur, et c'est là encore qu'un fournisseur de confiance peut leur être d'une aide précieuse"

À quoi ressemble un programme de défense en profondeur qui soit conforme?

CSC est bien placé pour aider les entreprises dans l'écosystème de la sécurité des noms de domaine. En effet, nous fournissons une sécurité multicouche, une approche de la cybersécurité qui utilise plusieurs mesures de sécurité à différents niveaux, y compris les noms de domaine. Nous protégeons contre les menaces cyber telles que les attaques DDoS, l'usurpation et le piratage de noms de domaine, l'utilisation abusive de marques en ligne et le phishing.

"Sans sécurité des noms de domaine, votre posture de sécurité est incomplète", explique ***Ihab.*** *"Sans dispositif d'enforcement global, vous vous contentez d'informer l'entreprise qu'il y a un problème, sans avoir la capacité de le résoudre. Lorsque des noms de domaine sont compromis, les criminels peuvent rediriger les visiteurs vers des sites de phishing, usurper l'identité de marques pour vendre des contrefaçons et mettre hors service des sites Web et des opérations critiques pour l'entreprise, ce qui compromet la confiance des clients et la réputation de l'entreprise."*

Lorsque des domaines sont compromis, les criminels peuvent rediriger les visiteurs vers des sites d'hameçonnage, usurper l'identité de marques pour vendre des contrefaçons et mettre hors service des sites Web et des opérations critiques pour l'entreprise, ce qui compromet la confiance des clients et la réputation de l'entreprise.

Mark F. souligne que les noms de domaine et les DNS constituent le fondement de la présence en ligne d'une entreprise. *"Imaginez votre organisation comme une maison construite avec des cartes à jouer. La rangée du bas représente vos domaines et votre DNS, qui soutiennent toutes vos activités en ligne. Si je retire la couche inférieure de cartes, tout ce que vous avez construit au-dessus s'effondre. Votre site web, votre messagerie électronique et, si vous utilisez la voix sur IP, vos téléphones disparaissent. Les RSSI doivent se demander : "Quel est notre plan B?" au cas où cela se produirait."*

En d'autres termes, les entreprises doivent considérer la sécurité des domaines comme une partie intégrante et fondamentale de leur stratégie globale de sécurité, car si cette partie échoue, c'est toute la structure qui est menacée.

Conclusion

Les RSSI sont chargés de l'une des tâches les plus difficiles dans le monde de l'entreprise : assurer la sécurité des données de leur organisation et se conformer à des réglementations de plus en plus complexes. Les cybermenaces sont de plus en plus nombreuses et sophistiquées, notamment celles visant les noms de domaine et les DNS.

L'IA a des applications précieuses dans le domaine de la sécurité, mais elle permet également l'émergence d'une nouvelle vague de méthodes sophistiquées conçues pour semer le chaos dans les organisations qui ne disposent pas d'une protection adéquate.

Malgré ces défis, notre premier rapport Perspectives RSSI 2025 a révélé que les budgets consacrés à la sécurité informatique n'augmentent que modestement d'une année sur l'autre pour la plupart des RSSI. Cela peut refléter un manque de compréhension au sein de la direction générale quant à la nature réelle des menaces les plus importantes auxquelles sont confrontées les organisations aujourd'hui.

Il est particulièrement important de veiller à ce que le personnel et les partenaires soient toujours en phase avec les programmes de gouvernance, explique Nina.

"Il suffit qu'une seule personne de votre équipe clique sur le mauvais e-mail et divulgue les mauvaises données, et il en va de même pour vos partenaires", explique Nina. *"Il suffit qu'un seul partenaire commette une erreur pour que cela entraîne de très gros problèmes..."*

Il est tout aussi important de rester agile dans un environnement où les menaces évoluent rapidement, en particulier lorsqu'il s'agit de risques liés aux domaines et à l'infrastructure numérique.

Dans ce contexte, nous encourageons les RSSI à :

- Adopter une stratégie de sécurité bien structurée et multicouche qui intègre la bonne combinaison d'outils, de processus et de compétences.
- Mettre en place un programme GRC axé en particulier sur la surveillance des utilisateurs la formation des employés et les pratiques de sécurité des données des fournisseurs.
- Collaborer avec un fournisseur fiable et avant-gardiste qui peut alléger la charge de travail des équipes internes et améliorer la résilience globale.

Pour découvrir comment CSC peut aider votre organisation à garder une longueur d'avance en matière de gestion de domaine et de cybersécurité, rendez-vous sur cscdbs.com/fr.

"Il y a une raison pour laquelle nous sommes obligés de changer fréquemment nos mots de passe : plus ils restent longtemps en circulation, plus quelqu'un a de chances de les pirater", conclut **Mark F.** *"Il en va de même pour toute violation ou tout détournement, ou pour tout site web frauduleux. Plus il reste longtemps en circulation, plus son impact sera important. Ce n'est pas facile à gérer, mais il faut garder une longueur d'avance."*

Aperçu de nos **participants à l'enquête**

Secteurs d'activité

- **19%** *Institutions financières*
- **18%** *Santé et assurance*
- **17%** *Commerce de détail et produits de consommation*
- **16%** *echnologies, médias et télécommunications*
- **11%** *Biens industriels, énergie et services publics*
- **20%** *Tous les autres*

Fonction des répondants

Responsable de la sécurité des systèmes d'information **60%**

Directeur des Systèmes d'Information **13%**

Directeur Cybersécurité et Responsable Cybersécurité **11%**

Directeur de la technologie (CTO) **8%**

Responsable informatique (ou équivalent) **8%**

Sièges sociaux des entreprises par région

33%
Europe

33%
Amérique du Nord

33%
Asie-Pacifique

Discutons +33 1 40 41 65 30 | cscdbs.com/fr

À propos de CSC

CSC est le partenaire de confiance des entreprises du classement Forbes Global 2000 (Interbrand®) et 100 Best Global Brands en matière de sécurité et de veille sur les menaces et propose des solutions de gestion de la sécurité des domaines et, de protection des marques en ligne et contre la fraude. Les entreprises internationales investissent considérablement dans leur stratégie de sécurité. C'est la raison pour laquelle notre plateforme DomainSecSM peut les aider à identifier leurs failles en matière de cybersécurité et leur permettre de protéger leurs actifs numériques et leur marque en ligne. En s'appuyant sur la technologie exclusive de CSC, les entreprises peuvent consolider leur stratégie de sécurité pour se protéger contre les vecteurs de cybermenaces qui pèsent sur leur patrimoine numérique, et éviter les pertes de revenus catastrophiques et les atteintes à la réputation de leur marque.

CSC propose également une protection de la marque en ligne (une combinaison de la surveillance de la marque en ligne et des activités de mise en œuvre) et une vue multidimensionnelle des différentes menaces à l'extérieur du pare-feu ciblant des noms de domaine spécifiques. Des services de protection contre la fraude, qui luttent contre l'hameçonnage dès les premiers stades de l'attaque, viennent compléter nos solutions.

Basée à Wilmington (Delaware) aux États-Unis depuis 1899, CSC possède des bureaux sur tout le territoire des États-Unis, mais également au Canada, en Europe et dans la région Asie-Pacifique. CSC est une entreprise d'envergure mondiale, ce qui nous permet d'intervenir là où sont nos clients en mettant à leur disposition nos équipes d'experts dans chacune de nos activités.

Copyright ©2025 Corporation Service Company. Tous droits réservés.

DBS09082025

Ce document est fourni par CSC à titre informatif uniquement et ne constitue ni une offre, ni une invitation, ni une incitation à conclure un contrat. Les informations contenues dans le présent document ne constituent pas des conseils juridiques, fiscaux, réglementaires, comptables ou autres conseils professionnels. Il convient donc de consulter un professionnel compétent avant d'envisager une transaction telle que décrite dans le présent document. Nous déclinons toute responsabilité pour toute perte directe ou indirecte résultant de l'utilisation du présent document.