GlobalData.

AUTOMNE 2023

# Cybersécurité en Europe

PARRAINÉ PAR

TANIUM

# Contenu

# Introduction

**Le paysage de la cybersécurité en Europe est aussi divers que les 44 pays qui la forment.** Leurs perspectives en matière de cybersécurité reflètent l'impact de multiples facteurs, notamment des attitudes variables en termes de risque, confidentialité et sécurité dans chaque pays, ainsi que dans les organisations clés qui opèrent au niveau national ou régional. Il en résulte des réglementations diverses, spécifiques à chaque pays, et qui varient en termes de portée, d'exigences et de mise en œuvre.

En outre, les principales industries en Europe ont des exigences uniques en matière de cybersécurité, en fonction de la nature de leurs opérations et de la sensibilité des données qu'elles traitent. La diversité de l'infrastructure technologique et des niveaux de maturité numérique des secteurs influence également la complexité et l'efficacité des systèmes de cybersécurité, à un moment où le nombre et la complexité des attaques augmentent.

Ce document illustre les actions que vous pouvez prendre pour prévenir ces attaques. Il présente l'étendue des défis auxquels se mesurent les entreprises européennes et prend en compte l'impact de la situation réglementaire et des exigences de conformité. Il examine également l'évolution du paysage de la cybersécurité et ses implications pour les entreprises.

Il comprend plusieurs exemples de la manière dont les organisations ont amélioré leur position préventive et relevé les défis auxquels elles étaient confrontées en matière de cybersécurité. Il présente les mesures prises par les entreprises pour obtenir, ou regagner, la visibilité, le contrôle et la planification nécessaires pour être en mesure **a)** d'anticiper, et **b)** de réagir correctement et efficacement afin de répondre de rester résilientes face aux attaques. Enfin, il décrit des recommandations destinées à permettre aux organisations d'atteindre ces objectifs.

ZAC WARREN

CONSEILLER PRINCIPAL EN MATIÈRE DE SÉCURITÉ, EMEA, TANIUM

*« Le paysage de la cybersécurité en Europe est indéniablement complexe et diversifié, mais je suis fermement convaincu qu'il existe des mesures simples et réalisables que les organisations peuvent prendre pour renforcer leurs mesures préventives et se protéger contre les attaques potentielles. Ce document offre des informations précieuses sur les principaux défis auxquels les entreprises européennes sont confrontées et fournit des exemples concrets de la manière dont les organisations renforcent avec succès leurs défenses en matière de cybersécurité. »*

# L'étendue des défis auxquels se mesurent les entreprises européennes

**Partout dans le monde, 2023 a été une année difficile pour ceux qui tentent de garder une longueur d'avance sur les cyberattaques.** Bien qu'il existe une tendance mondiale vers un nombre croissant et une sophistication toujours plus grande des cyberattaques, certains facteurs spécifiques affectent le marché européen.

Parmi ces derniers, on compte notamment l'invasion russe de l'Ukraine, qui a augmenté la tension géopolitique dans la région et mobilisé davantage de groupes parrainés par l'État, ainsi que la nécessité pour de nombreuses entreprises et institutions établies de passer par une transformation numérique et de gérer la transition depuis les systèmes existants.

Le sombre tableau montre que les dépenses consacrées à la cybersécurité augmentent, car les violations coûtent plus cher, et les organisations doivent par conséquent prendre des mesures préventives pour les contrer. Selon le rapport IBM Cost of a Data Breach (Coûts d'une violation de données) pour 2023, le coût moyen d'une violation de données en Europe est de 4,38 millions EUR en Allemagne, de 3,95 millions EUR au Royaume-Uni, de 3,82 millions EUR en France et de 3,62 millions EUR en Italie. Seuls le Canada, le Moyen-Orient et les États-Unis font l'objet de coûts supérieurs à ceux de l'Allemagne.

Les organisations européennes victimes de cyberattaques de grande envergure comprennent le Royal Mail (Royaume-Uni), le fournisseur de logiciels Nebu (Pays-Bas), la société de lunettes Luxottica (Italie), le fournisseur de logiciels gouvernementaux Xplain (Suisse) et British Airways, Boots et la BBC (Royaume-Uni). Nous constatons des violations dans tous les secteurs, des compagnies aériennes à la vente au détail, en passant par les services bancaires et la production industrielle. Et le rythme des attaques ne cesse d'augmenter.

En conséquence, le marché européen de la cybersécurité évolue pour suivre la tendance de la transformation numérique qui est évidente dans toute la région. Selon GlobalData, le marché européen de la cybersécurité valait 31,2 milliards EUR en 2022, contre 146,3 milliards EUR à l'échelle mondiale. D'ici 2026, les revenus de la sécurité mondiale atteindront 217,5 milliards EUR, dont 45,6 milliards EUR pour l'Europe à elle seule.

En Europe, les services de sécurité gérés constitueront le segment le plus important des différents produits et services en 2026. L'augmentation des revenus connaîtra un taux de croissance annuel composé (TCAC) de 8,2 % entre 2022 et 2026, atteignant 18,7 milliards EUR en 2026 (soit environ 41 % du marché européen). La gestion des identités et des accès arrivera loin derrière au second rang, avec une part de revenus de 9 %, suivie par les plateformes de sécurité des endpoints. La prévention de la fraude et la sécurité transactionnelle seront le segment qui connaîtra la croissance la plus rapide, avec un TCAC de 13 % entre 2022 et 2026.

Les trois principaux secteurs qui stimulent la croissance du marché de la cybersécurité en Europe sont la production industrielle, les technologies de l'information (TI) et la vente au détail. Comme illustré par le tableau ci-dessous, les revenus du marché de la cybersécurité augmentent dans les secteurs de la production industrielle, des technologies de l'information et de la vente au détail, ainsi que dans l'assurance. Au Royaume-Uni, les revenus de la cybersécurité dans le secteur de la production industrielle devraient passer de 340 millions EUR en 2022 à 457 millions EUR en 2026. Dans le secteur de la vente au détail, cette augmentation passera de 311 millions EUR à 403 millions EUR, et dans l'assurance, de 207 millions EUR à 293 millions EUR. En Allemagne, le chiffre d'affaires de la cybersécurité dans le secteur manufacturier passera de 870 millions EUR en 2022 à 1,1 milliards EUR en 2026. Dans le secteur informatique, la hausse est passée de 383 millions EUR à 676 millions EUR, et dans le commerce de détail de 292 millions EUR à 417 millions EUR. Les revenus pour la France, l'Irlande, les Pays-Bas et l'Espagne suivent une trajectoire à la hausse similaire.

Les investissements publics dans la cybersécurité au sein de l'UE ont été fragmentés et souvent mal soutenus par des initiatives menées par le gouvernement. (Veuillez consulter la section Conformité pour plus de détails sur les mesures réglementaires). Étant donné que l'investissement en cybersécurité est réparti sur plusieurs catégories budgétaires (recherche et développement, défense, numérisation, informatique, etc.), il est difficile d'estimer des chiffres précis, mais les dépenses publiques de l'UE en matière de cybersécurité sont comprises entre 1 et 2 milliards d'euros par an, selon le rapport de la *Plateforme européenne d'investissement dans la cybersécurité* de la Banque européenne d'investissement.

## La production industrielle, les technologies de l'information (TI) et la vente au détail sont les moteurs clés de la cybersécurité en Europe

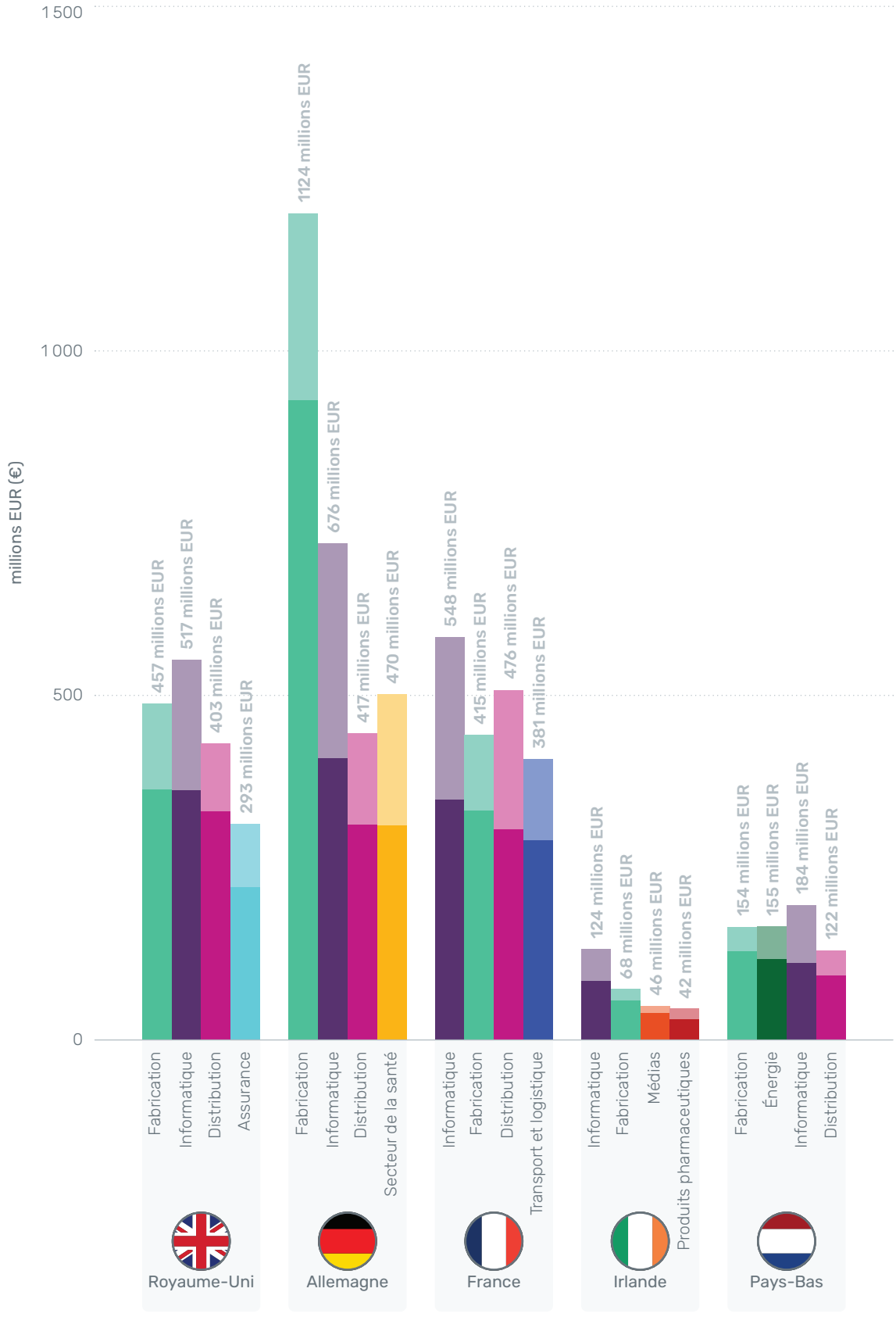
Les revenus du marché de la cybersécurité en 2022 et 2026 sont générés par les cinq principaux secteurs d'activité dans certains pays européens

**Principales**

valeurs projetées affichées pour 2026 en EUR

Couleurs unies = 2022

Couleurs teintées = 2026




Source :

GlobalData

Remarque :

Le segment « Autres » comprend l'agriculture, les arts et divertissements, les loisirs, la vente en gros, les services professionnels et commerciaux, la construction et l'ingénierie, les services liés aux TIC, les services divers et l'immobilier et la location.

L'Allemagne et la France devraient conserver leurs positions de leader sur le marché de la cybersécurité de l'UE, suivies de l'Italie, de l'Espagne, de la Pologne et des Pays-Bas. En outre, la France et l'Allemagne sont les pays qui dépensent le plus en matière de cybersécurité en Europe. Avant le Brexit, le Royaume-Uni était le plus gros investisseur européen en matière de cybersécurité, à la fois en termes de volume total d'investissements et en termes de nombre d'entreprises, selon le rapport de la *Plateforme européenne d'investissement dans la cybersécurité*.

Comme le montre le tableau ci-dessous, par chiffre d'affaires, l'Allemagne, le Royaume-Uni et la France continueront d'être les plus grands marchés de la cybersécurité en Europe d'ici 2026.

L'Allemagne, suivie du Royaume-Uni et de la France, sera à la tête du marché européen de la cybersécurité d'ici 2026

**ALLEMAGNE**

2022 : 5,3 milliards EUR

2026 : 8,4 milliards EUR

**ROYAUME-UNI**

2022 : 4,9 milliards EUR

2026 : 6,9 milliards EUR

**FRANCE**

2022 : 4,4 milliards EUR

2026 : 6,6 milliards EUR

**PAYS-BAS**

2022 : 1,4 milliards EUR

2026 : 2,1 milliards EUR

**BELGIQUE**

2022 : 842 millions EUR

2026 : 1,3 milliards EUR

**IRLANDE**

2022 : 579 millions EUR

2026 : 798 millions EUR

Source : GlobalData

## Anticiper et persévérer au lieu de juste répondre

La problématique majeure pour les entreprises de premier plan en Europe ne se cantonne pas à l'évitement des cybermenaces, qu'elles surviennent par le biais d'attaques d'hameçonnage, de piratages de la chaîne logistique ou de manipulations sociales, mais réside dans la nécessité de développer une résilience permettant une récupération post-attaques. Prendre des mesures pour vous défendre contre une cyberattaque ne garantit pas qu'elle ne se produira pas (bien que cela aidera), mais vous pouvez également mettre en place des mesures pour être aussi résilient que possible et vous donner la meilleure chance de vous rétablir après une cyberattaque.

Cela sera plus facile si, en tant qu'organisation, vous avez investi dans la cybersécurité. C'est loin d'être toujours le cas. Trop souvent, les professionnels de la sécurité estiment que leur travail est ignoré ou négligé jusqu'à ce qu'il soit trop tard. Selon une enquête de Tanium menée en 2022 *et intitulée « Cybersecurity : Prevention is better than the cure » (Cybersécurité : mieux vaut prévenir que guérir)*, près des deux tiers des personnes interrogées (65 %) s'accordent à dire que les équipes informatiques et de sécurité pensent qu'un incident doit se produire avant qu'elles ne reçoivent des investissements plus élevés pour la cybersécurité.

Une caractéristique courante des organisations en croissance est la valeur qu'elles accordent à la réactivité après une attaque. Elles tendent à accorder moins d'importance à la résilience, une qualité moins prestigieuse, qui a tendance à rester sous les radars jusqu'à ce qu'elle soit nécessaire. L'analyse menée par Tanium en 2022 a montré qu'il fallait parfois qu'une cyberattaque se produise avant que les équipes de direction n'approuvent un budget de cybersécurité plus important ; 77 % des organisations ayant subi une cyberattaque/violation de données au cours des 6 derniers mois s'accordent sur le fait que « le leadership de mon organisation ne s'intéresse à la cybersécurité que suite à un incident de cybersécurité ».

**79 %** **Parmi les professionnels interrogés, huit sur 10 (79 %) ont déclaré qu'un budget de cybersécurité plus important serait probablement attribué à la suite d'une violation de données, plutôt qu'avant qu'une violation ne se produise.** Cela revient à agir après les faits. On doit en conclure que certains dirigeants n'apprécient toujours pas à sa pleine mesure le rôle préventif que joue la cybersécurité dans la protection de l'entreprise. Lorsque les bons outils ne sont pas en place, les organisations manquent de visibilité, de contrôle et de planification pour pouvoir **a)** prévenir une attaque et **b)** y réagir correctement.

**32 %** **Moins d'un tiers (seulement 32 %) des entreprises européennes ont une stratégie de cybersécurité.** Le rapport a révélé que 52 % des personnes interrogées en Europe ont signalé avoir subi un incident de cybersécurité en 2022. Les incidents ont coûté au moins 468 567 EUR ou plus à 32 % des organisations européennes concernées. Sur une note plus positive, 81 % des organisations européennes ont indiqué qu'elles prévoyaient d'augmenter leur budget de cybersécurité d'au moins 10 % au cours des 12 prochains mois.

**< 10** **% Dans la plupart des pays européens, moins de 10 % des entreprises sont jugées comme étant suffisamment préparées pour traiter les problèmes de cybersécurité actuels.** Le Royaume-Uni et l'Allemagne font exception, avec 17 % et 11 % respectivement des entreprises ayant un état de préparation à pleine maturité, selon l'indice de préparation à la cybersécurité de Cisco. Seules 9 % des entreprises européennes ont le niveau de préparation « mature » nécessaire pour résister aux cyberrisques, explique le rapport. Au niveau mondial, 15 % des entreprises sont à un stade mature.

**Bien que la cybersécurité soit devenue un problème mondial, les besoins des clients sont extrêmement variés.** Par exemple, les services bancaires, d'assurance et financiers, où les transactions sont principalement numériques aujourd'hui, investissent largement depuis longtemps pour défendre leurs systèmes. En revanche, dans les secteurs de la production industrielle, de la vente au détail et de la santé, la révolution numérique ne fait que commencer. Par conséquent, dans ces secteurs, les vulnérabilités sont déjà exploitées par les attaquants lorsque les mises à niveau de sécurité des systèmes existants ne sont pas mises en œuvre dans l'ensemble de la chaîne de valeur.

Ayant reconnu ces menaces en constante évolution, certaines entreprises adoptent des outils tels que des pare-feux et le cryptage des données pour protéger leurs systèmes informatiques. Pour se préparer aux attaques, elles développent leur expertise par le biais de simulations de crise et de plans de communication. En outre, elles doivent se concentrer stratégiquement et investir dans des outils de détection précoce et de réponse rapide afin d'être résilientes face aux cyberattaques potentielles.

# Conformité et réglementation

**La fréquence croissante et la nature multidimensionnelle des cybermenaces remettent en question le statu quo.** Toute organisation qui ne se conforme pas aux réglementations spécifiques de son secteur présente un risque élevé de violation de la cybersécurité. Le non-respect des réglementations peut entraîner d'autres conséquences, notamment des sanctions légales, une atteinte à la réputation de l'entreprise et une perte de confiance des tiers. Le besoin de conformité en matière de cybersécurité est désormais reconnu par les gouvernements du monde entier, y compris l'Union européenne (UE).

Aucune entreprise ne peut être totalement à l'abri des cyberattaques. La plupart des organisations connaissent des risques. Le facteur clé de la cybersécurité est la résilience de l'entreprise face à ces cyberattaques.

Au niveau national, le Royaume-Uni a introduit une obligation de signalement obligatoire pour les prestataires de services gérés, qui doivent divulguer les incidents de cybersécurité. Le gouvernement a également introduit une exigence de sécurité minimale, qui pourrait voir les prestataires de services gérés condamnés à une amende de 17 millions GBP (18,7 millions EUR) pour non-conformité.

Veuillez consulter les réglementations de l'UE et du gouvernement national ci-dessous et les utiliser comme liste de contrôle pour la conformité.

## RÉGLEMENTATIONS DE L'UE

### Une nouvelle directive de l'UE, NIS2, énonce des obligations plus strictes en matière de cybersécurité en ce qui concerne la gestion des risques, les obligations de déclaration et le partage des informations.

La directive a été officiellement adoptée en novembre 2022 et les États membres ont jusqu'au 17 octobre 2024 pour transposer ses mesures dans le droit national. La directive introduira de nouvelles règles dans les États membres de l'UE pour améliorer la sécurité des réseaux et des systèmes d'information. Les États membres sont tenus de respecter des mesures de surveillance et d'application plus strictes et d'harmoniser leurs sanctions. Les exigences comprennent les réponses aux incidents, la sécurité de la chaîne d'approvisionnement, le cryptage et la divulgation des vulnérabilités, entre autres dispositions. La directive établit également un cadre pour une meilleure coopération et un meilleur partage des informations entre les autorités et les États membres et crée une base de données européenne sur les vulnérabilités. La directive européenne initiale sur la cybersécurité a été mise en place en 2017, mais les pays de l'Union européenne l'ont mise en œuvre de différentes façons, donnant lieu à des niveaux de cybersécurité insuffisants.

## INFRASTRUCTURE NATIONALE CRITIQUE

### Chaque pays européen disposera également de sa propre législation nationale critique en matière d'infrastructures.

Par exemple, en Allemagne, les infrastructures critiques (KRITIS) sont des organisations et des installations d'une importance majeure pour la société, dont la défaillance ou la déficience entraînerait une pénurie durable des fournitures, des perturbations significatives de l'ordre public, de la sûreté et de la sécurité ou d'autres conséquences considérables. Elles comprennent les technologies de l'information et les télécommunications.

## LOIS EUROPÉENNES SUR LA CYBERSÉCURITÉ 2019 ET 2023

**La loi européenne sur la cybersécurité de 2019 présentait un cadre de certification de la cybersécurité pour les produits, services et processus TIC pour les pays de l'UE.**

Les entreprises qui mènent leurs activités dans l'UE doivent certifier une fois leurs produits, processus et services TIC pour obtenir un certificat reconnu dans l'UE. En avril 2023, une proposition d'amendement a été annoncée, destinée à élargir le programme de certification pour inclure les services de sécurité gérés couvrant des domaines tels que la réponse aux incidents, les tests de pénétration, les audits de sécurité et les activités de conseil. En avril 2023, la Commission européenne a proposé la loi sur la cybersolidarité de l'UE, afin d'améliorer la préparation, la détection et la réponse aux incidents de cybersécurité dans l'UE. Cette loi comprenait la création d'un bouclier européen de cybersécurité et d'un mécanisme d'urgence en matière de cybersécurité.

## LOI SUR LA RÉSILIENCE OPÉRATIONNELLE NUMÉRIQUE (DIGITAL OPERATIONAL RESILIENCE ACT, OU DORA)

**Les autorités de contrôle européennes ont conclu une consultation publique sur un ensemble initial de produits stratégiques en vertu de la loi Digital Operational Resilience Act (DORA).**

La Loi vise à assurer un cadre juridique cohérent et harmonisé dans les domaines de la gestion des risques liés aux TIC, du signalement des incidents majeurs liés aux TIC et de la gestion des risques liés aux TIC tiers. La loi DORA, qui est entrée en vigueur le 16 janvier 2023 et s'appliquera à partir du 17 janvier 2025, vise à améliorer la résilience opérationnelle numérique des entités du secteur financier de l'UE et à harmoniser les exigences clés de résilience opérationnelle numérique pour toutes les entités financières de l'UE. Elle couvre des domaines tels que la gestion des risques liés aux TIC, la gestion et le signalement des incidents liés aux TIC, les tests de résilience opérationnelle numérique et la gestion des risques liés aux TIC tiers.

## PROJET DE LOI DE SÉCURITÉ EN LIGNE

**Ce projet de loi a été proposé dans le but de rendre Internet plus sûr pour les enfants.**

L'objectif était de réduire la possibilité que les enfants soient exposés à du contenu nocif et inapproprié pour leur âge, y compris du harcèlement en ligne, ainsi que du contenu qui glorifie le suicide, l'automutilation et les troubles alimentaires. Ce projet de loi exige que les personnes puissent filtrer le contenu répréhensible pour ne pas le voir, introduit la vérification de l'âge pour les sites pornographiques, criminalise les publicités frauduleuses et exige que les sites appliquent leurs conditions de service. Les entreprises qui ne se conforment pas à la loi pourraient être condamnées à une amende pouvant atteindre 18 millions GBP (environ 21 millions EUR) ou 10 % de leur chiffre d'affaires mondial, et voir leurs services bloqués.

## NOUVEAU RAPPORT OBLIGATOIRE POUR LES PRESTATAIRES DE SERVICES GÉRÉS (MSP)

**En 2022, le Royaume-Uni a introduit une nouvelle obligation de signalement obligatoire pour les prestataires de services gérés (MSP), qui doivent divulguer les incidents de cybersécurité.**

Le gouvernement a également introduit une exigence de sécurité minimale, qui pourrait voir les MSP condamnés à une amende de 17 millions GBP (18,7 millions EUR) pour non-conformité.

## OBLIGATIONS DE DÉCLARATION

**En avril 2023, la France a introduit une nouvelle obligation selon laquelle toutes les victimes d'une cyberattaque doivent signaler l'attaque dans les 72 heures.**

Si elles ne le font pas, elles courent le risque de se voir refuser tout remboursement en vertu de leur police d'assurance cybersécurité. L'attaque doit être signalée à la police et aux autorités judiciaires.

## LOI SUR LA SÉCURITÉ DES RÉSEAUX ET DES SYSTÈMES D'INFORMATION

**Cette loi adoptée en 2018 impose des exigences strictes aux opérateurs de services essentiels et aux prestataires de services numériques.**

Elle assure que ces fournisseurs apportent une preuve suffisante démontrant qu'ils mettent en œuvre les mesures nécessaires pour gérer les risques et protéger leurs réseaux et systèmes d'information.

## LOI SUR L'INTELLIGENCE ARTIFICIELLE DE L'UNION EUROPÉENNE (LOI SUR L'IA)

**Le 14 juin 2023, le Parlement européen a largement voté en faveur de l'adoption de la proposition de Loi sur l'intelligence artificielle de l'Union européenne (Loi sur l'IA).**

Le Royaume-Uni et l'UE adopteront des approches différentes, mais les principes fondamentaux resteront les mêmes en ce qui concerne une approche « basée sur les risques » de l'utilisation de l'IA. On ne sait pas encore comment cette législation affectera le marché européen, mais elle aura certainement un impact significatif d'ici 2024, et est à surveiller pour l'avenir.

Source :
GlobalData

# L'évolution du paysage de la cybersécurité

**L'évolution du paysage de la cybersécurité regorge de défis technologiques et commerciaux.** L'agression militaire de la Russie contre l'Ukraine a remodelé le paysage des menaces en Europe en 2022, et cela s'est poursuivi en 2023. Le conflit a mobilisé de nombreux « hacktivistes », cybercriminels et groupes parrainés par l'État.

Les méthodes typiques des cyberattaques en Europe sont les suivantes :

## Attaques par déni de service distribué

Il s'agit d'attaques empêchant les utilisateurs d'un réseau ou d'un système d'accéder aux informations, services ou autres ressources pertinents. Ces attaques peuvent être réalisées en épuisant le service et ses ressources ou en surchargeant les composants de l'infrastructure réseau. En 2022, les menaces contre la disponibilité et les rançongiciels se classaient parmi les principales menaces, un changement par rapport à 2021 où les rançongiciels étaient clairement en tête. Juillet 2022 a vu les plus grandes attaques jamais enregistrées contre un client européen.

## Extorsion

Les tactiques de rançongiciel ont évolué à mesure que les entreprises s'adaptaient aux attaques en mettant à niveau leurs protocoles de sécurité et en améliorant leurs processus de sauvegarde et de restauration. Les auteurs de menaces ont commencé à faire des informations contenues dans les fichiers des armes. La première étape des techniques d'extorsion multiples était la double extorsion, dans laquelle les auteurs des menaces exfiltraient les fichiers avant de les chiffrer. Ils augmentaient ensuite la probabilité que la rançon soit payée en menaçant de divulguer et de vendre des informations sensibles.

## Programme malveillant

Le terme « programme malveillant » désigne un logiciel malveillant conçu pour endommager, perturber ou obtenir un accès non autorisé à un appareil. Traditionnellement, des exemples de types de codes malveillants comprennent les virus, les vers, les chevaux de Troie ou d'autres entités basées sur le code qui infectent un hôte. Les logiciels espions et certaines formes de logiciels publicitaires sont également des exemples de code malveillant. Rien qu'en juin 2022, des chevaux de Troie sous forme de logiciels publicitaires ont été téléchargés environ 10 millions de fois.

## Menaces d'ingénierie sociale

Il s'agit de menaces qui tentent d'exploiter une erreur humaine ou un comportement humain pour accéder à des informations ou services. L'ingénierie sociale incite les utilisateurs à ouvrir des documents, des fichiers ou des e-mails, à visiter des sites Web ou à accorder à des personnes non autorisées l'accès aux systèmes ou aux services. Et bien que ces ruses puissent faire usage d'un abus de la technologie, elles comptent toujours sur un élément humain pour réussir. Ce paysage de menaces se compose principalement des vecteurs suivants : hameçonnage, harponnage, chasse à la baleine, hameçonnage par SMS, hameçonnage par message vocal, compromission des e-mails professionnels (BEC), fraude, usurpation d'identité et contrefaçon. 82 % des violations de données impliquaient un élément humain.

## Antivirus

Des produits de cybersécurité tels que les antivirus et les systèmes de détection des intrusions basés sur l'hôte et le réseau peuvent être utilisés, et continueront d'offrir certains avantages dans la détection des codes malveillants. Leur efficacité risque cependant d'être réduite, car il est possible que les produits ne soient pas mis à jour lorsqu'ils sont exécutés sur un système d'exploitation non pris en charge, et les signatures peuvent ne pas être configurées pour détecter les attaques ciblant des systèmes obsolètes.

## Attaques de la chaîne d'approvisionnement

Une stratégie d'attaque ciblant une organisation par le biais des vulnérabilités dans sa chaîne d'approvisionnement, et qui a le potentiel d'induire des effets en cascade. Une attaque de la chaîne d'approvisionnement cible la relation entre les organisations et leurs fournisseurs. Une attaque est considérée comme ayant un composant lié à la chaîne d'approvisionnement lorsqu'elle consiste en une combinaison d'au moins deux attaques. Pour qu'une attaque soit classée comme une attaque de la chaîne d'approvisionnement, le fournisseur et le client doivent tous deux être des cibles. SolarWinds a été l'un des premiers exemples de ce type d'attaque et a montré l'impact potentiel des attaques de la chaîne d'approvisionnement. Les attaques de la chaîne d'approvisionnement représentaient 17 % des intrusions en 2021, contre moins de 1 % en 2020. L'une des attaques les plus efficaces en juin 2023 a été une attaque de la chaîne d'approvisionnement ciblant le programme de transfert de fichiers MOVEit ; elle a touché près de 600 organisations, dont en Europe la BBC, British Airways, Boots et Aer Lingus.

## Intelligence artificielle (IA)

L'IA entretient une relation complexe avec le paysage en constante évolution de la cybersécurité. Elle constitue à la fois une menace formidable et une solution puissante. Les acteurs malveillants utilisent de plus en plus l'IA pour améliorer la sophistication et l'efficacité des cyberattaques, ce qui à son tour pousse les entreprises à l'utiliser pour améliorer leur protection. Cette situation souligne la nécessité pour les experts en cybersécurité d'améliorer continuellement leurs défenses pour suivre l'évolution rapide des menaces alimentées par l'IA. Les attaques d'ingénierie sociale basées sur l'IA peuvent manipuler les individus et diffuser la désinformation, exploitant les vulnérabilités humaines à une vitesse et à une échelle sans précédent. Pour contrer ces menaces, les algorithmes d'apprentissage automatique peuvent analyser de vastes ensembles de données en temps réel, permettant ainsi une détection beaucoup plus rapide des anomalies et des menaces.

## Attaques par rançongiciel

Au cours des dernières années, le plus grand développement en matière de cybercriminalité a été l'essor des rançongiciels et, plus récemment, de l'extorsion. Les rançongiciels chiffrent les données sur les systèmes des victimes jusqu'à ce qu'un paiement soit effectué. Étant donné que les systèmes informatiques sont désormais omniprésents, les attaques par rançongiciel peuvent être véritablement dévastatrices pour les victimes et leurs clients, c'est pourquoi elles restent la cybermenace la plus sérieuse pour les entreprises et les organisations européennes. Avec plus de 10 téraoctets de données volés chaque mois, le rançongiciel est l'une des plus grandes cybermenaces visant l'UE, et l'hameçonnage est désormais le vecteur initial le plus courant de ces attaques. On estime que jusqu'à 60 % des organisations affectées payent. Les rançongiciels ont été l'une des principales menaces en 2022 et cela s'est poursuivi en 2023, bien que les attaquants menacent désormais plus brutalement de faire des extorsions.

## Secteurs d'activité et infrastructures critiques

Les secteurs critiques tels que le transport, l'énergie, la santé et la finance, y compris l'assurance, sont de plus en plus dépendants des technologies numériques pour gérer leur activité principale. Bien que la numérisation fournisse des solutions à bon nombre des défis auxquels l'Europe est confrontée, et se soit avérée particulièrement utile pendant la crise du COVID-19, elle expose également l'économie et la société aux cybermenaces. Les infrastructures nationales critiques sont menacées, car les criminels sont prêts à tirer parti de toute vulnérabilité informatique/technologie opérationnelle (OT). Dans les systèmes industriels, y compris la production industrielle, l'énergie, le pétrole et le gaz, il existe une peur constante d'un passage des systèmes informatiques aux systèmes OT. Bien que cela se soit produit aux États-Unis, l'attaque des systèmes informatiques Colonial Pipeline qui a eu lieu en mai 2021 a été un signal d'alarme pour les gouvernements et les organisations d'infrastructures nationales critiques du monde entier, y compris en Europe. Ce piratage a été la plus grande cyberattaque divulguée publiquement contre les infrastructures critiques des États-Unis. Heureusement, les systèmes OT du pipeline qui assurent le déplacement du pétrole n'ont pas été directement compromis pendant l'attaque.

## Une nouvelle approche pour la défense contre les cyberattaques : la croissance du modèle Zero Trust

Un modèle Zero Trust fournit une protection contre les rançongiciels et les menaces de cybersécurité en attribuant l'accès minimum requis pour effectuer des tâches spécifiques. Au lieu d'estimer que tout ce qui se trouve derrière le pare-feu de l'entreprise est sûr, le modèle Zero Trust part du principe qu'il existe une violation et vérifie chaque demande comme si elle provenait d'un réseau ouvert.

Quelle que soit l'origine de la demande ou la ressource à laquelle elle accède, Zero Trust apprend aux organisations à « ne jamais faire confiance, toujours vérifier ». Chaque demande d'accès est totalement authentifiée, autorisée et cryptée avant que l'accès ne soit accordé. Zero Trust propose une solution moins sujette aux violations et offre une meilleure protection aux utilisateurs et aux données. En authentifiant et en autorisant chaque utilisateur, appareil et application, quel que soit leur emplacement, l'approche Zero Trust minimise le risque de violation de la sécurité. Mais ce n'est pas facile à mettre en œuvre.

### LES AVANTAGES D'UNE ARCHITECTURE ZERO TRUST

1. Réduit la surface d'attaque et le risque de violation des données.
2. Fournit un contrôle d'accès granulaire sur les environnements cloud et conteneur.
3. Atténue l'impact et la gravité des attaques réussies, réduisant ainsi le temps et les coûts du nettoyage.
4. Soutient les initiatives de conformité.

# Un calendrier des attaques

Décembre 2022

**ROYAUME-UNI**

Janvier 2023

Le Royal Mail a subi une attaque par rançongiciel qui a interrompu ses activités de traitement des colis. Les attaquants, un gang de rançongiciel appelé LockBit et lié à la Russie, ont exigé un important paiement de rançon en échange de la clé de décryptage. Il a fallu six semaines avant que le Royal Mail puisse redémarrer les livraisons internationales de colis et de lettres.

Février 2023

**PAYS-BAS**

Mars 2023

En mars 2023, les données personnelles d'environ deux millions de Néerlandais ont été exposées en raison d'une fuite de données dans certaines agences d'études de marché qui utilisaient des logiciels du fournisseur de logiciels d'études de marché Nebu. Les données de plusieurs organisations, dont la Fédération néerlandaise de golf (NGF), les clients du transporteur NS et du fournisseur VodafoneZiggo, ont été exposées à la suite de la violation des données.

Avril 2023

**ITALIE ET CHINE**

Mai 2023

Luxottica, l'une des plus grandes sociétés de lunettes au monde, a été la cible d'une cyberattaque. Luxottica, qui possède des marques populaires telles que Ray-Ban, Oakley et Costa, a fait l'objet de plusieurs incidents de sécurité ces dernières années. En août 2020, elle a été au centre d'une violation de données affectant plus de 800 000 patients EyeMed et Lenscrafters.

Juin 2023

**ROYAUME-UNI ET AUTRES**

Une cyberattaque de juin 2023 a touché British Airways, Boots et la BBC ; elle était le fait du gang de rançongiciel Clop, qui avait exploité un élément d'infrastructure commerciale appelé MOVEit, soit un logiciel utilisé pour transférer des fichiers en toute sécurité sur des réseaux internes. La Banque européenne d'investissement (BEI) a également été touchée par une cyberattaque que l'on soupçonne d'avoir été orchestrée par des pirates russes.

**SUISSE**

Le gouvernement suisse a déclaré que des données opérationnelles avaient pu être volées lors d'une cyberattaque contre une entreprise technologique qui fournit des logiciels à plusieurs services gouvernementaux. Xplain, un fournisseur suisse de logiciels gouvernementaux, avait été victime d'une attaque par rançongiciel.

## À l'avenir, la question est de savoir qui sera le prochain ?

# Comment les organisations ont-elles relevé le défi de la cybersécurité

ÉTUDE DE CAS 1 :

FRASERS GROUP

**En matière de cybersécurité, l'une des principales tâches que les organisations doivent effectuer consiste à améliorer leur cyberhygiène.** Le détaillant britannique Frasers Group exploite des centaines de magasins, emploie plus de 25 000 personnes et gère des opérations physiques et en ligne dans 25 pays. Le rapport fiscal 2021 de Frasers montre que les ventes ont atteint 3,6 milliards GBP (environ 4,4 milliards EUR).

Une grande partie de la croissance de Frasers provient d'acquisitions, souvent d'entreprises en difficulté. C'est une stratégie que l'entreprise continue de pratiquer. Début 2022, Frasers Group a acquis Studio Retail, spécialiste e-commerce en faillite, l'ajoutant à un portefeuille de marques qui comprend désormais Sports Direct, Game et Sofa.com.

Toute cette activité de fusions et acquisitions implique également la fusion de systèmes informatiques, une tâche complexe qui inclut l'application des meilleures politiques de cybersécurité. Pour superviser ce défi, il y a environ un an, Frasers a créé un groupe mondial pour la sécurité de l'information et la confidentialité ; ce groupe a établi la longue liste des incontournables de Frasers en matière de cybersécurité. Ces exigences comprennent notamment de nouvelles capacités de test de pénétration et d'analyse des vulnérabilités, ainsi qu'une meilleure visibilité des endpoints. Ce dont Frasers avait vraiment besoin, c'était d'améliorer sa cyberhygiène, d'obtenir une visibilité sur ses vulnérabilités et de protéger ses systèmes. L'utilisation d'une plateforme dédiée a permis à Frasers Group de détailler les vulnérabilités existantes des endpoints et d'établir les actions à prendre pour les atténuer.

ÉTUDE DE CAS 2 :

**Les organisations doivent s'assurer que les systèmes sont bien entretenus et administrés tout au long de leur vie.** Les appareils et interfaces utilisés à des fins administratives sont fréquemment ciblés, ils doivent donc être bien protégés. Le harponnage reste une méthode couramment utilisée pour compromettre les comptes ayant un accès privilégié. Empêcher l'utilisation de ces comptes pour des activités de routine telles que l'envoi d'e-mail et la navigation sur le Web limite considérablement les options dont disposent les pirates informatiques pour compromettre les systèmes clés.

Prenons le cas de Sodexo Benefits and Rewards Services (BRS), une unité commerciale de Sodexo S.A. qui propose des produits et services à environ 36 millions de consommateurs et de bénéficiaires dans plus de 30 pays. Soutenir les activités informatiques du groupe BRS est complexe. Certaines de ses entités ont de minuscules services informatiques, tandis que d'autres comptent jusqu'à 200 employés informatiques. Les compétences de ces services sont également très variables.

L'un des problèmes dont souffrait Sodexo était le manque de visibilité sur tous ses actifs informatiques. BRS ignorait le nombre d'endpoints utilisés, et ne savait donc pas non plus si ces endpoints étaient correctement sécurisés. Le deuxième problème concernait les mauvaises pratiques d'hygiène informatique. La mise en œuvre de correctifs était incohérente, et une grande partie de ces derniers étaient appliqués manuellement. Le troisième problème était une feuille de route de sécurité solide mais difficile à exécuter et à suivre sur les plus de 30 marchés, principalement en raison de la variabilité des compétences et des outils disponibles sur le terrain pour faire avancer les activités, en particulier dans des conditions de travail à distance.

Pour surmonter certains de ces défis, BRS a lancé une initiative autour de l'application des correctifs aux actifs, en demandant aux groupes de sécurité et d'infrastructure de s'associer pour trouver et mettre en place une solution mondiale d'application des correctifs. Les principaux objectifs étaient de retrouver une visibilité sur tous les endpoints et de soutenir le déploiement de solutions de sécurité, ce qui n'a pas été un défi facile au vu du nombre d'employés qui travaillaient à domicile pendant la pandémie.

ÉTUDE DE CAS 3 :

**Zurich Insurance Group exerce ses activités depuis 150 ans, avec une présence mondiale dans 210 pays et territoires, et des marques connues, dont Farmers Insurance.** Zurich fournit des produits et services d'assurance-vie et de biens et victimes (P&C) aux particuliers, aux petites et moyennes entreprises et aux multinationales.

Mais la réussite de l'entreprise attire également les cybercriminels. Avec plus de 100 000 endpoints numériques dans un environnement géographiquement distribué et hautement hétérogène, Zurich doit assurer la sécurité de ces endpoints.

Zurich avait besoin d'aide pour répondre aux incidents. En cas d'attaque, Zurich peut déterminer ce qui est arrivé, quand et où cela s'est produit, quels appareils ont été affectés et comment les endpoints attaqués peuvent être isolés, comment les problèmes peuvent être mitigés, puis comment les endpoints peuvent être remis en fonctionnement en toute sécurité.

Auparavant, Zurich manquait d'outils capables à la fois de fournir une visibilité sur les endpoints et de les gérer. Sa nouvelle solution (Tanium) signifie que l'entreprise dispose maintenant de ces capacités dans un tableau de bord centralisé avec un ensemble d'outils. Paige Adams, directeur mondial de la sécurité de Zurich, et son équipe ont désormais une visibilité complète sur leurs endpoints et sont en mesure de maintenir les correctifs de Zurich à jour. Zurich estime les économies réalisées à 100 heures de ressources par mois, sur la base des capacités d'application de correctifs automatisées que Zurich a développées en plus de l'outil de correctifs de Tanium.

# Les implications commerciales de la cybersécurité

**Bien que la cybersécurité soit devenue un problème mondial, les besoins des clients sont extrêmement variés.** Par exemple, les entreprises de services bancaires, d'assurance et financiers, où les transactions sont principalement numériques aujourd'hui, investissent largement depuis longtemps pour défendre leurs systèmes. En revanche, dans les secteurs de la production industrielle, de la vente au détail et de la santé, la révolution numérique ne fait que commencer. Par conséquent, dans ces secteurs, les vulnérabilités sont déjà exploitées par les attaquants lorsque les mises à niveau de sécurité des systèmes existants ne sont pas mises en œuvre dans l'ensemble de la chaîne de valeur.

Ayant reconnu ces menaces en constante évolution, certaines entreprises adoptent des outils tels que des pare-feux et le cryptage des données pour protéger leurs systèmes informatiques. Pour se préparer aux attaques, elles développent leur expertise par le biais de simulations de crise et de plans de communication. En outre, elles doivent se concentrer stratégiquement et investir dans des outils de détection précoce et de réponse rapide afin d'être résilientes face aux cyberattaques potentielles.

Un problème critique en matière de cybersécurité est le recrutement, en particulier la mise en place du bon leadership en matière de sécurité.

## Trouver les ressources humaines : le rôle vital du RSSI

Les responsables de la sécurité de l'information (RSSI) sont chargés de protéger les actifs d'une entreprise (physiques et numériques) contre les cyberattaques. À mesure que leur rôle devient plus crucial, les RSSI ont tendance à se répartir dans l'une de trois catégories distinctes (faire passer la souris pour plus d'informations) :

| TYPE DE RSSI | FOCUS | RESPONSABILITÉ | COMPÉTENCES CLÉS |
|---|---|---|---|
| **Technique** | Experts pratiques en technologie de cybersécurité | Gérer les outils, systèmes et aspects techniques de la sécurité pour se protéger contre les cybermenaces | Connaissances techniques approfondies et expérience en cybersécurité |
| **Centré sur l'entreprise** | Combler le fossé entre la cybersécurité et les objectifs de l'organisation | Aligner les stratégies de sécurité sur les objectifs commerciaux, en veillant à ce que la sécurité soutienne la croissance et la conformité | Sens des affaires, gestion des risques et communication efficace |
| **Risque et conformité** | Hiérarchiser l'évaluation des risques, la gestion et la conformité réglementaire | Identifier et atténuer les risques de sécurité, assurer le respect des réglementations et protéger la réputation de l'organisation | Expertise en matière d'évaluation des risques, connaissances en matière de conformité et capacités d'audit |

Cependant, les RSSI sont traditionnellement sous-représentés dans les conseils d'administration. En Europe, le rapport Heidrick & Struggles's Board Monitor Europe 2022 a montré qu'en 2021, seulement 5 % des sièges dans les conseils d'administration étaient occupés par des personnes ayant une quelconque expérience en cybersécurité. La fréquence croissante et la nature multidimensionnelle des cybermenaces remettent en question le statu quo ; les RSSI jouent désormais un rôle crucial dans la gouvernance des conseils.

Dans une enquête réalisée en 2023 par le Forum économique mondial, seul 25 % des personnes interrogées ont indiqué que le cadre senior en matière de cybersécurité dans leur organisation rendait compte directement au PDG. Cela dit, un défi clé pour les RSSI est d'obtenir le soutien du conseil d'administration pour permettre des actions efficaces. Ce problème provient du fait que les RSSI ont souvent du mal à traduire le jargon technique en langage commercial, avec des termes tels que risque, réputation et résilience. Cela est exacerbé par le fait que les dirigeants du conseil d'administration de nombreuses organisations manquent de la compréhension et de la sensibilisation nécessaires pour donner la priorité à la cybersécurité.

Un article de la Harvard Business Review « Boards Are Having the Wrong Conversations About Cybersecurity (les conseils d'administration n'ont pas les bonnes conversations à propos de la cybersécurité) » indique que les conseils d'administration se concentrent trop souvent sur la protection plutôt que sur la résilience. Dans de nombreuses réunions de conseil d'administration, le principal sujet est la fréquence à laquelle l'entreprise administre un test d'hameçonnage et les résultats statistiques. Ce n'est pas la perspective que le conseil d'administration devrait adopter pour la supervision. Aucune entreprise ne peut être totalement à l'abri des cybermenaces, quel que soit le montant qu'elle consacre aux technologies censées prévenir les attaques. Bien que la protection des actifs soit essentielle, la planification de la reprise après l'attaque est primordiale. Chaque entreprise doit poser le scénario d'une cyberattaque et se préparer à réagir et à se remettre avec un minimum de dommages, de coûts et d'impact sur la réputation. Le conseil d'administration doit considérer la résilience de la cybersécurité comme un paramètre opérationnel clé, et demander aux équipes opérationnelles de concevoir des approches permettant de répondre à une attaque et de s'en remettre.

**LES CONSEILS D'ADMINISTRATION DOIVENT CONSIDÉRER QUE LA CYBERSÉCURITÉ EST UN IMPÉRATIF STRATÉGIQUE ET INSISTER POUR RECEVOIR DES MISES À JOUR RÉGULIÈRES SUR :**

1. Les risques techniques et organisationnels auxquels l'entreprise est confrontée en raison de cyber-violations potentielles
2. Le degré de préparation pour tempérer tout dommage résultant de l'identification d'un risque spécifique
3. La vitesse de la reprise suite à une violation
4. Le risque encouru par la chaîne d'approvisionnement suite à des incidents potentiels de cybersécurité
5. Le niveau de protection permettant de ne pas perdre un jour ouvrable

L'un des principaux facteurs en raison desquels les RSSI peuvent remettre en question une carrière dans la cybersécurité est la crainte de ce qui arrivera à leur réputation professionnelle si leur entreprise subit une violation de données. Les RSSI et les responsables de la sécurité (CSO) craignent de voir leur nom traîné dans la boue après une violation de données, voire de devoir faire face à des accusations pénales. Par exemple, une violation subie par Uber fin 2022 a conduit le CSO Joe Sullivan à être condamné à une peine de trois ans de liberté surveillée ainsi qu'à payer une amende de 46 845 EUR après qu'un jury l'ait reconnu coupable de deux crimes, y compris la dissimulation d'une violation de données impliquant des millions de dossiers d'utilisateurs d'Uber.

## Combler les lacunes en matière de compétences et de responsabilités

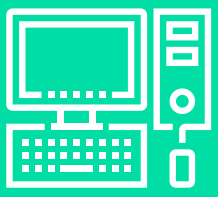
Il existe un manque important de compétences en cybersécurité, et la demande l'emporte de manière significative sur l'offre. Selon l'analyse des emplois de GlobalData, en 2022, le nombre moyen mondial d'offres d'emploi dans le domaine de la cybersécurité par mois était d'un peu moins de 180 000. Le nombre moyen d'offres d'emploi dans la cybersécurité remplies par mois était nettement inférieur (un peu plus de 60 000), illustrant bien la difficulté à remplir ces postes vacants. Une enquête réalisée en 2022 par le Forum économique mondial a révélé que 59 % des entreprises auraient du mal à répondre à une cyberattaque en raison de la pénurie de talents et de compétences en cybersécurité. Les cybercriminels exploitent les lacunes en matière de compétences dans les organisations pour extraire des informations. Par exemple, en 2015, le parlement fédéral allemand, le Bundestag, a

été compromis. Un manque de compétences au sein de l'équipe de cybersécurité du Bundestag a permis aux attaquants d'exploiter les vulnérabilités de l'infrastructure réseau.

En outre, il existe également des lacunes en matière de responsabilité, soit des situations dans lesquelles il existe un manque de responsabilité claire ou de rôles définis dans les équipes de cybersécurité. Les professionnels de la cybersécurité passent d'une entreprise à une autre, ce qui crée une ambiguïté ou un manque de consensus sur qui est responsable, et dans quelle mesure, d'aspects spécifiques de la cybersécurité. Cela entraîne des lacunes potentielles dans le système. Les carences générales en personnel de cybersécurité partout dans le monde ne font qu'aggraver le problème.

Pour y répondre, il faut développer des lignes de responsabilité claires et des rôles clairement définis, promouvoir la sensibilisation et l'éducation parmi les employés et favoriser les collaborations entre les parties prenantes, en particulier les fournisseurs tiers. Les régulateurs ont également un rôle essentiel à jouer dans ce domaine. Ils doivent appliquer des cadres de sécurité robustes qui clarifient les responsabilités et encouragent la conformité, en faisant la promotion d'un écosystème numérique sécurisé.

Le tableau ci-dessous met en évidence les principales complications auxquelles sont confrontées les entreprises européennes en matière de cybersécurité.



## Dettes technologiques

**La dette technologique fait référence à l'accumulation de systèmes technologiques, de logiciels et d'infrastructures obsolètes ou non sécurisés au sein d'une organisation.** Les systèmes d'exploitation obsolètes, les logiciels existants et le matériel non pris en charge peuvent créer des vulnérabilités qui peuvent ensuite être exploitées par les cybercriminels. Par exemple, le rançongiciel WannaCry de 2017 a ciblé des milliers d'entreprises, y compris des systèmes de santé au Royaume-Uni et en Espagne, qui utilisaient Windows XP sans correctifs. En 2020, l'attaque SolarWinds a affecté des entreprises, y compris des agences gouvernementales, aux États-Unis et en Europe en raison de retards dans la mise à jour des logiciels et de mauvaises pratiques de sécurité. La dette technologique freine l'adoption de solutions de sécurité à jour et entrave la capacité d'une organisation à répondre à des risques émergents sophistiqués. Cela expose l'infrastructure critique de l'organisation et les données sensibles à l'exploitation. Une évaluation fréquente des systèmes d'exploitation et une mise à niveau en temps opportun sont d'une importance capitale pour la cyber-résilience des entreprises.

## Cyber-assurance

**La fréquence et la gravité des cyberattaques augmentent, tout comme les coûts des primes et du règlement des sinistres.** Une enquête menée en 2022 par GlobalData sur l'assurance des PME britanniques a révélé que 32,7 % des PME britanniques ont perçu une augmentation ou une augmentation considérable du niveau de cyberrisque auquel elles faisaient face au cours de l'année. On peut comparer ces chiffres à 30,7 % en 2021, à mesure que les inquiétudes continuent à augmenter après la pandémie de COVID. Cependant, le taux d'adoption de la cyberassurance reste extrêmement faible. Il était de 12,1 % en 2022, en légère hausse par rapport à 11,2 % en 2021.

La crise de l'inflation est un défi pour les entreprises et la forte augmentation des primes d'assurance cyber est la raison principale pour laquelle les taux de pénétration sont faibles, malgré une préoccupation accrue concernant les cyberattaques subies par les entreprises. Les assureurs ont du mal à convaincre les entreprises qu'une police préventive à grande échelle offre un bon rapport qualité-prix, et un débat est en cours sur les assureurs qui ne couvrent pas les attaques des États-nations.

Certains gangs de rançongiciel ciblent des entreprises ayant des polices de cyber-assurance, car ils sont plus susceptibles de payer une rançon. Par conséquent, les assureurs repensent leurs cyberpolitiques pour atténuer les risques plus élevés de paiements, et mettent en place des primes plus élevées et une couverture client réduite. Les cyberassureurs sont également de plus en plus sélectifs quant aux entreprises qu'ils assurent, insistant pour recevoir d'énormes quantités d'informations sur la sécurité mise en place par leurs clients, et excluant certains types d'incidents de la couverture proposée. Les petites entreprises sont les principales perdantes, car elles n'ont pas les moyens de mettre en place des systèmes de sécurité sophistiqués et des polices d'assurance à grande échelle, car les deux deviennent simultanément plus coûteuses à mesure que le niveau de risque croît.

## Améliorer la cyberhygiène

**La cyberhygiène est un ensemble de pratiques courantes destinées à assurer la sécurité du traitement des données critiques et à sécuriser les réseaux.** Elle constitue une obligation, et non un choix, pour toutes les organisations.

L'Europe est une cible importante pour les cyberattaques en raison de son importance économique, de ses défis géopolitiques et de l'abondance de données précieuses. Ces facteurs rendent la cyberhygiène cruciale pour toutes les entreprises européennes. En outre, le Règlement général sur la protection des données oblige les entreprises de l'UE à mettre l'accent sur la protection des données, ce qui rend impératif de donner la priorité à la cyberhygiène et de se conformer aux règles. Parmi les incidents résultant du manque de cyberhygiène, on peut citer la violation de données subie par British Airways en 2018 et due à des vulnérabilités sur le site Web de la compagnie aérienne, et l'attaque Colonial Pipeline en 2021 qui a souligné l'importance des pratiques de cyberhygiène telles que la mise à jour des systèmes informatiques, la mise en œuvre d'un contrôle d'accès robuste et la réalisation de sauvegardes régulières. Ces incidents auraient pu être évités par la mise en place de pratiques de codage sécurisées, ainsi que la réalisation d'évaluations régulières et de sauvegardes, respectivement.

Les entreprises doivent s'engager à investir et hiérarchiser les domaines clés pour assurer la cyberhygiène et la résilience. Les pratiques de cyberhygiène peuvent aider à la surveillance continue des surfaces d'exposition et permettre de colmater les endpoints présentant des risques de sécurité. La communication liée à la sécurité est de la plus haute importance dans le développement d'une pratique de cyberhygiène destinée à protéger les « joyaux de la couronne » (c.-à-d. les systèmes et données informatiques).

## Le dilemme de la cybersécurité interne ou externalisée

**Investir dans la cybersécurité est indispensable pour toutes les entreprises, quelles que soit leur nature et leur taille.** Cependant, elles sont toutes confrontées à un choix crucial : cybersécurité interne ou cybersécurité externalisée. La cybersécurité interne nécessite la mise en place d'une équipe interne de professionnels de la cybersécurité pour protéger les actifs numériques de l'organisation, tandis que l'externalisation implique de s'appuyer sur des prestataires de services de sécurité gérés ou tiers pour les services de cybersécurité.

Les deux approches présentent des avantages et des inconvénients spécifiques. La cybersécurité interne offre un contrôle plus fort sur les systèmes de sécurité, car les programmes peuvent être adaptés pour répondre à des besoins spécifiques, superviser directement les opérations de sécurité et aligner les stratégies de cybersécurité sur leurs objectifs commerciaux. Cependant, elle nécessite un investissement important dans l'acquisition de talents, la formation, l'infrastructure et la maintenance. Les grandes organisations disposant de ressources financières et technologiques solides peuvent choisir la cybersécurité interne pour maintenir le contrôle et la confidentialité.

En revanche, l'externalisation offre l'accès à une expertise spécialisée avec des technologies de sécurité avancées, en temps réel et tout au long de la journée, sans nécessiter de grandes ressources internes. Elle peut constituer une option rentable pour les organisations, en particulier les PME, qui ne disposent pas du budget ou de l'expertise nécessaire pour mettre en place des équipes de cybersécurité internes. Cependant, elle peut également introduire des préoccupations en termes de confidentialité des données, de fiabilité des fournisseurs et de dépendance potentielle vis-à-vis d'entités externes. Il est vital que les organisations évaluent leurs besoins commerciaux, les ressources, les vecteurs de menace, la tolérance au risque et les exigences réglementaires lorsqu'elles choisissent entre cybersécurité interne et cybersécurité externalisée.

# Recommandations

1

**LA FRÉQUENCE CROISSANTE ET LA NATURE MULTIDIMENSIONNELLE DES CYBERMENACES REMETTENT EN QUESTION LE STATU QUO, C'EST POURQUOI LES RESPONSABLES DE LA SÉCURITÉ DE L'INFORMATION (RSSI) DEVIENNENT INCONTOURNABLES POUR LA GOUVERNANCE DU CONSEIL D'ADMINISTRATION.**

Mais ils restent sous-représentés dans les conseils d'administration en Europe. En 2021, seuls 5 % des sièges des conseils d'administration étaient occupés par des personnes ayant une expérience quelconque en matière de cybersécurité. Les lecteurs de cet article devraient s'assurer de faire partie de ce vertueux quota de 5 %, et non des 95 % restants.

2

**MIEUX VAUT PRÉVENIR QUE GUÉRIR.**

La recherche montre que les organisations qui adoptent une approche principalement préventive de la cybersécurité sont nettement moins susceptibles d'avoir subi une cyberattaque/violation de données que celles qui adoptent une approche essentiellement réactive. Compte tenu de la fréquence des cyberattaques/violations de données, l'adoption d'une approche préventive robuste de la cybersécurité est une solution clé pour contrer ces menaces.

3

**TROP SOUVENT, UN BUDGET DE CYBERSÉCURITÉ PLUS IMPORTANT N'EST ATTRIBUÉ QU'À LA SUITE D'UNE VIOLATION DE DONNÉES, ET NON AVANT QUE CELLE-CI NE SE PRODUISE.**

Cela revient à agir après les faits. On doit en conclure que les dirigeants n'apprécient toujours pas à sa pleine mesure le rôle préventif que joue la cybersécurité dans la protection de l'entreprise. Lorsque les bons outils ne sont pas en place, les organisations manquent de visibilité, de contrôle et de planification pour pouvoir **a)** prévenir une attaque et **b)** y réagir correctement.

4

**TOUTE ORGANISATION QUI NE SE CONFORME PAS AUX RÉGLEMENTATIONS SPÉCIFIQUES DE SON SECTEUR PRÉSENTE UN RISQUE ÉLEVÉ DE VIOLATION DE LA CYBERSÉCURITÉ.**

Le non-respect des réglementations peut entraîner d'autres conséquences, notamment des sanctions légales, une atteinte à la réputation de l'entreprise et une perte de confiance des tiers. Le besoin de conformité en matière de cybersécurité est désormais reconnu par les gouvernements du monde entier, y compris l'Union européenne (UE). Aucune entreprise ne peut être totalement à l'abri des cyberattaques. Le facteur clé de la cybersécurité est la résilience de l'entreprise face à ces cyberattaques.

5

**UN MODÈLE ZERO TRUST FOURNIT UNE PLUS GRANDE PROTECTION CONTRE LES RANÇONGICIELS ET LES MENACES DE CYBERSÉCURITÉ EN ATTRIBUANT L'ACCÈS MINIMUM REQUIS POUR EFFECTUER DES TÂCHES SPÉCIFIQUES.**

Il offre une solution moins sujette aux violations, ainsi qu'une meilleure protection aux utilisateurs et aux données. En authentifiant et en autorisant chaque utilisateur, appareil et application, l'approche Zero Trust minimise le risque de violation de la sécurité.

# Promoteur

**Tanium, unique fournisseur de Converged Endpoint Management (XEM), est à l'origine d'un changement de paradigme dans les approches existantes de gestion des environnements technologiques et sécuritaires complexes.** Seul Tanium protège chaque équipe, chaque endpoint et chaque workflow contre les cybermenaces en intégrant informatique, conformité, sécurité et risques dans une seule plateforme qui offre une visibilité complète sur les appareils, un ensemble unifié de contrôles et une taxonomie commune dans un seul but commun : protéger les informations et les infrastructures critiques à grande échelle.

Tanium a figuré au classement Forbes Cloud 100 pendant six années consécutives et figure dans le classement Fortune recensant les entreprises des nouvelles technologies offrant le meilleur cadre de travail. En fait, plus de la moitié des entreprises du Fortune 100 et des forces armées des États-Unis font confiance à Tanium pour protéger les personnes, défendre les données, sécuriser les systèmes et surveiller chaque endpoint, où qu'ils se trouvent. C'est le pouvoir de la certitude.

Rendez-vous sur www.tanium.com
Suivez-nous sur Linkedin : Tanium
Suivez-nous sur Twitter : @Tanium

# Nous sommes le fournisseur d'informations de référence de confiance pour les plus grandes industries au monde

Nous avons fait nos preuves en aidant des milliers d'entreprises, d'organisations gouvernementales et de professionnels du secteur à tirer profit de décisions plus rapides et plus éclairées.

Notre approche unique axée sur les données, sur l'humain et sur la technologie donne naissance aux informations fiables, exploitables et prospectives dont vous avez besoin pour prédire l'avenir et éviter les points aveugles.

En tirant parti de nos données uniques, de notre analyse experte et de nos solutions innovantes, nous vous donnons accès à des capacités inégalées via une seule plateforme.


SIÈGE SOCIAL

John Carpenter House
7 Carmelite Street
Londres
EC4Y 0AN
Royaume-Uni

Tél. : +44 20 7936 6400

GlobalDataPlc
GlobalDataPlc
GlobalData.com



CLAUSE DE NON-RESPONSABILITÉ

Tous droits réservés. Aucune partie de cette publication ne peut être reproduite, stockée dans un système de récupération ou transmise sous quelque forme que ce soit par quelque moyen que ce soit, électronique, mécanique, photocopie, enregistrement ou autre, sans l'autorisation préalable de l'éditeur, GlobalData. Les faits de ce rapport sont considérés comme exacts au moment de la publication mais ne peuvent être garantis. Veuillez noter que les résultats, conclusions et recommandations fournis par GlobalData seront basés sur des informations recueillies de bonne foi auprès de sources primaires et secondaires, dont nous ne sommes pas toujours en mesure de garantir l'exactitude. À ce titre, GlobalData ne peut en aucun cas être tenue responsable des mesures prises sur la base de toute information qui pourrait s'avérer incorrecte par la suite.