ivanti

Les menaces cachées en 2023

L'impact des données démographiques des collaborateurs sur la posture de sécurité des organisations

S'inscrit dans la série Ivanti de rapports sur l'état de la cybersécurité.

Les données démographiques, une mine d'informations à explorer

Dans les entreprises, la sécurité descendante et à « taille unique » ne tient pas compte des risques spécifiques liés à la situation géographique, à l'âge, au genre et à la fonction des collaborateurs, entre autres facteurs.

Dans ce nouveau rapport d'Ivanti, nous faisons table rase des moyennes trop générales et examinons tous les aspects, des comportements risqués des collaborateurs (les moins prudents ne sont pas ceux que vous croyez) aux incohérences dans la culture de sécurité de votre organisation.

Ivanti a interrogé plus de 6 500 dirigeants, professionnels de la cybersécurité et collaborateurs de bureau partout dans le monde pour comprendre :

L'attitude des collaborateurs face à la cybersécurité et leur perception de leur rôle dans la protection de l'entreprise

Le diagnostic des professionnels de la sécurité concernant les principales problématiques et vulnérabilités

Le comportement technologique des dirigeants, ainsi que leur niveau d'adhésion à la stratégie de cybersécurité

ivanti

Sommaire :

ivanti

Méthodologie

Ivanti a interrogé plus de 6 500 dirigeants, professionnels de la cybersécurité et collaborateurs de bureau au 4e trimestre 2022 pour comprendre les risques d'aujourd'hui et savoir comment les entreprises se préparent aux menaces futures encore inconnues.

Dans ce rapport, nous étudierons comment la démographie spécifique des utilisateurs finaux des organisations impacte leur attitude et leur comportement personnels... et comment ces variations peuvent présenter des risques avancés susceptibles d'être exploités par les acteurs de la menace.

Démographie des personnes interrogées :

5 202
Collaborateurs de bureau
Collaborateurs de bureau ≤40 ans : 3 609
Collaborateurs de bureau >40 ans : 2 769

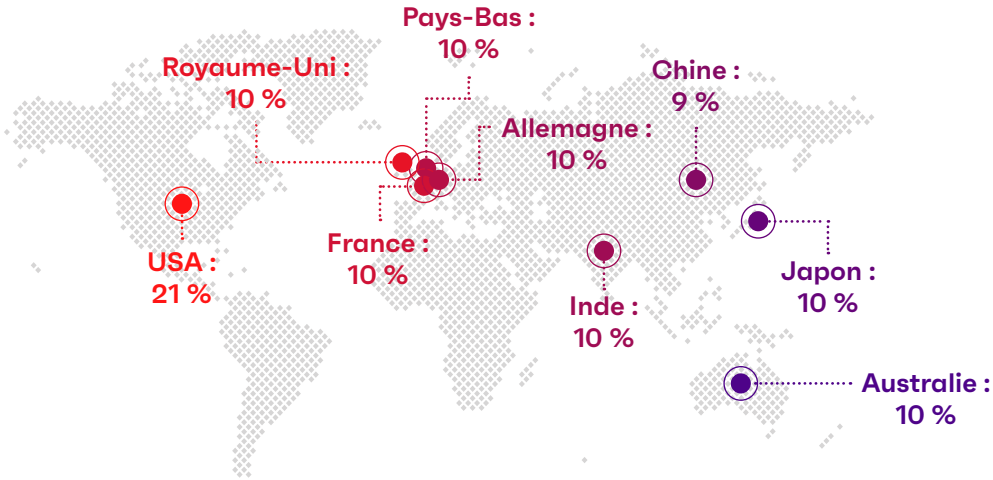
902
Professionnels de la sécurité

454
Dirigeants exécutifs

3 414
Femmes

3 119
Hommes

27
Non binaires/ Préfèrent ne pas répondre



01

Le mythe générationnel :

Les plus jeunes ont-ils un comportement plus éclairé en matière de sécurité ?

ivanti

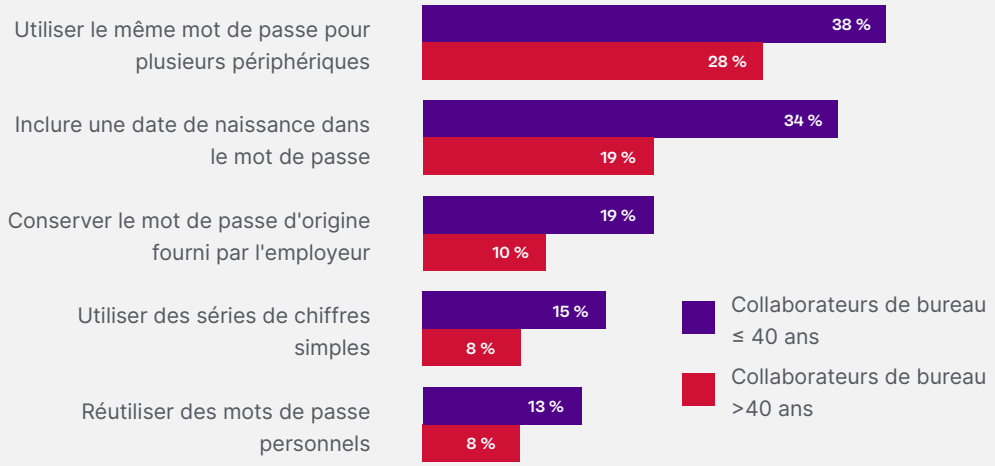
Problème actuel

Nombreux sont ceux qui pensent que les collaborateurs les plus âgés maîtrisent moins bien la technologie, et qu'ils sont donc plus susceptibles d'avoir un comportement risqué. En fait, c'est le contraire.

Les professionnels les plus jeunes (moins de 40 ans) sont bien plus susceptibles d'ignorer des consignes de sécurité importantes que leurs collègues de la génération X ou plus âgés. C'est vrai pour l'application d'une bonne hygiène de mots de passe, les clics sur des liens d'hameçonnage, et le partage de périphériques avec les amis et la famille.

Les collaborateurs de bureau les plus jeunes ont davantage tendance à avoir des habitudes de sécurité dangereuses.

Q : Après qu'on vous ait demandé de créer un mot de passe de connexion au travail, lesquelles de ces opérations avez-vous exécutées ces deux dernières années ?



	Collaborateurs de bureau ≤ 40 ans	Collaborateurs de bureau >40 ans
A cliqué sur un lien d'hameçonnage qui le ciblait	13 %	8 %
A partagé un ou plusieurs périphériques professionnels avec la famille ou les amis	34 %	19 %

Pourquoi c'est important

Ces oublis, ces erreurs et ces contournements s'ajoutent à des vulnérabilités de sécurité nettement plus élevées chez les collaborateurs les plus jeunes.

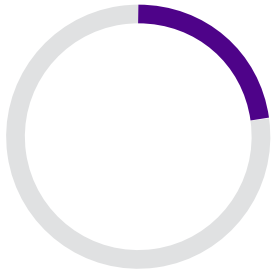
Les stéréotypes concernant la maîtrise de la technologie en fonction de l'âge peuvent induire les organisations en erreur. Et le problème ne se limite pas à la cyberhygiène (habitudes concernant les mots de passe, partage de périphériques, etc.). Les recherches montrent que les collaborateurs les plus jeunes sont également moins susceptibles de mentionner les signaux d'alarme lorsqu'ils les rencontrent.

Parmi les travailleurs de 40 ans et moins, 23 % disent n'avoir pas signalé le dernier e-mail ou message d'hameçonnage qu'ils ont reçu. Par comparaison, les plus de 40 ans qui ne les ont pas signalés sont seulement 12 %.

Quelle est la cause la plus fréquente de cette absence de signalisation ?

« J'ai pensé que ce n'était pas important. »

Collaborateurs de bureau qui n'ont PAS signalé à la sécurité le dernier message d'hameçonnage reçu



Collaborateurs de bureau ≤ 40 ans

Collaborateurs de bureau >40 ans

Les stéréotypes sur les collaborateurs âgés sont particulièrement insidieux, car les travailleurs du secteur technologique sont plus jeunes, et sont donc plus susceptibles de croire que leurs collègues plus âgés sont mal informés ou vulnérables.

Par exemple, une étude menée auprès de 2 250 professionnels au Royaume-Uni a montré que les travailleurs du secteur technologique considèrent leurs collègues comme « dépassés » et « trop vieux pour leur travail » lorsqu'ils atteignent 38 ans.[1]

(Attention, cela s'applique aux professions technologiques, pas au collaborateur moyen, souvent moins averti des technologies.)

Ces résultats soulignent que les organisations doivent moins s'appuyer sur le jugement personnel des collaborateurs et davantage sur la technologique qui facilite le respect des règles.

Mieux encore : les organisations doivent envisager de déployer des systèmes automatisés qui s'exécutent entièrement en arrière-plan sans que les utilisateurs finaux connaissent leur existence.

« Considérer que les collaborateurs les plus jeunes sont plus conscients de la sécurité et maîtrisent mieux les technologies, c'est une vision dépassée et souvent dangereuse. Les entreprises doivent tester la véracité de ces suppositions en menant des recherches internes pour connaître l'attitude de leurs propres collaborateurs envers les risques de sécurité et leur rôle pour les contrer. »

Daniel Spicer
Chief Security Officer chez Ivanti

02

Les réactions face aux incidents :

Tendances de signalisation des incidents par séniorité, genre et région

ivanti

Problème actuel

Pour protéger une organisation, il faut obtenir des informations en temps quasi réel sur les incidents ou failles de sécurité. Notre étude dévoile que certains collaborateurs sont moins enclins à mentionner les signaux d'alarme.

Vos collaborateurs signalent-ils rapidement leurs problèmes de sécurité ? L'étude d'Ivanti montre que certaines catégories de collaborateurs peuvent hésiter à communiquer leurs problèmes… c'est un point dont les entreprises doivent tenir compte lorsqu'elles développent des programmes de sensibilisation et de formation.

Séniorité

La variable d'évolution la plus importante de ces tendances de signalisation des incidents est la séniorité. 72 % des dirigeants que nous avons interrogés disent avoir contacté le personnel de sécurité pour une question ou une inquiétude, contre seulement 28 % du personnel de bureau.

Genre

Les femmes sont moins enclines que les hommes à signaler les incidents. 28 % ont contacté un professionnel de cybersécurité pour une question ou une inquiétude, contre 36 % des hommes.

Le saviez-vous ?

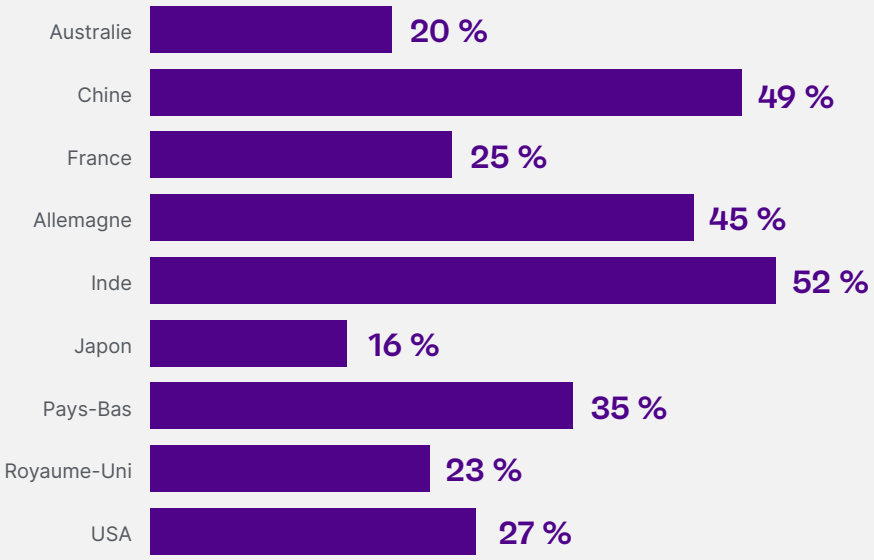
Les dirigeants sont deux fois plus susceptibles de dire que leurs interactions avec l'équipe Sécurité sont « maladroites » ou « embarrassantes » que les employés de bureau.[2]

Ces échanges plus fréquents mais négatifs avec l'équipe Sécurité peuvent encourager les dirigeants à solliciter un support technique externe non approuvé… d'après le rapport, 4 fois plus souvent que les employés de bureau.

L'inclinaison des utilisateurs à contacter la sécurité varie considérablement d'un pays à l'autre.

Par exemple, en Chine, près de la moitié des collaborateurs de bureau a contacté l'équipe de sécurité pour une question ou une inquiétude, contre seulement 20 % en Australie.

Personnel de bureau ayant contacté l'équipe Sécurité pour une question ou une inquiétude, par région



Pourquoi c'est important

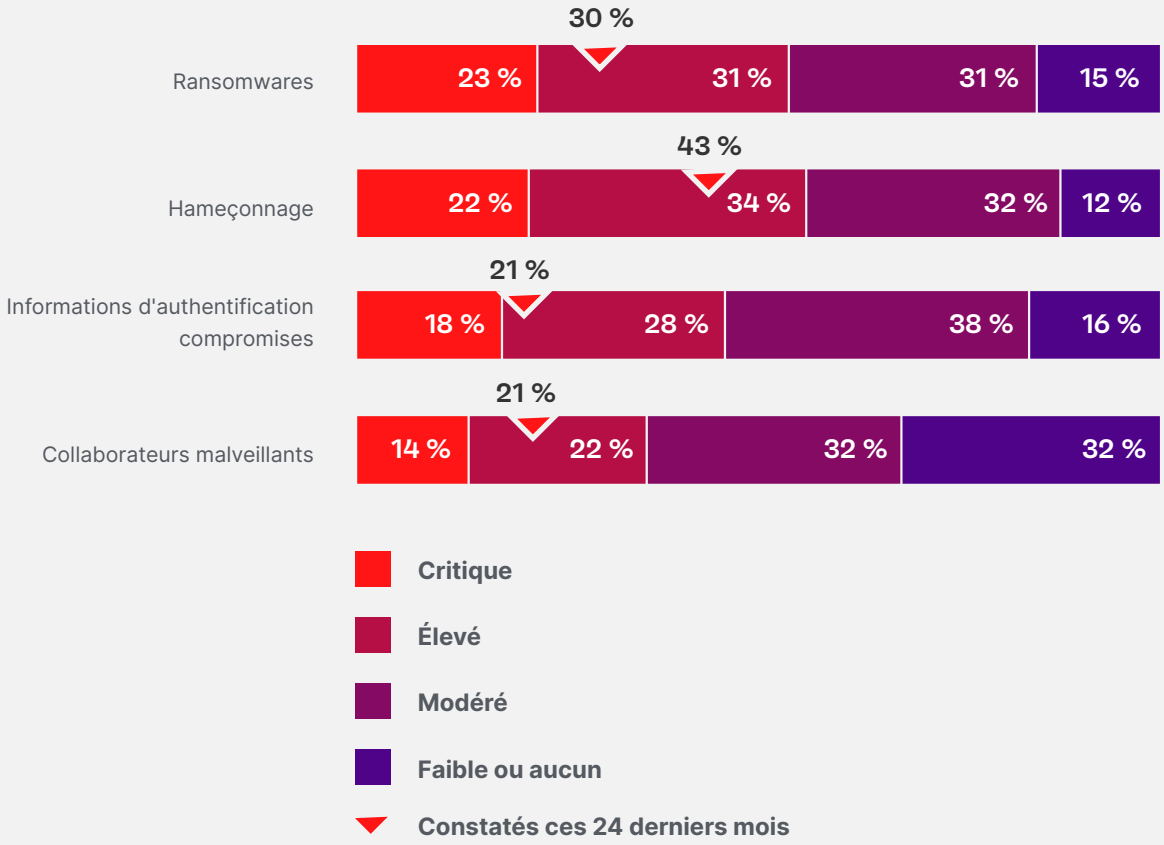
Votre sécurité dépend de milliers de collaborateurs qui doivent jouer en défense. Ces collaborateurs savent-ils qu'ils sont des membres précieux de l'équipe de sécurité étendue ?

Dans le cadre de son rapport sur l'état de la cybersécurité, Ivanti a interrogé les professionnels de la sécurité sur leurs plus grandes vulnérabilités à l'échelle du secteur. Le ransomware et l'hameçonnage arrivent en 1re et 2e positions.

Et ces menaces deviennent de plus en plus dangereuses chaque année, surtout en raison des progrès de l'IA générative, qui rend l'hameçonnage plus difficile à détecter.

Les menaces et faiblesses de sécurité qui viennent en tête ciblent particulièrement vos collaborateurs d'où la nécessité de les protéger

Q : Évaluez le niveau de menace prévu en 2023 dans votre secteur pour chacun des éléments suivants...



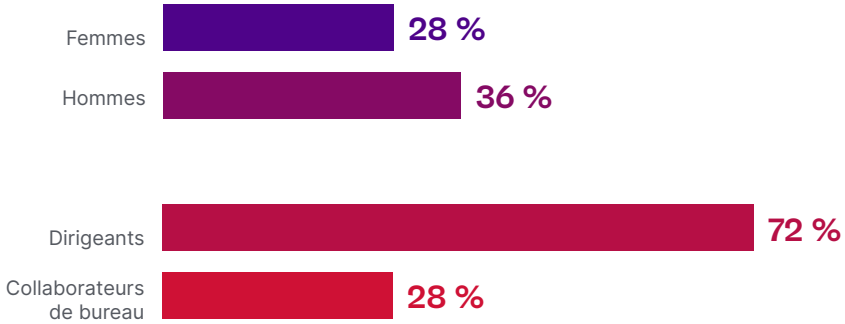
Face à l'accélération des menaces et à l'augmentation des risques, vos collaborateurs doivent se sentir à l'aise pour contacter votre équipe de sécurité… même si la seule « preuve » d'attaque imminente dont ils disposent est un doute tenace.

(Exemples : demande de virement bancaire inhabituelle, relance de facture suspecte ou lien de réinitialisation du mot de passe non sollicité.)

Après tout, lors d'un incident de sécurité actif, la vitesse de réaction est vraiment le facteur le plus important pour vous protéger d'une attaque.

En définitive, quand les employeurs enquêtent sur le ressenti des collaborateurs pour comprendre leur attitude, ils doivent approfondir leurs profils démographiques et leurs vulnérabilités.

Utilisateurs ayant contacté la sécurité pour une question ou une inquiétude



« Nous avons subi quelques tentatives d'hameçonnage avancées et les collaborateurs ignoraient totalement qu'ils étaient ciblés. Ce type d'attaque est devenu tellement plus sophistiqué au cours des deux dernières années… même nos collaborateurs les plus expérimentés tombent dans le piège. »

— Personne répondant à l'enquête 2023 « Repartez sur de nouvelles bases » [3]

03

Les critères géographiques :

Selon le pays de résidence des collaborateurs, des différences se rencontrent dans les formations dispensées et dans les postures de la sécurité

ivanti

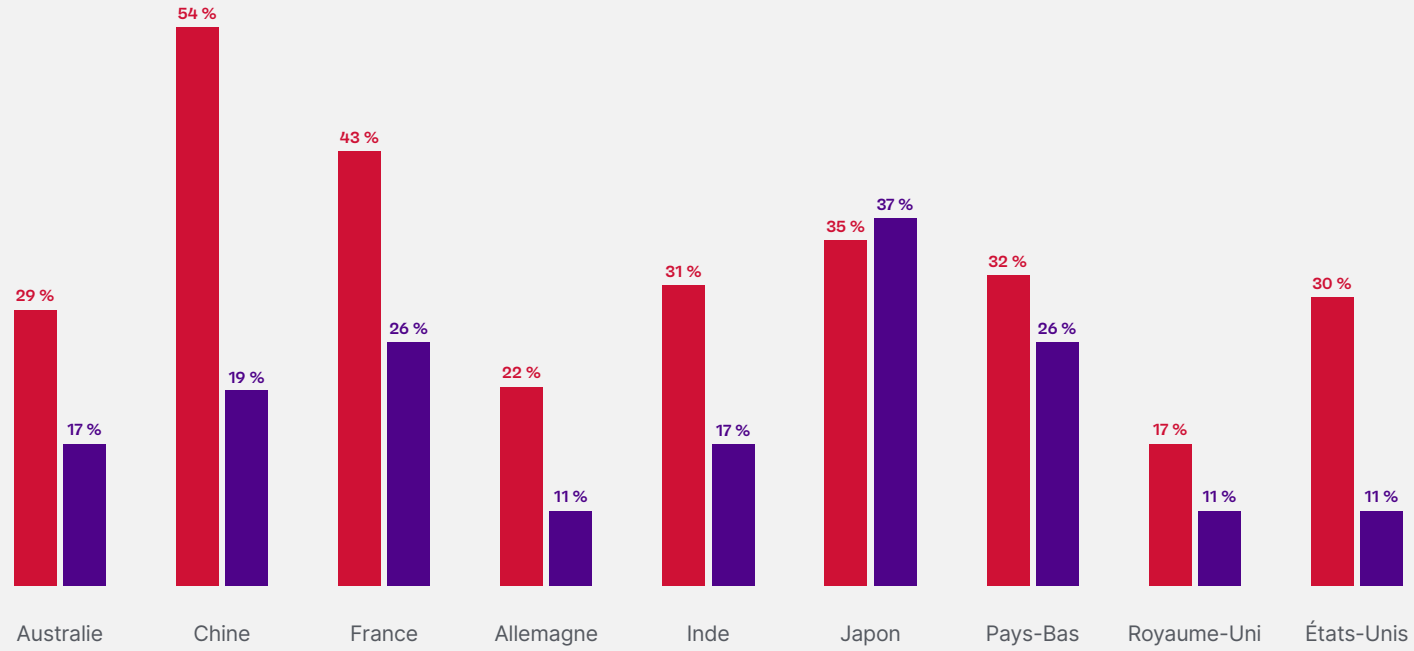
Problème actuel

La culture de sécurité et les programmes de formation d'une organisation influent significativement sur la préparation à la sécurité, mais nos études montrent qu'il existe des différences entre les pays.

L'enquête d'Ivanti révèle d'importantes différences dans la culture de sécurité de chaque pays… à la fois concernant la formation dispensée par l'organisation, et l'attitude des dirigeants et du personnel de bureau.

Variations régionales de la formation et de l'attitude envers la cybersécurité

- « Mon entreprise ne fournit AUCUNE formation obligatoire à la cybersécurité. »
- « Non, je ne me sentirais pas à l'aise [pour signaler une erreur à l'équipe Sécurité.] »



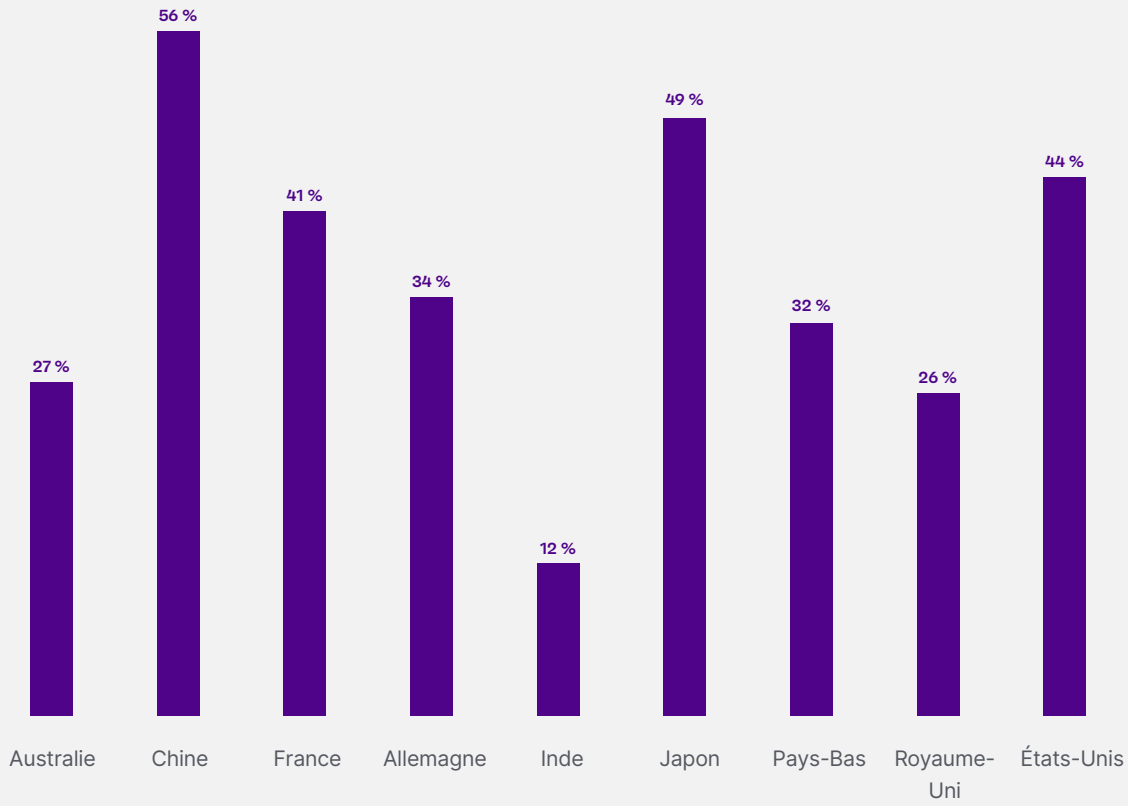
Pourquoi c'est important

La plupart des organisations ont une approche descendante de la formation et de la culture de sécurité, mais les études montrent qu'il est primordial de comprendre la culture de sécurité locale (et même, la culture du pays) pour établir un plan cohérent.

D'où qu'ils viennent, tous les nouveaux collaborateurs apportent dans l'entreprise leurs propres vulnérabilités, volontairement ou non. Des collaborateurs mal formés risquent de faire baisser le niveau global de préparation de l'entreprise.

Pour atténuer ce risque, les entreprises doivent investir dans de puissants programmes de formation à la sécurité, lors de l'onboarding et en continu, tant au niveau international que régional.

Collaborateurs de bureau : « Mes actions n'ont AUCUN impact sur la capacité de mon entreprise à se protéger [des cybermenaces]. »



Comment la culture locale interagit avec les programmes de sécurité internationaux

La culture peut influer sur la façon dont l'organisation protège ses actifs et son personnel, ainsi que sur sa façon de réagir aux attaques.

Problèmes culturels possibles concernant la sécurité

Inconfort des collaborateurs face à la formation fournie au niveau international (ex., mauvaise traduction des supports de formation dans la langue et la culture locales).

Malaise des salariés face aux nouvelles normes ou règles qui n'ont pas été « socialement adaptées » aux usages locaux.

Culture de bureau locale descendante, qui laisse peu de place aux individus pour signaler des erreurs ou des inquiétudes.

Support de sécurité insuffisant pour les bureaux locaux. Par exemple, les collaborateurs qui ont une question ou une inquiétude doivent contacter un technicien de sécurité dans un autre pays... avec les barrières de langue et de culture que cela entraîne.

« Ces différences entre les divers pays constituent un angle intéressant pour l'étude du niveau de préparation.

Il est facile (et courant) pour l'équipe Sécurité d'évaluer la sécurité d'après ce qui se passe dans son bureau, plus ou moins près d'elle.

Nos recherches montrent combien il est important d'explorer les données plus en détail et de connaître les procédures de sécurité de tous les sites (siège social, installations R&D, avant-postes de supply chain ou sites de production. »

Daren Goeson
SVP, Product Management chez Ivanti

04

Comment réagir :

Comment prendre en compte les données démographiques sur les utilisateurs finaux dans votre stratégie de sécurité

ivanti

Comment réagir

Une image globale d'excellence peut cacher des poches de risque.

Explorons en détail les risques de sécurité en lien avec les données démographiques. Interrogez-vous sur la façon dont vous pouvez évaluer les risques démographiques dans votre organisation, et comment ajuster votre approche pour y remédier correctement.

5 façons d'atténuer les risques cachés

1. ### Effectuez des enquêtes auprès de vos collaborateurs.

   Comparez les attitudes et comportements de vos utilisateurs en matière de sécurité aux résultats obtenus à l'échelle internationale.

2. ### Remettez en question vos stéréotypes.

   Examinez les idées reçues et les préjugés qui existent au sein de votre équipe de sécurité.

3. ### Traduisez vos supports et adaptez-les au pays.

   Faites plus qu'une simple traduction de vos supports de formation et de stratégies en effectuant une véritable adaptation aux spécificités régionales afin d'éviter des interprétations erronées.

4. ### Faites une refonte de votre back-end.

   Réduisez au minimum les interactions humaines afin de renforcer l'automatisation de la conformité.

5. ### Repensez votre culture.

   Renforcez la confiance des collaborateurs envers votre équipe de sécurité : la sécurité globale de votre organisation s'en trouvera améliorée.

Solution 1 contre les risques cachés :

Effectuez des enquêtes auprès de vos collaborateurs pour connaître les habitudes démographiques de votre organisation.

Menez une enquête anonyme pour obtenir des informations sur votre base de collaborateurs, en prêtant une attention particulière aux différences démographiques potentielles. (Certains résultats sont inattendus ? Des réponses contredisent vos suppositions initiales ?)

Utilisez les résultats pour intensifier vos efforts de formation et de sensibilisation, en adaptant les solutions aux catégories de personnel qui ont besoin d'un soutien supplémentaire.

Exemples de questions dans le cadre d'une étude anonyme sur l'attitude des collaborateurs

Savez-vous identifier une tentative d'hameçonnage ?

Vous a-t-on fourni des ressources et/ou des outils pour identifier les tentatives d'hameçonnage ?

Vous sentez-vous à l'aise pour poser une question à l'équipe Sécurité ?

Vous sentez-vous à l'aise pour signaler une erreur à l'équipe Sécurité ?

Pensez-vous que vos actions ont un impact sur la sécurité de l'entreprise ?

« Il est difficile d'expliquer pourquoi certains collaborateurs cliquent sur les liens d'hameçonnage, car de nombreux facteurs entrent en jeu.

Dans une entreprise de 5 000 personnes, certaines personnes de par leur fonction sont naturellement tentées de cliquer en dépit ce qu'elles ont appris lors de leur formation ou dans le cadre d'un programme de sensibilisation. Je pense aux départements sans cesse en manque de personnel, à ceux qui doivent traiter de très gros volumes d'e-mails (comme pour l'embauche), etc.

Avant de blâmer l'utilisateur final, l'entreprise doit essayer de savoir si elle ne place pas, accidentellement, certaines catégories d'utilisateurs dans cette situation délicate. »

- Admin système anonyme parlant des stratégies de formation des utilisateurs finaux[4]

Solution 2 contre les risques cachés :

Remettez en question vos stéréotypes sur les connaissances numériques des utilisateurs et la sécurité.

Demandez à votre équipe de sécurité de répondre à une enquête anonyme qui examine ses préjugés sur les différents groupes de collaborateurs. Comparez ensuite ces résultats à ceux de votre enquête générale. Vous mettrez ainsi en lumière les préjugés non seulement injustes mais aussi erronés et leur impact sur votre posture de sécurité.

3 vulnérabilités d'origine humaine qui impactent les professionnels de la sécurité

Satisfaction

Processus décisionnel spécifique qui vise un résultat minimal viable, plutôt que faire tous les efforts pour atteindre le meilleur résultat possible.[5]

Même si ce type de processus fonctionne avec des équipes à court de ressources, ce qui sera classé comme « pas assez important » et non pris en compte dans une implémentation de base peut être perçu différemment sous un autre angle et revêtir une importance plus grande.

Négligence basée sur les probabilités

Souvent, les gens considèrent qu'il est peu probable qu'un événement se produise lorsque son impact est important, surtout si des émotions fortes sont impliquées.

Les études montrent que les professionnels de la sécurité sont plus souvent tentés de prioriser et de corriger les événements peu probables mais très dommageables, même si, statistiquement, les risques moins sévères (comme le fait qu'un utilisateur final ne signale pas un incident de sécurité potentiel) se produisent plus souvent.[6]

Parti pris et excès de confiance

Les personnes ayant un niveau de formation élevé ont tendance à surestimer leurs compétences, ce qui les conduit à omettre de faire contrôler leurs solutions par des experts ou de demander l'avis de leurs pairs.

Notre enquête auprès des professionnels de la sécurité montre que, plus un professionnel a un niveau de formation élevé, plus il est susceptible d'être influencé par des partis pris dans sa prise de décision, parce qu'il a l'impression de déjà connaître la bonne réponse ![7]

Solution 3 contre les risques cachés :

Examinez comment la culture de sécurité internationale est traduite et adaptée localement.

Vos stratégies et vos formations de sécurité s'adressent à un vaste public interdépartemental. Vous ne pouvez pas vous contenter de traduire simplement vos supports pour chaque pays. Vous devez adapter (« localiser ») vos documents pour garantir qu'ils sont exempts d'éléments culturels pouvant prêter à confusion.

Pour cela, il est conseillé de consulter proactivement vos équipes locales et régionales, en vue de leur demander leur avis et d'obtenir leur aval quant au contenu de vos nouveaux supports avant l'envoi en traduction.

Et n'oubliez pas, les dirigeants locaux peuvent être de formidables porte-paroles, par exemple en partageant votre message de sécurité d'une manière que les collaborateurs du pays comprendront naturellement et qui gagnera leur confiance et leur adhésion.

Critères à prendre en compte concernant la localisation des programmes de sécurité et la communication

Couleurs

Les utilisateurs chinois peuvent considérer les éléments portant un drapeau rouge comme favorables et positifs… sans se rendre compte immédiatement que la maison mère occidentale voulait en fait dire « stop ». Le vert peut déclencher une réaction négative chez les utilisateurs indonésiens et sud-américains, qui associent le vert, respectivement, à l'infidélité et à la mort.[8]

Sports

Une étude portant sur des documents anglais-arabe/arabe-anglais montre que les traductions de base comportaient des substitutions « inappropriées » pour le jargon sportif dans 37 % des cas.[9] D'autres études sur les traductions du jargon sportif montrent des difficultés similaires pour le polonais[10], le persan/farsi[11] et pratiquement toutes les autres langues.

Symboles

Dans de nombreux pays anglophones, une coche indique une réponse correcte ou une opération terminée. Par contre, en Suède et au Japon, la coche signale une réponse incorrecte, et une réponse correcte est marquée « R » ou « O ».[12] Même la signification des émojis change en fonction de l'âge de l'utilisateur[13] et du pays[14] !

Solution 4 contre les risques cachés :

Concevez votre pile technologique de façon à minimiser les poches de non-conformité et d'incohérence pour les utilisateurs.

Au lieu de compter sur les utilisateurs pour qu'ils se conforment aux protocoles de sécurité, créez une automatisation back-end plus forte, invisible pour les utilisateurs finaux.... la conformité deviendra plus fluide.

3 mises à niveau de sécurité courantes qui réduisent le stress des utilisateurs finaux

Mises à jour de sécurité au moment le plus opportun

La plupart des collaborateurs n'apprécient pas d'arrêter et de redémarrer leur ordinateur pour les mises à jour. C'est pourquoi ils ont tendance à retarder indéfiniment le processus... ou à tout simplement oublier de redémarrer !

Utilisez plutôt un système qui force automatiquement le redémarrage dans un délai précis, mais en autorisant l'utilisateur à planifier ce redémarrage hors de ses heures de travail, pour encourager une mise à jour rapide mais non gênante.

Politiques modernes relatives aux mots de passe

Récemment, de nombreuses structures mondiales de cybersécurité ont discrètement éliminé l'ancienne recommandation d'alterner les mots de passe, s'il n'y a aucune preuve de la divulgation du secret d'un utilisateur.[15] Au lieu de renforcer la sécurité, ces stratégies d'expiration des mots de passe ont un effet contraire, car les utilisateurs ont eu du mal à tenir le rythme (et à mémoriser !) de nouveaux codes d'accès ou codes PIN.[16]

Envisagez plutôt de déployer des outils de gestion des mots de passe, des stratégies SSO (connexion avec identification unique) ou des technologies sans mot de passe... plus besoin de compter sur la mémoire de l'utilisateur ou sur des post-it.

Politiques d'utilisation acceptable (AUP) silencieuses avec mise en œuvre intégrée

Même si votre processus d'onboarding des collaborateurs comprend la lecture de la politique AUP de votre entreprise, une politique non appliquée ne vaut même pas le prix du papier sur lequel elle est imprimée.[3]

Solution 5 contre les risques cachés :

Développez proactivement une culture de sécurité ouverte et accueillante.

Au regard des résultats de cette étude « *Les menaces cachées* », il apparaît qu'une culture de sécurité collaborative et positive doit être développée dans toutes les organisations. En définitive, les collaborateurs ne doivent jamais hésiter à contacter les professionnels de la sécurité, même si leur question paraît insignifiante ou leur erreur potentiellement ridicule.

Seule une culture non punitive peut permettre aux équipes de sécurité d'obtenir une coopération suffisante de la part des utilisateurs pour protéger correctement toute l'entreprise.

4 principes essentiels d'une culture de sécurité forte

Ouverture

Les collaborateurs se sentent à l'aise pour signaler un incident, et sont récompensés de leur honnêteté et de leur transparence. Ils n'hésitent pas à solliciter l'équipe Sécurité, même pour des raisons futiles.

Répétition

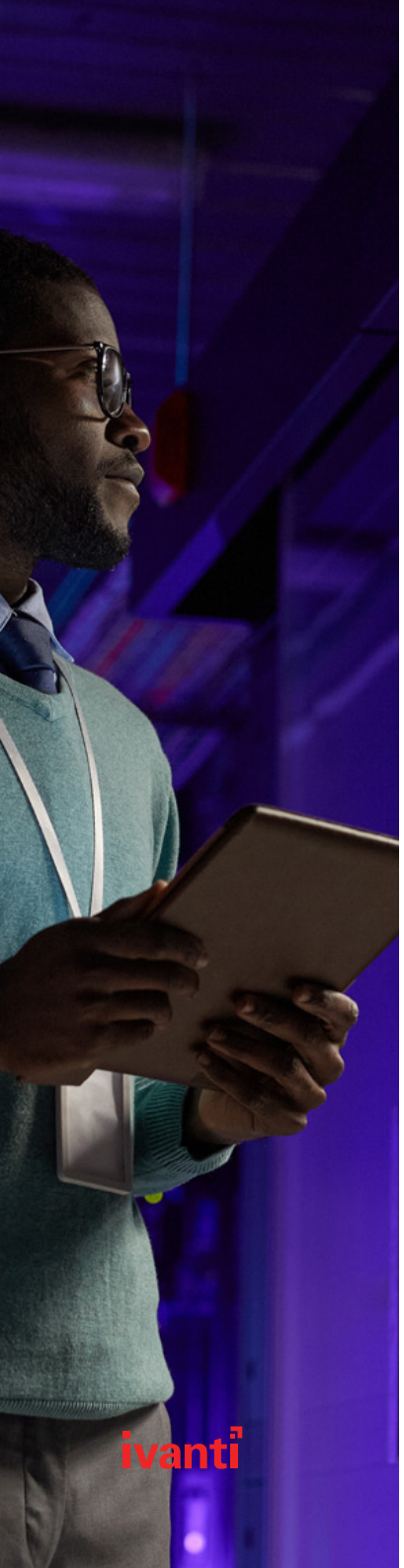
L'entreprise propose des formations fréquentes et régulières qui séduisent les collaborateurs. Il peut s'agir d'ateliers de formation formels, de communications régulières à l'échelle de l'entreprise, ou même de concours de sécurité gamifiés basés sur de véritables scénarios de sécurité.

Conception ad-hoc

Le comportement des collaborateurs dépend de leurs interactions avec la technologie. Les technologies devraient être conçues de façon à décourager totalement le recours aux solutions de contournement ou à des pratiques non conformes.

Intégration

La sécurité de l'entreprise est l'affaire de tous. Cette responsabilité est partagée par tous et vos collaborateurs s'investissent pour protéger la sécurité de l'organisation.



Références

1. Sevilla, C. (2022, May 23). Everyday ageism in the tech industry. From CWJobs: https://www.cwjobs.co.uk/advice/ageism-in-tech
2. Ivanti. (2023, August 29). 2023 Executive Security Spotlight: New research from Ivanti shows real risks facing the C-suite. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2773/17cca519291d
3. Ivanti. (2023, December 12). Press Reset: A 2023 Cybersecurity Status Report. From Ivanti: https://www.ivanti.com/resources/v/doc/ivi/2732/7b4205775465
4. u/CyberAndFolkloreGuy. (2023, January 19). Security Awareness: How to properly address colleagues who repeated fail Phishing tests? From Reddit: https://www.reddit.com/r/cybersecurity/comments/10g4688/comment/j55k4cn/
5. Frankenfield, J. (2022, August 23). Satisficing: Definition, How the Strategy Works, and an Example. From Investopedia: https://www.investopedia.com/terms/s/satisficing.asp
6. De Wit, J. J., Pieters, W., & Van Gelder, P. H. (2022). Individual Preferences In Security Risk Decision Making: An Exploratory Study Under Security Professionals. WIT Transactions on The Built Environment, 187-199. doi:10.2495/SAFE210161
7. De Wit, J., Pieters, W., Jansen, S., & van Gelder, P. (2021). Biases in Security Risk Management: Do Security Professionals Follow Prospect Theory in Their Decisions? Journal of Integrated Security and Safety Science, 1(1), 34-57. doi:https://doi.org/10.18757/jisss.2021.1.5700
8. Eriksen Translations. (2020, February 3). How Translating Colors Across Cultures Can Help You Make a Positive Impact. From Erksen Translations: https://eriksen.com/marketing/color_culture/
9. Nasser, L., & Al-Aazzawi, K. (2022). Context Impact in Translating Sport Idiomatic Expressions from English into Arabic with Regard to Types of Idioms. Adab Al-Rafidayn Journal, 1-26. doi:10.33899/radab.2021.170415
10. Mazurkiewicz, M. (2014). Sports Vocabulary and Idioms – Some Observations About the Specificty of English-Polish and Polish-English Translation. Cultures and Literatures in Translation, 140-153. From https://www.academia.edu/40425597/Sports_Vocabulary_and_Idioms_Some_Observations_about_the_Specificity_of_English_Polish_and_Polish_English_Translation
11. Suzani, S. M. (2007). Sports Idioms and Duality of Meaning in Translation. Iranian Journal of Translation Studies. From https://journal.translationstudies.ir/ts/article/view/126

12. Grove, L. (1989). Signs of the times: graphics for international audiences. International Professional Communication Conference 'Communicating to the World', 137-141. doi:10.1109/IPCC.1989.102119

13. Brants, W., Sharif, B., & Serebrenik, A. (2019). Assessing the Meaning of Emojis for Emotional Awareness - A Pilot Study. Companion Proceedings of The 2019 World Wide Web Conference, 419–423. doi:https://dl.acm.org/doi/abs/10.1145/3308560.3316550

14. Gao, B., & VanderLaan, D. P. (2020). Cultural Influences on Perceptions of Emotions Depicted in Emojis. Cyberpsychology, Behavior, and Social Networking, 567-570. doi:https://doi.org/10.1089/cyber.2020.0024

15. National Institute of Standards and Technology (NIST). (2020, March 03). NIST Special Publication 800-63B. From https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

16. WIlson, K. R.-H. (2020, March 9). The Debate Around Password Rotation Policies. From SANS Institute: https://www.sans.org/blog/the-debate-around-password-rotation-policies/

17. u/securebxdesign. (2023, April). What does your policy/training look like for people who fail phishing campaigns? From Reddit: https://www.reddit.com/r/cybersecurity/comments/13csxs0/comment/jjk37bo/

Les menaces cachées en 2023

L’impact des données démographiques des collaborateurs sur la posture de sécurité des organisations

Série Ivanti de rapports sur l'état de la cybersécurité

ivanti.fr
33 (0)1 76 40 26 20
contact@ivanti.fr