RAPPORT

proofpoint®

CYBERSÉCURITÉ CENTRÉE SUR LES PERSONNES :

ÉTUDE AUPRÈS DE RESPONSABLES DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION (RSSI) EN FRANCE

RÉSUMÉ

Le paysage des cybermenaces continue d'évoluer en Europe, et la France ne fait pas exception à la règle. Par ailleurs, les cybercriminels ciblent de plus en plus les personnes plutôt que l'infrastructure.

Les cybercriminels ont bien compris que piéger les collaborateurs était un jeu d'enfant, que ce soit via la compromission de comptes cloud, des attaques de ransomwares paralysantes ou des menaces propagées par email, telles que le piratage de la messagerie en entreprise (BEC, Business Email Compromise). Au moyen d'attaques d'ingénierie sociale, les cybercriminels peuvent dérober des identifiants de connexion, détourner des données sensibles et effectuer des virements bancaires frauduleux. Quel que soit le poste ou la fonction qu'ils occupent, les collaborateurs peuvent mettre votre entreprise en péril de nombreuses manières, par exemple en utilisant des mots de passe faibles, en partageant leurs identifiants de connexion, en cliquant sur des liens malveillants ou en téléchargeant des applications non autorisées.

À cela vient s'ajouter la généralisation du télétravail, qui crée de nouveaux défis de cybersécurité pour les entreprises du monde entier. Les collaborateurs ne sont pas soumis aux procédures de sécurité habituellement en place au bureau, et cela n'a pas échappé aux cybercriminels.

Pour lutter contre ces menaces, les entreprises doivent impérativement déterminer la fréquence à laquelle elles sont ciblées, les risques posés par ces attaques et leur niveau de préparation – mais surtout celui de leurs collaborateurs – pour se défendre contre celles-ci. Ce point revêt une importance particulière dans le contexte actuel, car la généralisation du télétravail accentue encore la pression sur les équipes de cybersécurité du monde entier.

La formation des collaborateurs et leur sensibilisation à la sécurité sont au cœur de toute stratégie efficace, et font souvent la différence entre l'échec et la réussite d'une cyberattaque.

Pour mieux comprendre l'impact sur les entreprises des cyberattaques centrées sur les personnes, Proofpoint a commandité une étude menée auprès de 150 RSSI français. L'étude a été réalisée par le bureau d'étude Censuswide, qui a interrogé des entreprises françaises issues de différents secteurs d'activité en octobre 2020.

L'étude a examiné plusieurs points clés, notamment :

- La fréquence des cyberattaques
- Le niveau de préparation des collaborateurs et des entreprises
- L'impact de la généralisation du télétravail au niveau mondial
- Comment les entreprises se préparent au paysage des menaces de demain

L'étude révèle que la nécessité de protéger les collaborateurs contre les menaces imminentes ne s'est jamais faite aussi impérieuse. En effet, la majorité des entreprises françaises ont essuyé plusieurs cyberattaques l'année dernière.

De l'adhésion de la direction au renforcement des formations de sensibilisation à la cybersécurité, les entreprises françaises prennent des mesures pour consolider leurs cyberdéfenses.

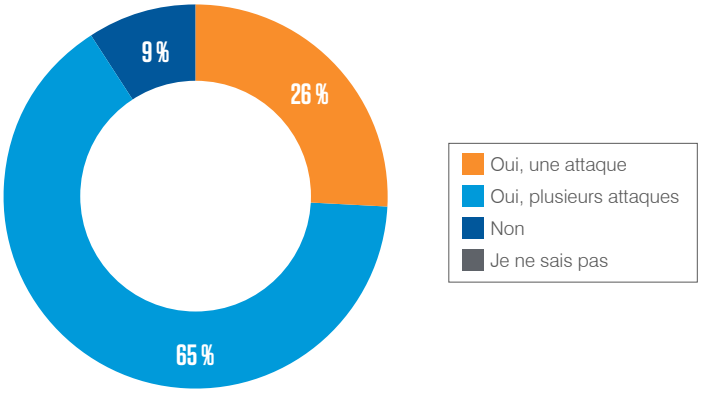
Ce rapport présente ces mesures ainsi que les principales conclusions de l'étude.

CONCLUSION N° 1 : LES ENTREPRISES FRANÇAISES SONT CONFRONTÉES À TOUTE UNE SÉRIE DE MENACES COMPLEXES

À l'instar de leurs homologues à travers le monde, les entreprises françaises sont sous la menace quasi constante des cybercriminels.

D'après notre étude, 91 % des entreprises françaises ont été victimes d'au moins une cyberattaque majeure au cours des 12 derniers mois. Près de deux tiers (65 %) ont fait état de plusieurs incidents, tandis qu'environ un quart (26 %) n'en ont subi qu'un seul.

Votre entreprise a-t-elle été victime d'une cyberattaque majeure au cours des 12 derniers mois ?



Les attaques par usurpation d'identité devraient mener la danse

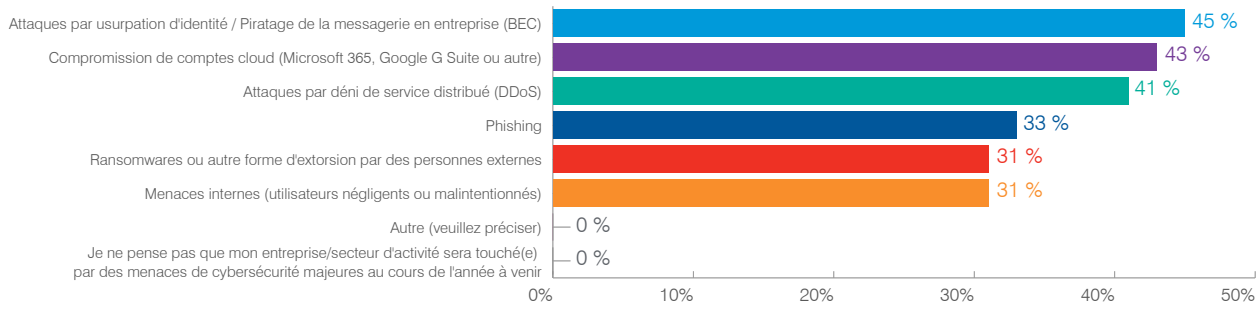
Les attaques par usurpation d'identité, telles que le piratage de la messagerie en entreprise ou l'usurpation de l'identité de PDG, sont en passe de devenir une des menaces de cybersécurité les plus coûteuses. En fait, le FBI a récemment estimé les pertes occasionnées par de telles attaques à 26,5 milliards de dollars pour les trois dernières années.

D'après notre étude, 45 % des RSSI français pensent que les attaques par usurpation d'identité deviendront l'une des principales méthodes employées par les cybercriminels au cours des 12 prochains mois, suivies de près par la compromission de comptes cloud (43 %), les attaques DDoS (41 %) et le phishing (33 %).

Ces prévisions concordent avec les tendances actuelles. De plus en plus, les cybercriminels utilisent des identifiants de connexion compromis pour accéder à des comptes de messagerie, des informations sensibles et des systèmes d'entreprise. Les identifiants de connexion font souvent l'objet d'attaques de phishing distribuées par email, une méthode d'attaque d'une efficacité redoutable.

Une étude de Proofpoint révèle par ailleurs que près d'un destinataire d'un email de phishing sur quatre l'ouvre. Plus de 10 % admettent cliquer sur les liens malveillants qu'il contient.

Selon vous, quelles sont les principales menaces de cybersécurité qui pèseront sur votre entreprise au cours de l'année à venir, le cas échéant ? (Cochez au maximum trois réponses.)



CONCLUSION N° 2 : LA GÉNÉRALISATION DU TÉLÉTRAVAIL S'ACCOMPAGNE DE NOUVEAUX DÉFIS POUR LES ÉQUIPES DE CYBERSÉCURITÉ

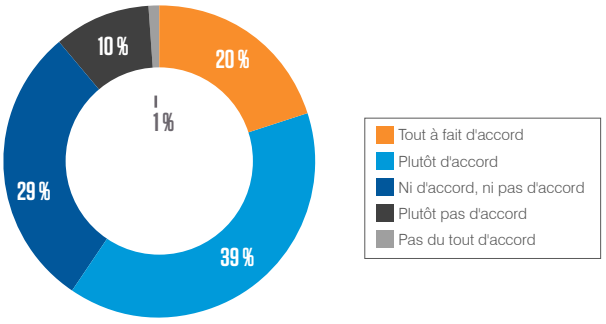
L'adoption massive du télétravail en raison de la pandémie mondiale de COVID-19 accentue encore la pression sur les équipes de cybersécurité. Chargées de défendre une surface d'attaque plus vaste et plus complexe, bon nombre d'entre elles admettent avoir des difficultés à effectuer la transition.

Seulement un cinquième (20 %) des RSSI français affirment être « tout à fait d'accord » que les collaborateurs disposent des moyens nécessaires pour travailler à distance, tandis que plus d'un tiers (39 %) sont « plutôt d'accord ».

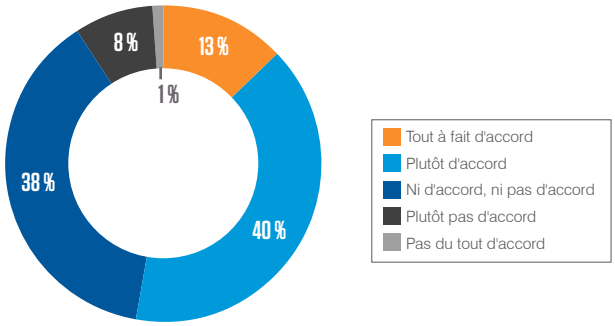
Les utilisateurs ne sont pas les seuls à être mal préparés. Les nouveaux effectifs dispersés ont également mis au jour les systèmes et applications mal sécurisés.

Plus de la moitié (53 %) des RSSI français reconnaissent que la transition vers le télétravail a rendu les systèmes et les applications obsolètes et peu efficaces pour protéger leur entreprise contre les cybermenaces actuelles.

Dans quelle mesure êtes-vous d'accord avec l'affirmation suivante ? Nos collaborateurs disposent des moyens nécessaires pour travailler à distance.



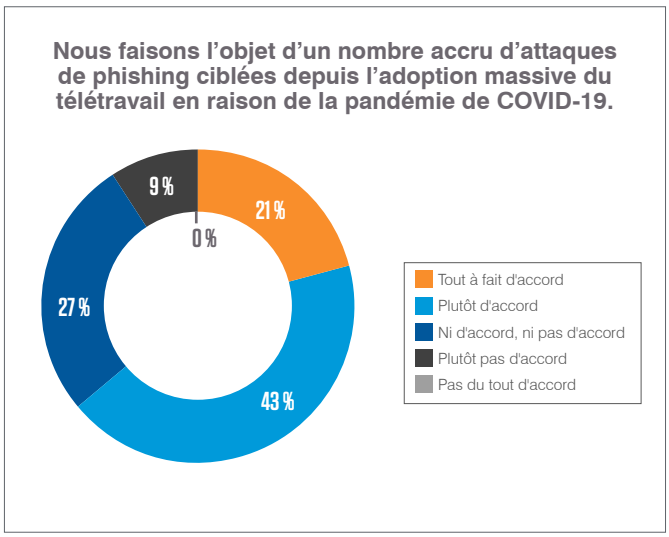
La transition vers le télétravail a rendu nos systèmes et applications obsolètes et peu efficaces pour nous protéger contre les cybermenaces actuelles.

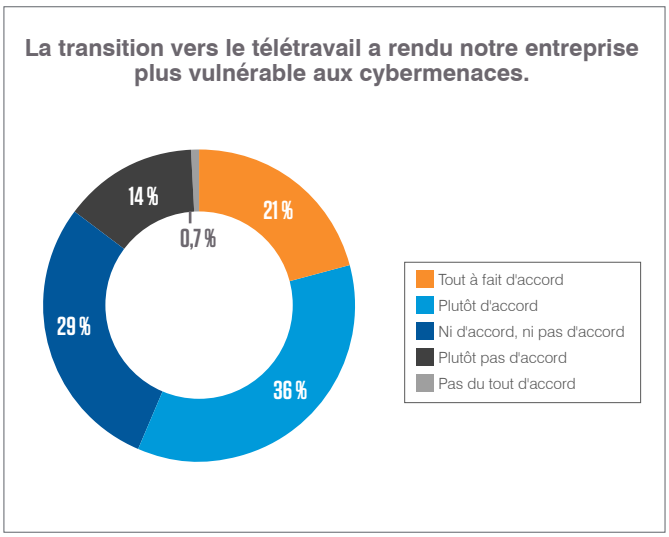


Les cybercriminels exploitent des collaborateurs en télétravail de plus en plus vulnérables

Cette lutte pour conserver des cyberdéfenses efficaces malgré la généralisation du télétravail n'a pas manqué d'attirer l'attention des cybercriminels. Bon nombre d'entre eux recourent activement à des leurres liés au coronavirus pour dérober des identifiants de connexion et autres informations sensibles à des victimes peu méfiantes.

À la question de savoir s'ils ont constaté une augmentation du nombre de tentatives d'attaques de phishing depuis le passage au télétravail, près de deux tiers (64 %) des RSSI ont répondu par l'affirmative. Seuls 9 % d'entre eux ont répondu que ce n'était pas le cas.





L'extension de la surface d'attaque, la multiplication des attaques et le manque de moyens des collaborateurs augmentent l'exposition des entreprises françaises.

Plus de la moitié (57 %) des RSSI français reconnaissent que l'adoption du télétravail les a rendus plus vulnérables aux cyberattaques. Seuls 15 % d'entre eux ne sont pas d'accord.

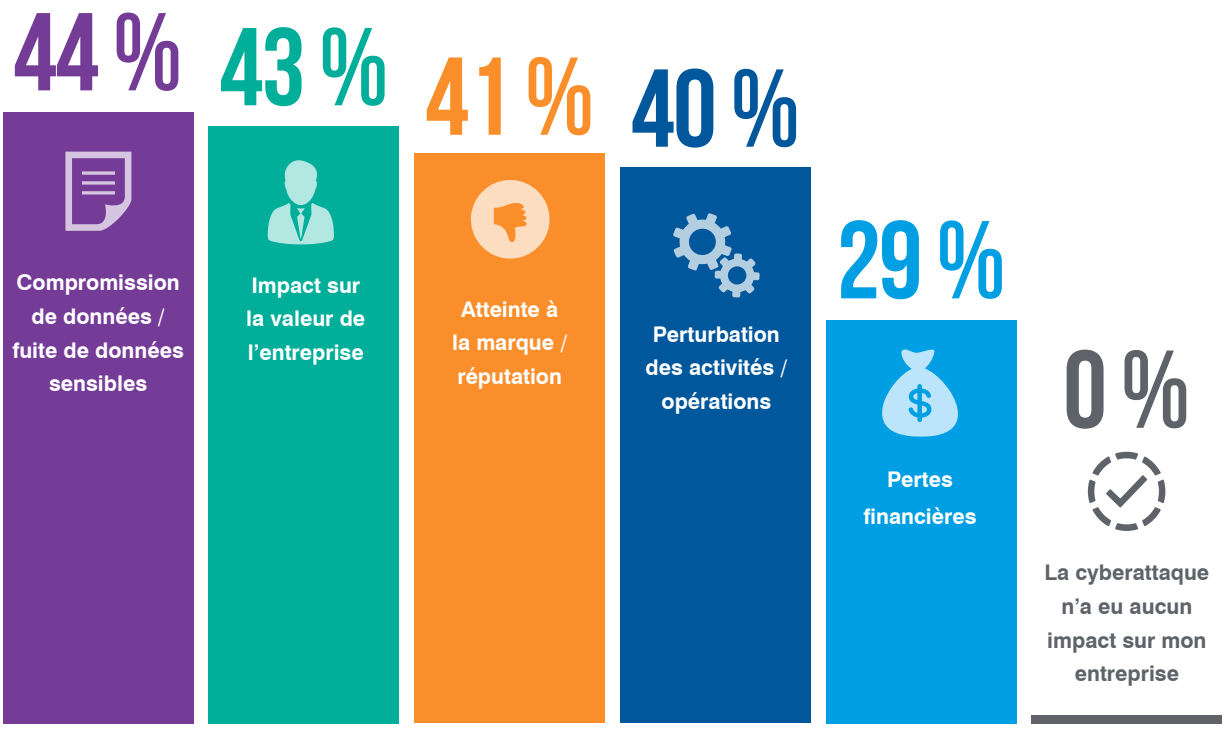
CONCLUSION N° 3 : LA FUITE DE DONNÉES ET L'IMPACT SUR LA VALEUR DE L'ENTREPRISE SONT LES PRINCIPALES CONSÉQUENCES DES CYBERATTAQUES

Les cyberattaques peuvent avoir des conséquences dramatiques sur les entreprises touchées. Le Forum économique mondial estime qu'entre 2019 et 2023, la valeur globale mise en péril par les cybercriminels s'élèvera à 5 200 milliards de dollars.

Ces pertes ont plusieurs causes, notamment la baisse des revenus, les temps d'arrêt, les frais juridiques, les dédommagements et la remédiation, ainsi que l'atteinte à la valeur de la marque.

Bien que les pertes financières directes demeurent une source de préoccupation, les RSSI français considèrent la fuite de données (44 %), l'impact sur la valeur de l'entreprise (43 %) et l'atteinte à la réputation (41 %) comme les principales conséquences des cyberattaques.

Le cas échéant, quelles ont été les conséquences de la cyberattaque subie pour votre entreprise ? (Cochez toutes les réponses pertinentes.)



Autre (veuillez préciser) 0 %

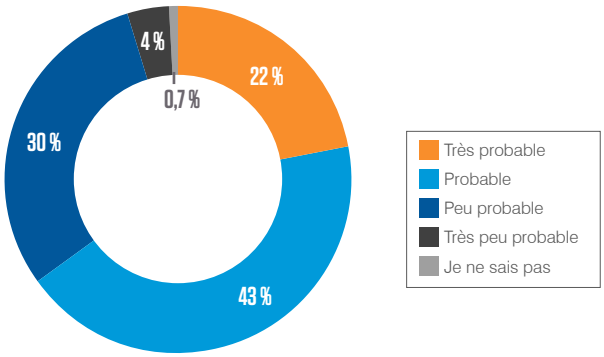
CONCLUSION N° 4 : LES ENTREPRISES FRANÇAISES SONT CONSCIENTES DES RISQUES AUXQUELS ELLES SONT CONFRONTÉES, MAIS SE SENTENT TOUT DE MÊME MAL PRÉPARÉES

Les entreprises françaises sont parfaitement conscientes des risques auxquels elles sont confrontées dans le vaste paysage de la cybersécurité, ainsi que de la façon dont les cybercriminels les ciblent.

Plus de deux tiers (65 %) des RSSI français estiment que leur entreprise risque d'être la cible d'une cyberattaque au cours des 12 prochains mois. Toutefois, le fait que près d'un tiers des participants à l'étude pensent qu'une attaque est peu probable est préoccupant.

Seulement 14 % des entreprises sont persuadées d'être prêtes à faire face à une cyberattaque

Selon vous, quelle est la probabilité que votre entreprise soit victime d'une cyberattaque au cours des 12 prochains mois ?



S'il est encourageant de constater que la majorité des décideurs en cybersécurité sont parfaitement conscients des risques et des difficultés auxquels ils sont confrontés, le manque d'intérêt des entreprises à l'égard de leur niveau de cybersécurité est surprenant.

Plus de la moitié (56 %) des RSSI français estiment que la direction de leur entreprise ne prête pas assez attention à sa stratégie de cybersécurité, et seuls 14 % d'entre eux sont persuadés que leur entreprise est prête à faire face à une cyberattaque.

Dans quelle mesure êtes-vous d'accord avec les affirmations suivantes ?

	Tout à fait d'accord	Plutôt d'accord	Ni d'accord, ni pas d'accord	Plutôt pas d'accord	Pas du tout d'accord
Mon entreprise est prête à faire face à une cyberattaque.	14 %	33 %	37 %	15 %	0,7 %
La direction de mon entreprise ne prête pas assez attention à la mise en place d'une stratégie de cybersécurité efficace.	15 %	41 %	28 %	15 %	0,7 %

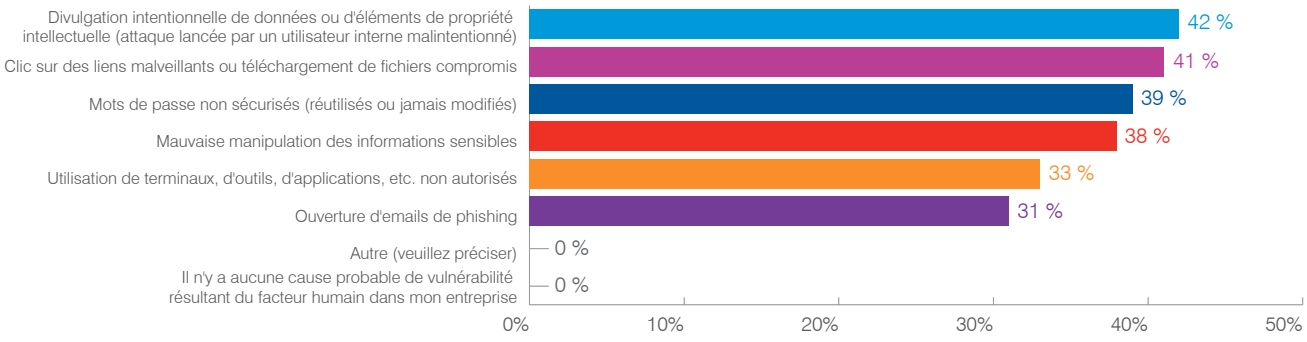
CONCLUSION N° 5 : LES COLLABORATEURS NE DISPOSENT PAS DES MOYENS NÉCESSAIRES POUR CONTRER LES CYBERATTAQUES

Bien que les utilisateurs constituent une dernière ligne de défense contre les cyberattaques, le personnel des entreprises françaises affiche une connaissance déficiente de la sécurité et n'y est pas assez sensibilisé. Les RSSI sont bien conscients de cette faille dans leurs défenses. En fait, 61 % d'entre eux estiment que le facteur humain représente la principale vulnérabilité de leur entreprise.

	Tout à fait d'accord	Plutôt d'accord	Ni d'accord, ni pas d'accord	Plutôt pas d'accord	Pas du tout d'accord
Le facteur humain représente la principale vulnérabilité de mon entreprise.	20 %	41 %	27 %	11 %	0,7 %

Les comportements des collaborateurs les plus susceptibles d'entraîner une cyberattaque sont la divulgation intentionnelle de données (42 %), suivie des clics sur des liens malveillants (41 %), une erreur que 10 % des utilisateurs admettent commettre, les mauvaises pratiques en matière de mots de passe (39 %), la mauvaise manipulation des informations sensibles (38 %), l'utilisation d'applications et de terminaux non autorisés (33 %) et l'ouverture d'emails de phishing (31 %).

Quelles sont les causes les plus probables d'une vulnérabilité résultant du facteur humain dans votre entreprise, le cas échéant ? (Cochez au maximum trois réponses.)



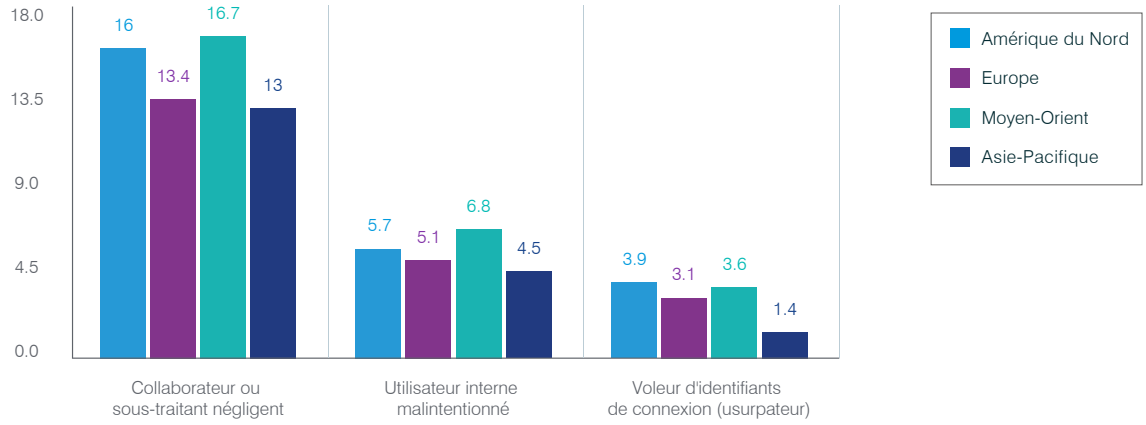
Les menaces internes sont en plein essor

Il est frappant de constater que près de la moitié des entreprises françaises considèrent les utilisateurs internes malintentionnés comme la cause la plus probable de vulnérabilité.

Partout dans le monde, les menaces internes représentent une préoccupation croissante pour les entreprises. En effet, le nombre d'incidents a grimpé de 47 % en seulement deux ans.

L'étude 2020 du Ponemon Institute sur le coût des menaces internes montre que les entreprises européennes font face à des taux élevés de négligence de la part des sous-traitants, de menaces internes et de vols d'identifiants de connexion.

Fréquence moyenne des incidents pour les trois profils

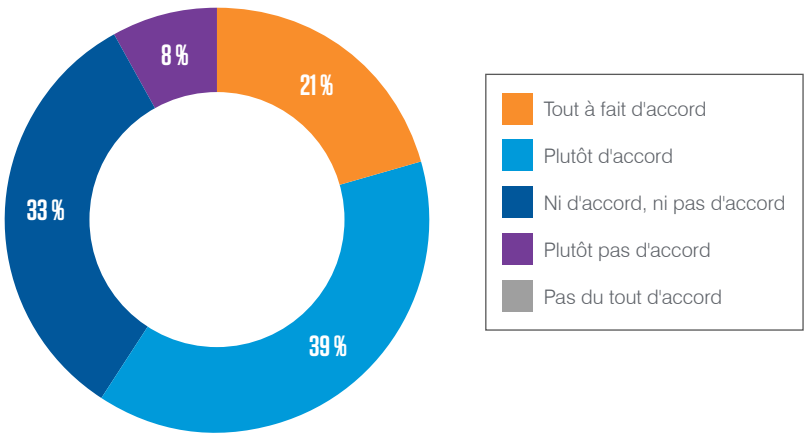


La source: Ponemon Institute 2020 Cost of Insider Threats Global Report

La sensibilisation des collaborateurs à la cybersécurité est sous le feu des projecteurs

Les RSSI français sont parfaitement conscients des menaces et des vecteurs d'attaque courants. Près de deux tiers (60 %) d'entre eux pensent que, malgré toutes les solutions de sécurité mises en place, le facteur humain et le manque de compétences des collaborateurs représentent le plus grand risque pour les entreprises.

Peu importe les solutions de cybersécurité mises en place, le facteur humain et le manque de sensibilisation à la cybersécurité (des collaborateurs ou des tiers au sein de mon écosystème) représentent le plus grand risque pour mon entreprise.



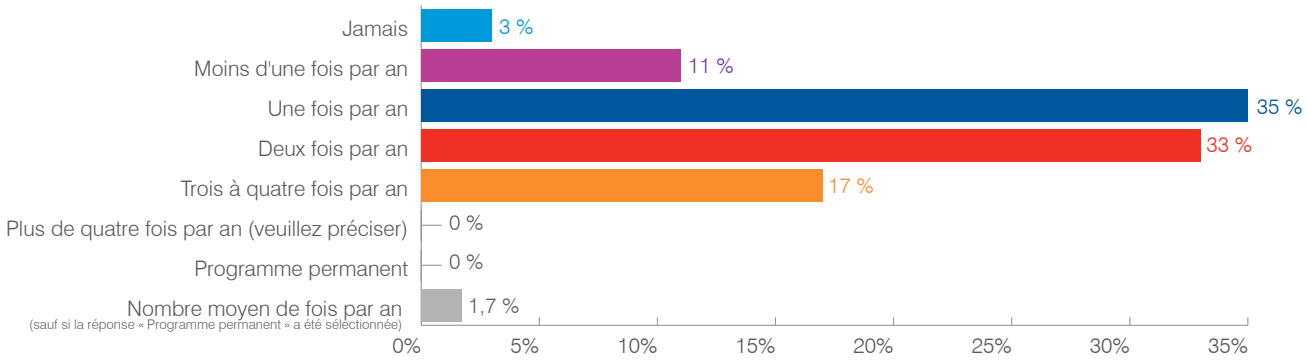
Si les RSSI français sont conscients des risques que les collaborateurs peuvent représenter pour leur entreprise, ils ignorent en revanche qui sont les personnes les plus ciblées. À la question de savoir s'ils savaient qui étaient les collaborateurs les plus à risque au sein de leur entreprise, plus de la moitié (53 %) ont répondu qu'ils l'ignoraient.

Pourtant, les programmes de formation et de sensibilisation à la cybersécurité de nombreuses entreprises françaises (ou l'absence de tels programmes) ne tiennent pas compte de ce degré de sensibilisation. Malgré l'évolution rapide du paysage des menaces, la majorité (82 %) des entreprises indiquent former leurs collaborateurs aux bonnes pratiques de cybersécurité deux fois par an ou moins régulièrement, tandis que 17 % d'entre elles proposent un programme complet trois fois par an ou plus régulièrement.

En revanche, un certain nombre d'entreprises adaptent leur formation de sensibilisation à la cybersécurité aux enjeux actuels liés à la pandémie. 14 % d'entre elles affirment notamment avoir mis en place une formation supplémentaire sur la sécurité dans le cadre du télétravail.

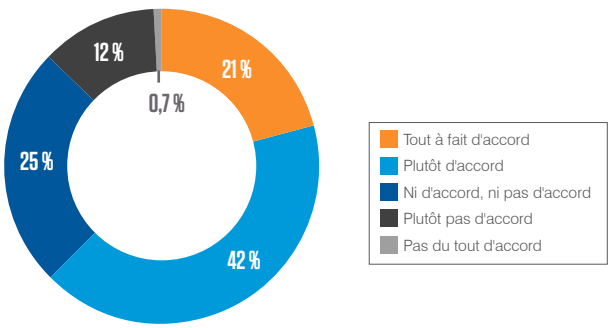
Une formation complète et régulière est essentielle pour assurer la protection des entreprises. Tous les programmes doivent être régulièrement évalués afin de s'assurer qu'ils restent pertinents et s'adaptent au paysage des menaces en constante évolution. La formation des collaborateurs et leur sensibilisation aux dernières menaces font souvent la différence entre l'échec et la réussite d'une cyberattaque. En ne mettant pas en place de tels programmes ou en ne les évaluant pas régulièrement, les entreprises s'exposent dangereusement.

En moyenne, à quelle fréquence formez-vous et sensibilisez-vous vos collaborateurs aux bonnes pratiques de cybersécurité, le cas échéant ?

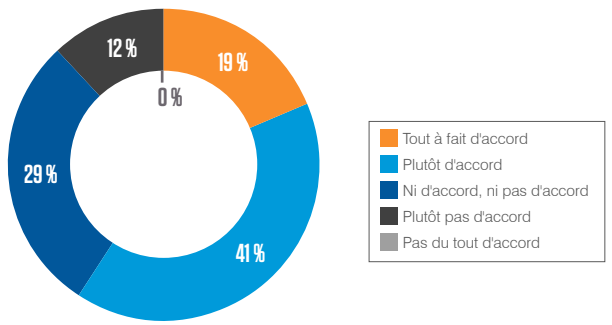


Cette question donne la migraine à de nombreux décideurs en cybersécurité français. Près de deux tiers (63 %) d'entre eux estiment que le programme de formation à la cybersécurité de leur entreprise doit être amélioré. Malheureusement, la majorité (60 %) d'entre eux pensent que le manque de temps et de ressources est le principal obstacle à la concrétisation de cet objectif.

Notre programme de formation et de sensibilisation à la cybersécurité doit faire l'objet d'améliorations pour être plus efficace.



Le manque de temps/ressources est le principal obstacle à la mise en place d'un programme de sensibilisation à la cybersécurité plus efficace au sein de mon entreprise.



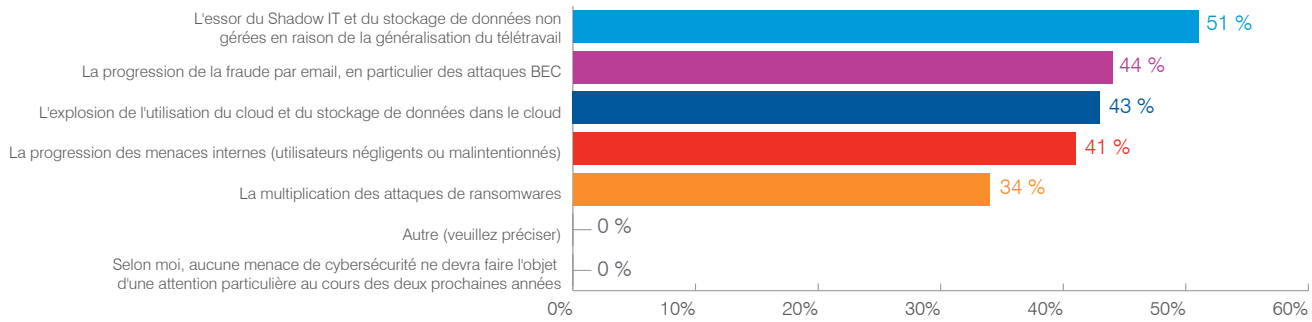
CONCLUSION N° 6 : L'AVENIR DES CYBERRISQUES EN FRANCE

Adaptation des stratégies de cybersécurité à l'évolution des vecteurs d'attaque

51 % des RSSI français pensent que l'essor du Shadow IT (informatique de l'ombre) et du stockage de données non gérées en raison de la généralisation du télétravail constituera probablement l'une des principales menaces de cybersécurité au cours des deux prochaines années, suivi par la progression de la fraude par email, en particulier des attaques BEC.

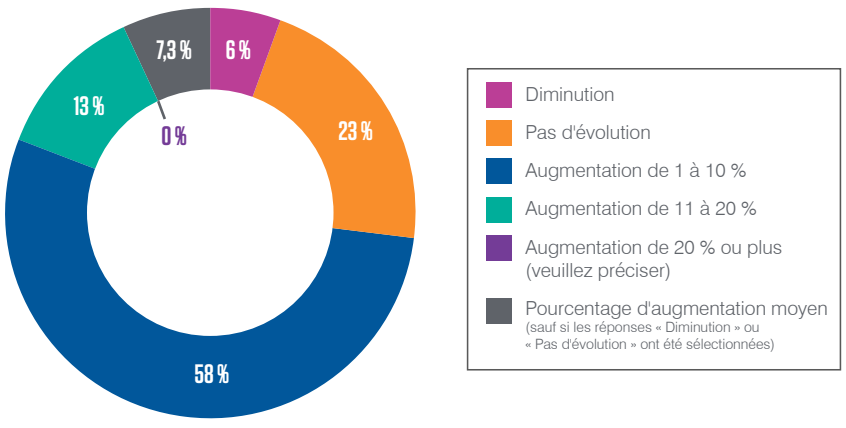
Les défis associés à l'explosion de l'utilisation du cloud et du stockage dans le cloud (43 %), à la progression des menaces internes (41 %) et à la multiplication des attaques de ransomwares (34 %) devraient également représenter une menace permanente au cours des 12 prochains mois.

En dehors de votre entreprise, quelles seront selon vous les principales menaces de cybersécurité au cours des deux années à venir ? (Cochez au maximum trois réponses.)



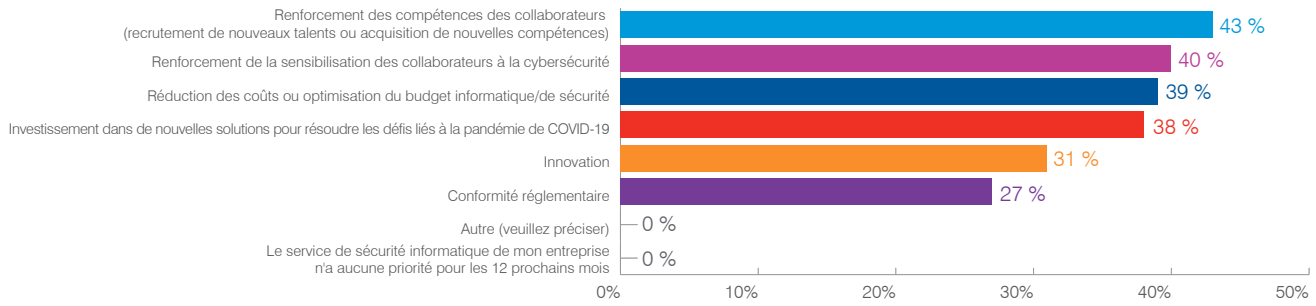
Ce paysage des menaces en constante évolution requiert l'adaptation des cyberdéfenses et une réévaluation constante des priorités stratégiques des entreprises. La plupart (71 %) des RSSI français s'attendent à une augmentation des investissements dans la cybersécurité à l'appui de cette stratégie adaptative. Seuls 6 % d'entre eux prévoient une diminution de leur budget de cybersécurité, tandis que 23 % estiment qu'il n'évoluera ni dans un sens, ni dans l'autre.

Selon vous, comment votre budget de sécurité évoluera-t-il au cours des deux prochaines années, le cas échéant ?



Les investissements devraient se concentrer sur plusieurs domaines. Les RSSI français vont chercher à combler le déficit de connaissances et de sensibilisation des utilisateurs en développant les compétences des collaborateurs ou en recrutant de nouveaux talents (43 %), ainsi qu'en renforçant la formation et la sensibilisation (40 %).

Quelles sont les trois principales priorités du service de sécurité informatique de votre entreprise pour les 12 prochains mois ? (Cochez au maximum trois réponses.)



D'après les prévisions, la pandémie de COVID-19 devrait également avoir un effet durable sur les stratégies numériques des entreprises françaises. Si 61 % des RSSI français reconnaissent dans une certaine mesure que la pandémie a accéléré la transformation numérique de leur entreprise, 59 % d'entre eux estiment que la crise mondiale pourrait limiter leurs dépenses futures dans la cybersécurité.

CONCLUSION

Quel que soit le vecteur d'attaque (messagerie électronique, applications cloud, Web ou réseaux sociaux), les cybercriminels continuent à tirer parti du facteur humain.

Qu'il s'agisse d'imposteurs se faisant passer pour des collègues de confiance ou d'emails de phishing de plus en plus convaincants contenant des liens malveillants, ce sont les utilisateurs qui sont en première ligne de la guerre contre la cybercriminalité.

C'est la raison pour laquelle vous devez impérativement adopter une stratégie centrée sur les personnes. Pour cela, vous devez commencer par identifier vos utilisateurs les plus vulnérables et vous assurer qu'ils disposent des connaissances et des outils nécessaires pour défendre votre entreprise.

Outre les contrôles et solutions techniques, votre stratégie de défense doit reposer sur un programme de formation complet. Les formations doivent être complètes, régulières et adaptatives et couvrir un large éventail de sujets, des motivations des cybercriminels et des mécanismes employés à la façon dont des comportements en apparence aussi inoffensifs que la réutilisation d'un mot de passe ou un niveau inadéquat de protection des données peuvent augmenter le risque d'attaque.

> *« Les cybercriminels sont déterminés et perfectionnent constamment leurs compétences et les techniques qu'ils emploient. Vous devez faire de même si vous voulez avoir une chance de les tenir en échec. »*
>
> **(Loïc Guézo, Cybersecurity Strategy, Proofpoint)**

Les cybercriminels sont déterminés et perfectionnent constamment leurs compétences et les techniques qu'ils emploient. Vous devez faire de même si vous voulez avoir une chance de les tenir en échec.

Toutes les données, sauf indication contraire, font référence à l'enquête menée par Censuswide auprès de 150 RSSI en France en octobre 2020.
Censuswide emploie des membres de la Market Research Society, dans le respect des principes d'ESOMAR.

proofpoint®

Pour découvrir comment Proofpoint peut vous aider à protéger votre entreprise, visitez notre site à l'adresse : www.proofpoint.com/fr.

A PROPOS DE PROOFPOINT

Proofpoint, Inc. (NASDAQ:PFPT) est une entreprise leader dans le domaine de la cybersécurité et de la conformité qui protège les ressources les plus importantes et les plus à risques des entreprises : leurs collaborateurs. Grâce à une suite intégrée de solutions cloud, Proofpoint aide les entreprises du monde entier à stopper les menaces ciblées, à protéger leurs données et à rendre leurs utilisateurs plus résistants face aux cyberattaques. Les entreprises de toutes tailles, y compris plus de la moitié des entreprises de l'index Fortune 1000, font confiance aux solutions de sécurité et de conformité de Proofpoint centrées sur les individus, pour diminuer leurs risques les plus critiques en matière de sécurité et de conformité via les emails, le cloud, les réseaux sociaux et le Web. Pour plus d'informations, rendez-vous sur www.proofpoint.com