LIVRE BLANC

Résultats de l'enquête de cybersécurité 2017 :
une confiance excessive peut-elle conduire à la fermeture d'entreprises ?

Rapport de SolarWinds® MSP sur la préparation des entreprises du Royaume-Uni et des États-Unis en matière de cybersécurité

watsoft

solarwinds msp

RÉSUMÉ

Les réponses globales de cette étude de sécurité de 2017 indiquent clairement que les dirigeants de PME et d'autres entreprises sont confiants dans leur préparation contre les cybermenaces, leur faible vulnérabilité et la protection de leurs données. Les résultats montrent que les DSI, responsables informatiques et RSSI sont unanimes : ils sont en sécurité.

Cette conviction est devenue si importante pour les organisations qu'à mesure que des violations et des piratages marquants sont révélés (souvent synonymes de pertes financières et d'atteintes à la réputation pour les marques), leurs budgets de sécurité augmentent. Chaque année, les entreprises investissent davantage dans la cybersécurité, simplement pour maintenir ce niveau de confiance.

Les résultats de l'enquête indiquent que les fournisseurs informatiques sont sûrs de leur préparation contre la cybercriminalité. Mais cette confiance est-elle déplacée ?

Selon notre étude, oui.

À PROPOS DE L'ENQUÊTE

Début 2017, SolarWinds MSP a interrogé 400 entreprises équitablement réparties entre le Royaume-Uni et les États-Unis sur leur préparation, leurs expériences et leurs échecs en matière de cybersécurité.

Alors que 87 % des organisations ont déclaré avoir une entière confiance dans leurs technologies et techniques de sécurité, et que 59 % pensent être moins vulnérables qu'elles ne l'étaient il y a 12 mois, 71 % de ces mêmes organisations ont subi une violation au cours de la dernière année. Croire que « cela ne nous arrivera jamais » est illusoire.

Pourquoi un tel écart avec la réalité ? En termes simples, les entreprises négligent sept principes de sécurité de base :

1. Les stratégies de sécurité sont appliquées de manière incohérente.
2. Le degré de priorité accordé à la formation des utilisateurs est inférieur à ce qu'il devrait être.
3. Seules des technologies de base sont déployées.
4. Les rapports de vulnérabilités sont insuffisants, voire inexistants.
5. Les organisations n'apportent souvent aucun changement à leurs technologies ou processus à la suite d'une violation.
6. Des techniques et processus de prévention largement reconnus sont ignorés.
7. Les temps de détection, de réponse et de résolution augmentent.

Les entreprises qui cherchent à maintenir ou à améliorer leur sécurité doivent prêter attention à ces principes clés, ou leur excès de confiance les conduira à une fermeture.

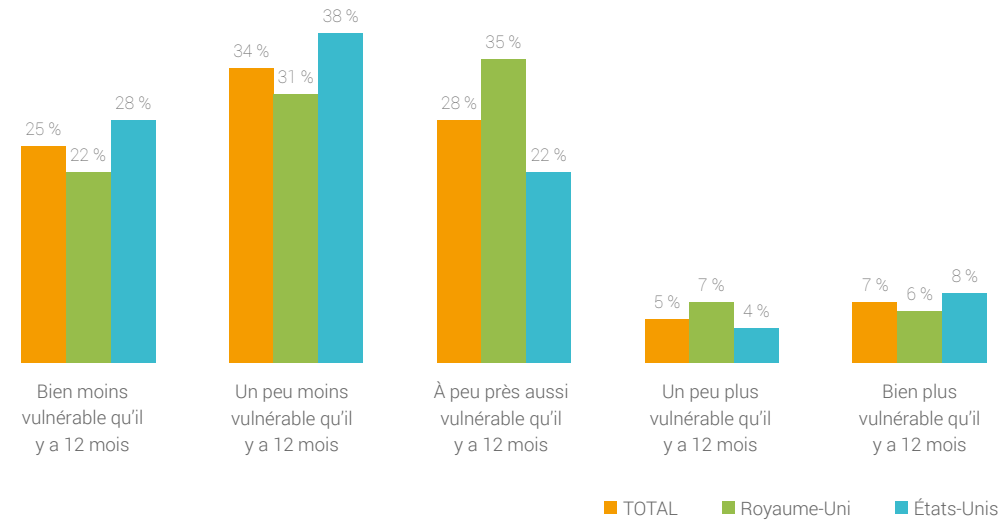
LES RESPONSABLES INFORMATIQUES SONT TROP CONFIANTS DANS LEUR PRÉPARATION EN MATIÈRE DE CYBERSÉCURITÉ

À première vue, les responsables informatiques du Royaume-Uni et des États-Unis ont peut-être raison d'être confiants. La grande majorité d'entre eux (87 %) pense qu'avec les technologies et techniques de sécurité mises en œuvre, leurs organisations se classent dans la « moyenne » voire au-delà. Par ailleurs, 61 % sont sur le point d'obtenir une augmentation importante de leurs budgets de cybersécurité, et ont la certitude que ce classement s'améliorera.

87 % pensent que leur implémentation de sécurité est dans la moyenne ou supérieure à celle-ci

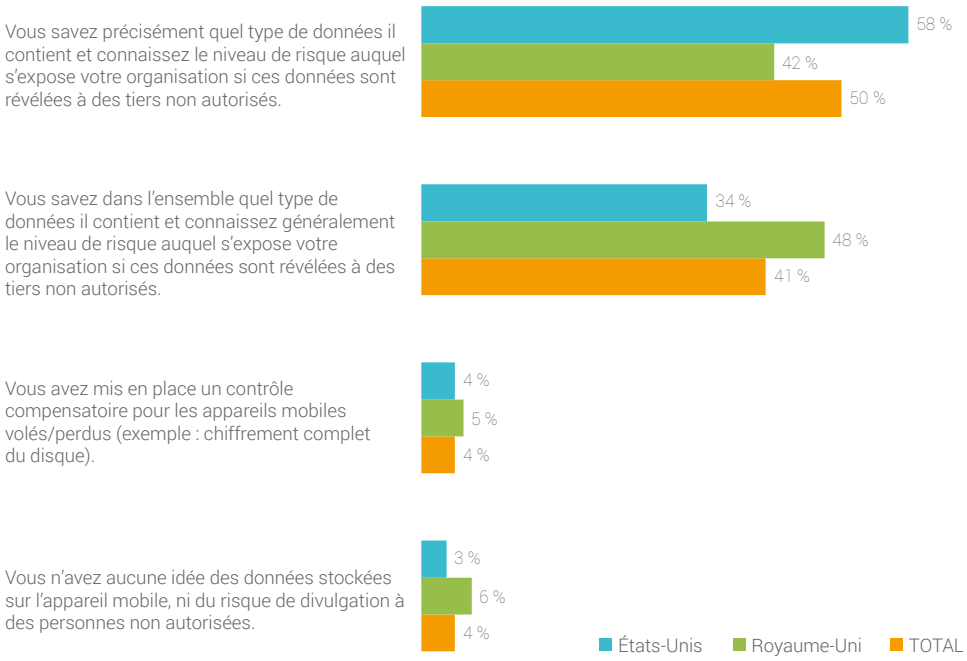
L'an dernier, l'« enquête de sécurité informatique » de SolarWinds (qui ciblait le même type d'entreprises qu'aujourd'hui), a montré que 50 % des personnes interrogées pensaient que leurs organisations étaient moins vulnérables en 2016 que les 12 mois précédents. Ce chiffre atteint désormais les 59 %.

Comment décririez-vous la vulnérabilité de votre organisation ?



Il ne s'agit pas uniquement d'une grande assurance en soi. Ces responsables ont également confiance dans leur capacité à faire face à des menaces et exigences spécifiques. Par exemple, 50 % d'entre eux sont certains qu'en cas de vol d'un appareil mobile, ils sauraient exactement quelles données y sont enregistrées, et quel niveau de risque cela représente pour leur entreprise. Malgré la forte augmentation récente des pertes de données et violations, 57 % sont sûrs des mesures mises en place pour protéger les données d'identification personnelle de leurs clients et employés.

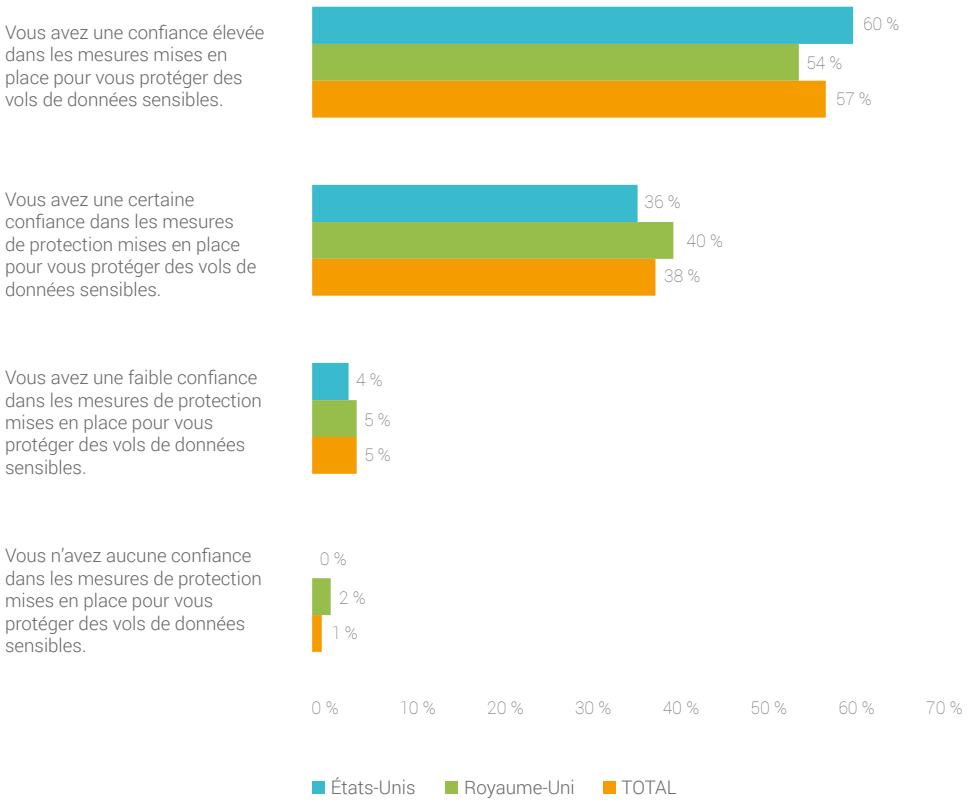
Si un responsable/directeur/vice-président des ressources humaines ou des opérations perd ou se fait voler son appareil mobile, laquelle de ces propositions vous correspond ?



Moins de 50 % des entreprises ont mis en œuvre de nouvelles technologies de sécurité après une violation de données

14 % n'ont rien fait du tout

En tenant compte de l'importance des données d'identification personnelle détenues par les entreprises à propos de leurs clients et employés, laquelle des propositions suivantes vous décrit le mieux ?



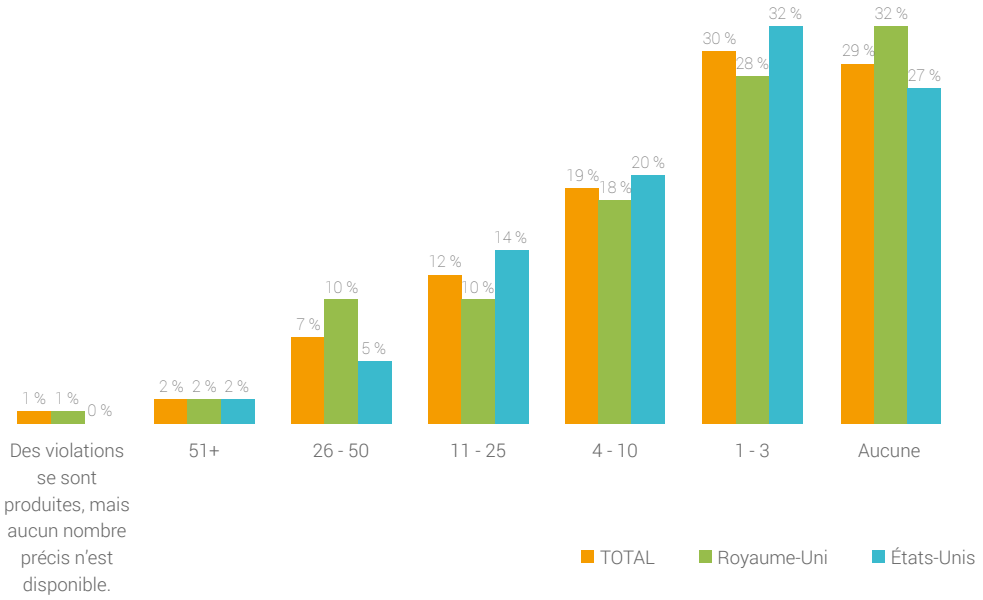
57 % des responsables informatiques ont une confiance élevée, mais comme le montrent les données, elle est peut-être inappropriée

LA RÉALITÉ

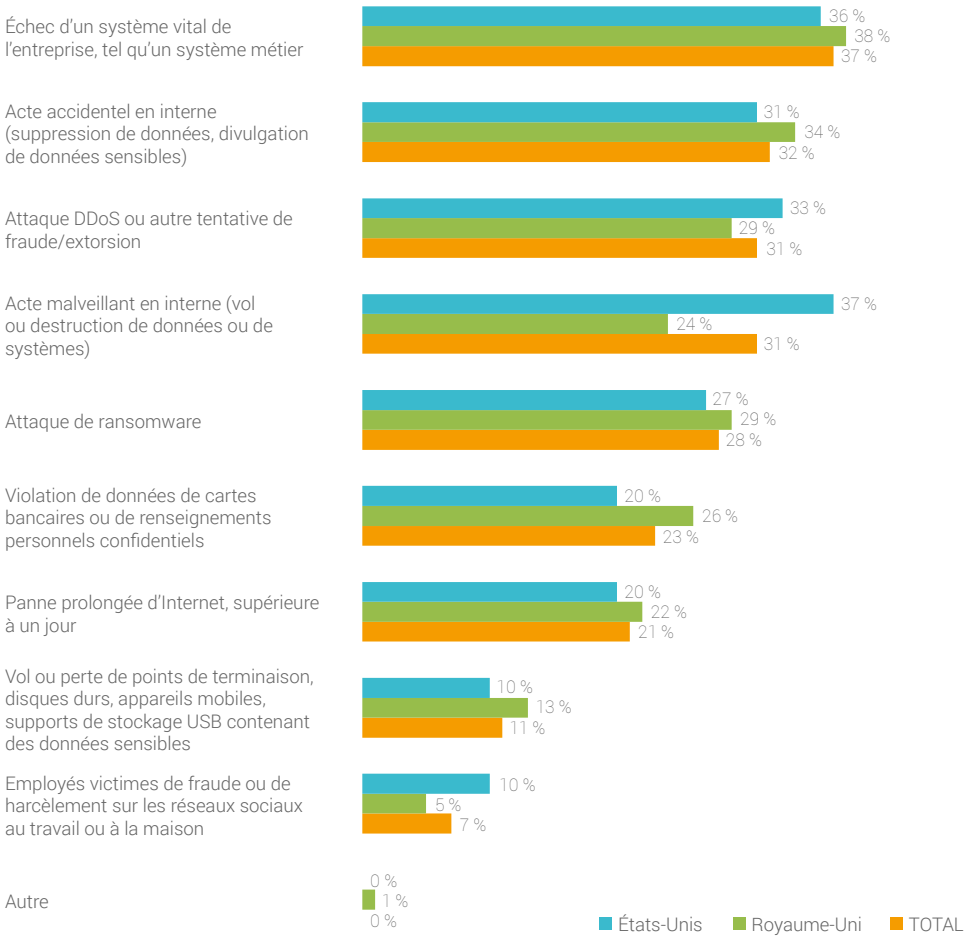
La grande ironie est que si 87 % considèrent avoir implémenté une protection de cybersécurité dans la moyenne ou supérieure à celle-ci, et se sentent moins vulnérables qu'ils ne l'étaient il y a 12 mois, 71 % ont signalé au moins une violation de données l'an dernier. En 2016, ce chiffre était de seulement 29 %.

71 % des personnes interrogées ont signalé au moins une violation au cours de la dernière année

Par combien de violations de sécurité votre organisation a-t-elle été touchée ces 12 derniers mois ?



Quels types de violations de sécurité avez-vous connus ces 12 derniers mois ? (parmi les 283 entreprises ayant signalé une violation au cours des 12 derniers mois)



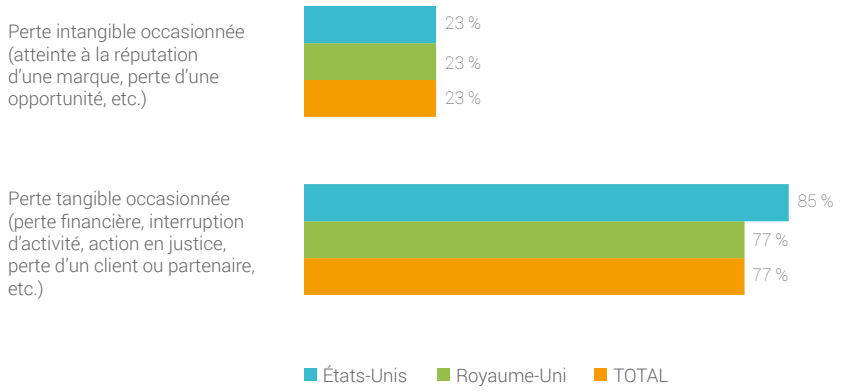
Les attaques DDoS (Distributed Denial of Service), fraudes et actes malveillants en interne représentent un tiers ou 31 % des violations

LES CONSÉQUENCES

Les conséquences de ces violations sont significatives.

Seulement 13 % des entreprises interrogées ayant subi une violation ont pu identifier un impact immédiatement visible. Dans certains cas, il s'agissait d'une perte tangible : perte d'un client ou d'un partenaire, perte financière ou impact opérationnel (ex. : temps d'arrêt). D'autres ont subi une perte intangible, comme l'atteinte à la réputation d'une marque ou une opportunité manquée.

En examinant votre dernier incident de sécurité, quelle proposition caractérise le mieux votre organisation ? (parmi les 52 entreprises interrogées ayant pu identifier une perte visible)



77 % des entreprises interrogées ont signalé une perte tangible (perte financière, action en justice, perte de client) à la suite d'un incident de sécurité

23 % des sondés ont signalé une perte intangible (atteinte à la réputation d'une marque, etc.)

D'un point de vue purement commercial, combien coûte cette vulnérabilité aux entreprises ? Au-delà des conséquences immédiatement perceptibles, telles que la perte d'un client ou un temps d'arrêt entraînant la perte d'une opportunité, quelles sont les implications les plus larges ?

Dans leur étude « 2016 Cost of Data Breach Study : Global Analysis »[1], IBM et Ponemon ont estimé le coût standard d'un enregistrement perdu ou volé à 158 $ (USD)/122 £ (GBP). Ce calcul inclut les dépenses directes (ex. : services d'un expert judiciaire, externalisation de la hotline, coûts de réparation de la relation client, tels que des remises sur les produits et les services) et les dépenses indirectes (enquêtes et communications internes). Il extrapole également les valeurs typiques de clients perdus, et l'impact des atteintes à la marque sur la future acquisition de clients.

En combinant ces indicateurs avec nos propres données, nous pouvons voir que l'impact sur les PME et autres entreprises est énorme :

	PME	AUTRES ENTREPRISES
Nombre moyen d'enregistrements* détenus	482	5 946
Coût par enregistrement* perdu/volé (IBM/Ponemon)	122 £ GBP 158 $ USD	122 £ GBP 158 $ USD
Coût typique d'une seule violation de données pour une PME/autre entreprise	58 703 £ GBP 76 214 $ USD	723 596 £ GBP 939 444 $ USD
Nombre moyen de violations subies en 12 mois	0,32	1,05
Coût annuel typique des violations de données pour une PME/autre entreprise	18 844 £ GBP 24 465 $ USD	757 251 £ GBP 983 139 $ USD

*Un enregistrement se définit comme un élément d'information ou champ de données lié à un ou plusieurs autres éléments d'information ou champs de données contenant des informations d'identification personnelle.

Aucune entreprise ne peut se permettre ce niveau de responsabilité. C'est pourquoi nous avons examiné de plus près les raisons de cette vulnérabilité. Nous avons identifié sept facteurs communs, qui expliquent cette confiance déplacée.

1 Source : https://securityintelligence.com/media/2016-cost-data-breach-study/

LES SEPT PIÈGES DE LA CYBERSÉCURITÉ

D'après nos recherches, les éléments suivants représentent les sept principaux pièges qui exposent les entreprises des États-Unis et du Royaume-Uni à de lourdes responsabilités financières, voire à un événement aussi grave qu'une fermeture.

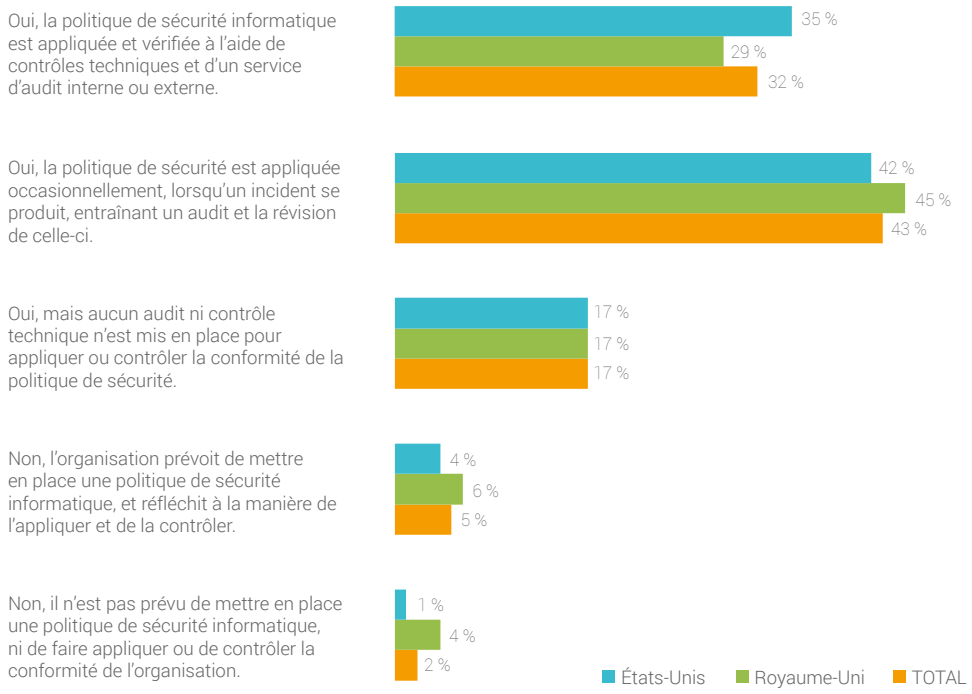
1. INCOHÉRENCE

DANS L'APPLICATION DES STRATÉGIES DE SÉCURITÉ

Une stratégie de sécurité n'a clairement aucune valeur si elle n'est pas correctement appliquée et si son adéquation n'est pas régulièrement vérifiée. Cependant, seulement 32 % des personnes interrogées ont pu affirmer que leurs politiques de sécurité étaient appliquées de manière fiable, et contrôlées à intervalles réguliers. Par ailleurs, moins de la moitié (43 %) ne les appliquent qu'occasionnellement, 17 % ne vérifient pas leur pertinence et 7 % n'ont aucune politique en place.

68 % des organisations interrogées n'appliquent pas et ne contrôlent pas leurs politiques de sécurité de manière fiable

Votre organisation dispose-t-elle d'une politique de sécurité informatique qui encadre l'utilisation, la création et le traitement des informations de vos clients et employés ?



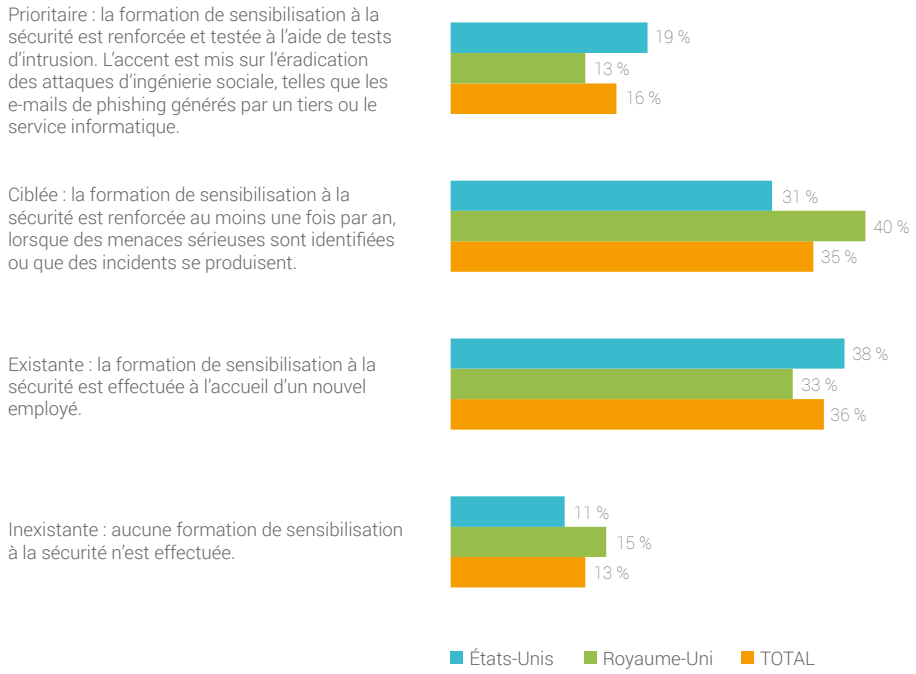
2. NÉGLIGENCE

DE L'APPROCHE DE SENSIBILISATION DES UTILISATEURS À LA SÉCURITÉ

Malgré tous les commentaires effectués sur son importance, seuls 16 % des sondés considèrent la sensibilisation à la sécurité comme une priorité. Un grand nombre d'entre eux (71 %) font semblant de s'y intéresser en l'abordant de manière ponctuelle, lors de l'accueil d'un nouvel employé ou d'un rappel annuel. Le reste, 13 %, admet ne rien faire.

Seuls 16 % des sondés considèrent les formations de sensibilisation à la sécurité comme une priorité

En tenant compte des utilisateurs de votre organisation, comment décririez-vous la sensibilisation actuelle ?



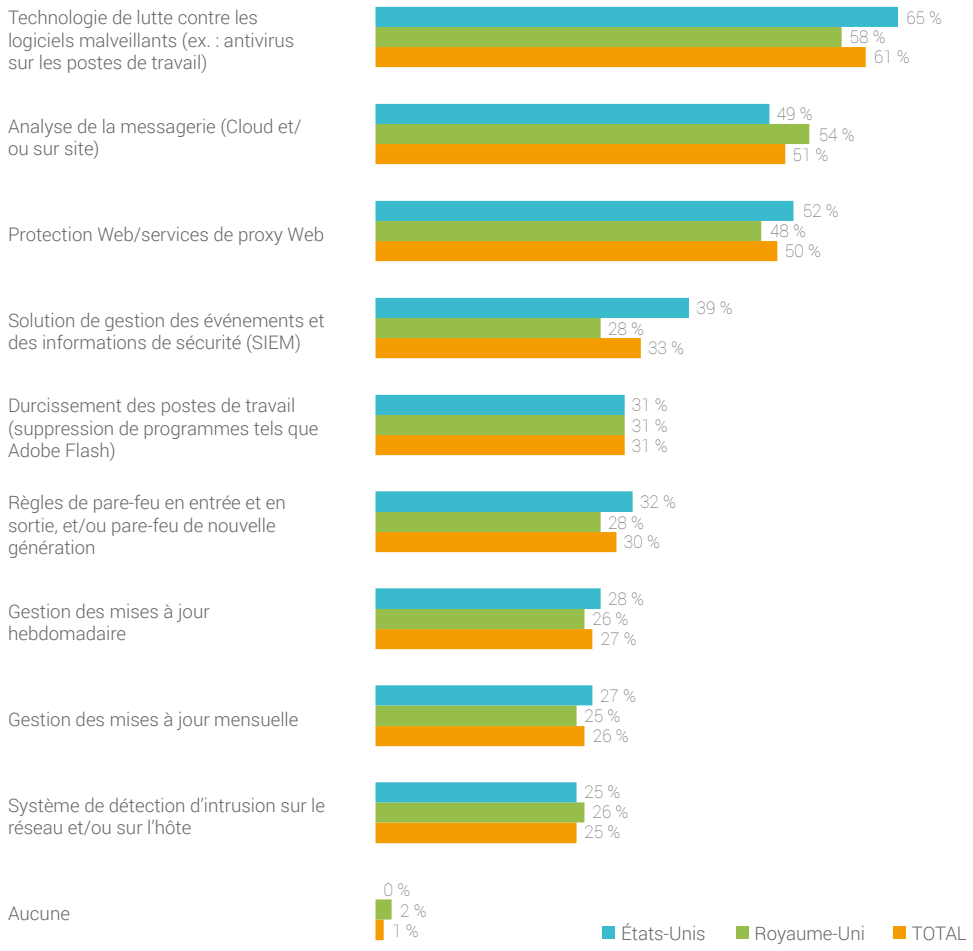
3. MANQUE DE VISION À LONG TERME

DANS L'APPLICATION DES TECHNOLOGIES DE CYBERSÉCURITÉ

Six des neuf technologies de cybersécurité les plus courantes n'ont été déployées que par une minorité des organisations interrogées. Les outils de protection Web, d'analyse de messagerie et de protection contre les logiciels malveillants ont tous été installés par 50 à 61 % des organisations. Les six restants (SIEM, règles de pare-feu, gestion des mises à jour…) ont été déployés par seulement 33 % des organisations au maximum (SIEM), et 25 % au minimum (systèmes d'intrusion).

6 des 9 technologies de cybersécurité les plus importantes ne sont déployées que par une minorité ou moins de 31 % des organisations

Laquelle de ces technologies avez-vous installée sur site pour empêcher les violations de données ?

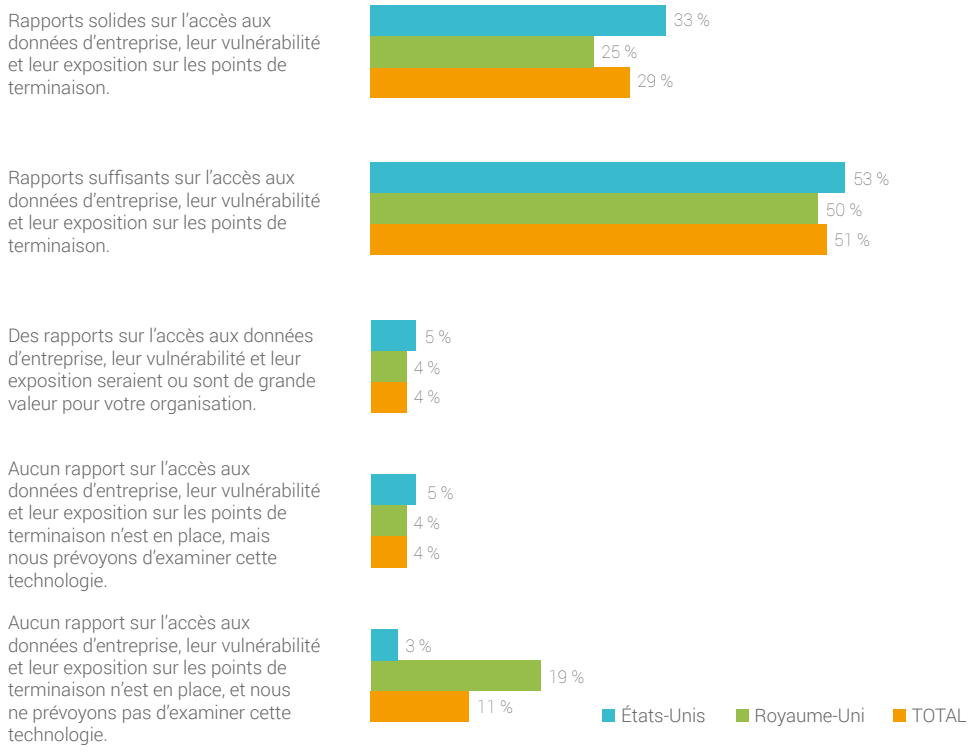


4. COMPLAISANCE

À L'ÉGARD DES RAPPORTS DE VULNÉRABILITÉS

Seules 29 % des personnes interrogées ont qualifié leurs rapports de vulnérabilités de « solides », la majorité d'entre elles (51 %) les considère de manière optimiste comme « suffisants ». Étonnamment, 19 % n'utilisent pas de rapports, et 11 % déclarent catégoriquement qu'elles ne prévoient pas d'étudier leur déploiement ou leur utilité.

Laquelle de ces propositions décrit le mieux les rapports mis en place dans votre organisation ?



Seules 29 % des personnes interrogées peuvent qualifier leurs rapports de vulnérabilités de « solides »

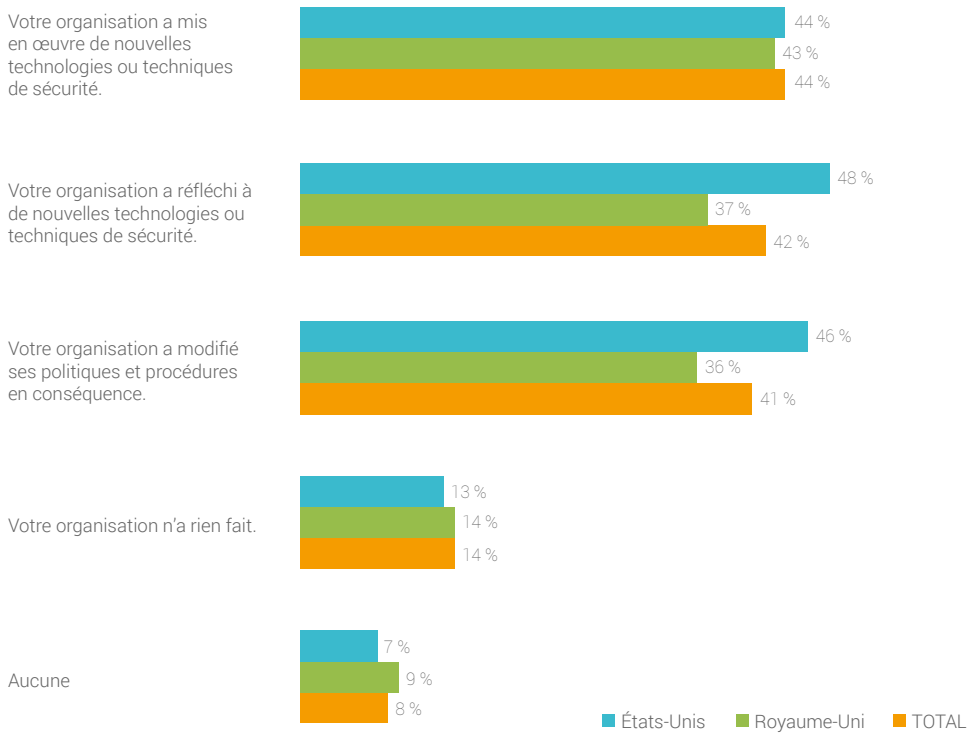
5. INFLEXIBILITÉ

DANS L'ADAPTATION DES PROCESSUS ET DE L'APPROCHE APRÈS UNE VIOLATION

Après une violation (déjà subie par 71 % des personnes interrogées), seules 44 % des entreprises ont implémenté une nouvelle technologie, et 41 % ont modifié leurs processus. En parallèle, 42 % ont commencé à s'intéresser à une nouvelle technologie, tandis que 14 % n'ont délibérément rien fait.

Seules 44 % des personnes interrogées ont déployé une nouvelle technologie à la suite d'une violation de sécurité

En examinant votre dernier incident de sécurité, laquelle de ces propositions décrit le mieux la manière dont votre organisation a répondu ?



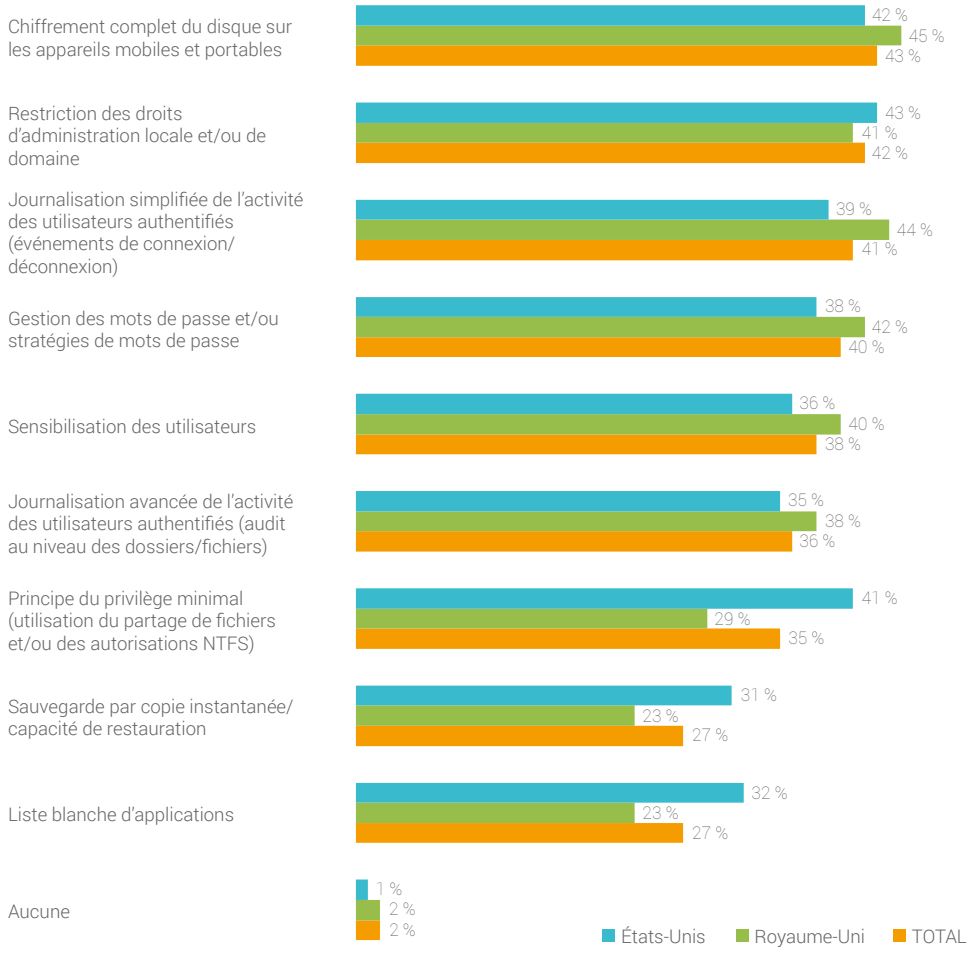
6. STAGNATION

DANS L'APPLICATION DE TECHNIQUES DE PRÉVENTION CLÉS

Seule une minorité d'organisations a mis en œuvre les neufs techniques de prévention énumérées. La plus courante était le chiffrement complet du disque sur les appareils mobiles et portables, mais même celle-ci n'a été appliquée que par 43 % des entreprises. La liste blanche d'applications n'a été intégrée que par 38 % des sondés, et la journalisation de l'activité des utilisateurs authentifiés, par 41 %.

La majorité des personnes interrogées n'a pas réussi à adopter les 9 principales techniques de prévention

Laquelle de ces techniques avez-vous installée sur site pour empêcher les violations de données ?



7. LÉTHARGIE

DES TEMPS DE DÉTECTION ET DE RÉPONSE

Au cours des 12 derniers mois, les temps de détection des entreprises interrogées ont augmenté de 40 %, les temps de réponse, de 44 %, et ceux de résolution, de 46 %. À titre de comparaison, dans notre rapport de 2016, les temps de détection avaient augmenté de 28 %, les temps de réponse, de 28 %, et ceux de résolution, de 27 %. Le taux de déclin (et de complaisance) est donc en hausse.

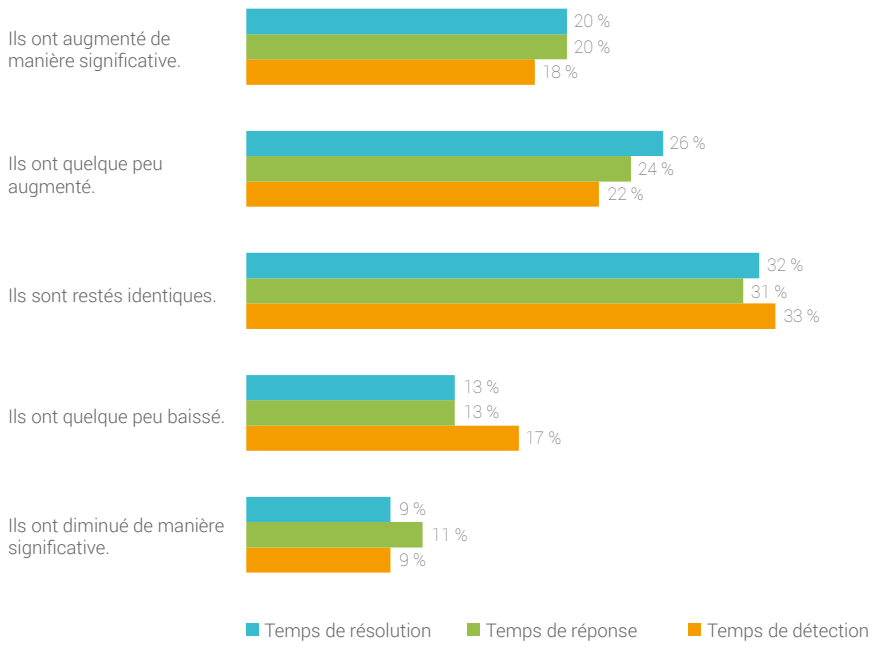
L'étude montre que :

Les temps de détection ont augmenté de 40 %

Les temps de réponse ont augmenté de 44 %

Les temps de résolution ont augmenté de 46 %

En comparant 2016 à 2015, comment les temps de détection, réponse et résolution de votre organisation ont-ils changé ?



CONSEILS POUR LES MSP

Les données et conclusions de ce rapport mettent en lumière un point essentiel : **les PME et autres entreprises sont trop confiantes dans leur préparation en matière de cybersécurité**.

Dans ce contexte, quelles sont les opportunités des fournisseurs de services gérés (MSP) ?

OPPORTUNITÉ 1 : OFFREZ UNE FORMATION DE CYBERSÉCURITÉ À VOS CLIENTS. La formation peut faire une différence de taille dans la sécurité de vos clients. Il est donc essentiel que vous leur transmettiez les connaissances nécessaires pour empêcher les violations. Que vous l'offriez sous forme de service afin de générer des revenus ou que vous la proposiez gratuitement dans un objectif de fidélisation, la formation contribue à réduire le nombre d'incidents de sécurité. Elle se traduit par une réduction des appels d'urgence et, en fin de compte, par des clients plus satisfaits.

OPPORTUNITÉ 2 : ASSUREZ-VOUS QUE VOTRE PROPRE MAISON EST EN ORDRE. Les MSP doivent s'assurer que leurs propres pratiques de sécurité sont à la hauteur. Vous devez vérifier que vos règles et technologies de sécurité répondent aux meilleures pratiques actuelles, tout en étant tournées vers l'avenir. Votre sécurité répond-elle aux besoins actuels et futurs des PME et autres entreprises ? Est-elle bien adaptée aux environnements sur site, dans le Cloud et hybrides ? Pouvez-vous répondre aux besoins de clients appartenant à des marchés spécialisés très réglementés ?

OPPORTUNITÉ 3 : PRÉPAREZ-VOUS À L'AIDE D'EXERCICES D'INCIDENTS. Les MSP peuvent proposer de tester la sécurité de leurs clients en mettant en place des « jeux de guerre ». De nombreux secteurs effectuent des exercices afin de se préparer à gérer les pires scénarios : les équipes marketing travaillent leurs réponses aux crises de relations publiques, les entreprises de services financiers testent leurs portefeuilles, et les équipes logistiques prévoient la fermeture inopinée des services de transport. Dans votre rôle de MSP, vous pouvez tester les situations d'incidents avec vos clients, que ce soit en termes de technologies ou de processus, afin d'identifier les faiblesses et d'apporter des améliorations. Les lignes de communication et les équipements sont-ils suffisamment solides ? Les attentes et les indicateurs sont-ils raisonnables ? Des opportunités de ventes additionnelles ne sont pas impossibles avec ce processus.

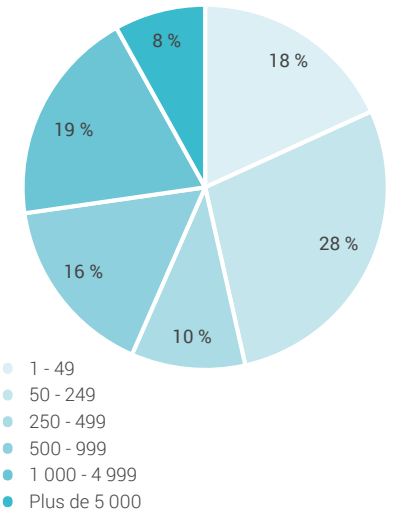
OPPORTUNITÉ 4 : DÉTERMINEZ LES PARTENARIATS ET COMPÉTENCES DONT VOUS AVEZ BESOIN. De nombreux incidents nécessitent l'intervention de spécialistes. Assurez-vous donc d'être prêt avant d'en avoir besoin. Qu'il s'agisse de contrer les attaques DDoS, de protéger l'infrastructure IoT ou d'implémenter des réponses aux incidents dans le respect des normes légales, vous devez envisager de recruter des experts, ou de vous associer à des personnes en mesure de gérer ces points pour vous. Vous ne devriez jamais avoir à développer de nouvelles compétences en situation de crise.

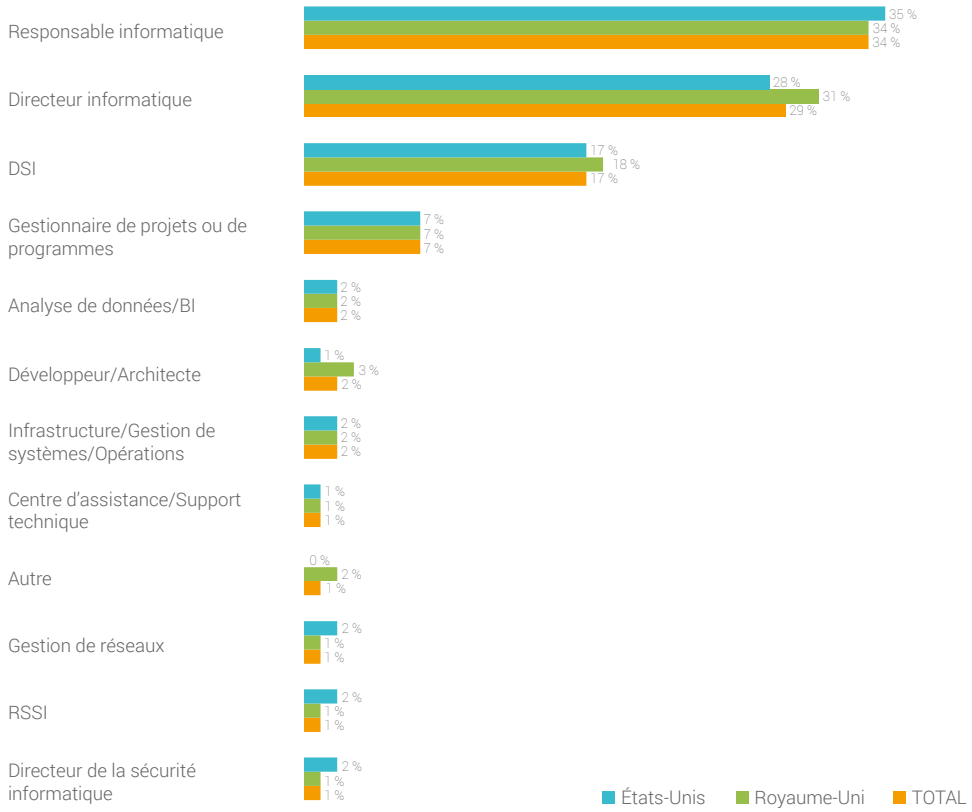
L'excès de confiance des organisations, conjugué à la prédominance des sept pièges de cybersécurité, crée des conditions idéales pour les cybercriminels et leurs méfaits. Avec la bonne approche, le dialogue, les relations et les outils adéquats, les MSP peuvent transformer ces failles en opportunités lucratives.

MÉTHODOLOGIE

En janvier 2017, SolarWinds MSP a chargé Sapio Research d'enquêter sur la préparation et l'expérience de 401 organisations en matière de cybersécurité. L'étude porte sur un nombre équitable de PME et autres entreprises (supérieures ou inférieures à 250 salariés), réparties de manière homogène entre le Royaume-Uni et les États-Unis.

EMPLOYÉS DANS L'ENTREPRISE INTERROGÉE	TOTAL (401)	ROYAUME-UNI (200)	ÉTATS-UNIS (201)
1 - 49	18 %	22 %	14 %
50 - 249	28 %	27 %	29 %
250 - 499	10 %	11 %	10 %
500 - 999	16 %	15 %	16 %
1 000 – 4 999	19 %	20 %	19 %
Plus de 5 000	8 %	6 %	11 %





SÉCURITÉ MULTICOUCHE INTELLIGENCE COLLECTIVE AUTOMATISATION INTELLIGENTE

SolarWinds MSP offre aux fournisseurs de services informatiques les technologies garantes de leur réussite. Axées sur la sécurité multicouche, l'intelligence collective et l'automatisation intelligente, les solutions de SolarWinds MSP sont disponibles sur site ou dans le Cloud, s'accompagnent de recommandations pratiques, et aident les fournisseurs de services informatiques à réaliser leurs tâches plus facilement et plus rapidement. Ils peuvent ainsi se concentrer sur l'essentiel : respecter leurs accords de niveau de service et fournir des services de manière efficiente et efficace.