ivanti

Pleins feux sur la sécurité des dirigeants en 2023

Dans une nouvelle étude, Ivanti dévoile les risques réels qui pèsent sur les hauts dirigeants

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

Bloquer les menaces de cybersécurité qui visent les dirigeants

Les entreprises lient rarement les lacunes en cybersécurité au manque de soutien de la direction. Dans le rapport « Repartez sur de nouvelles bases », seuls 21 % des DSI et professionnels de la sécurité considéraient la faible implication des dirigeants comme une entrave à la sécurité… soit 16 points de moins que l'obstacle principal, à savoir la complexité de la pile technologique (37 %).

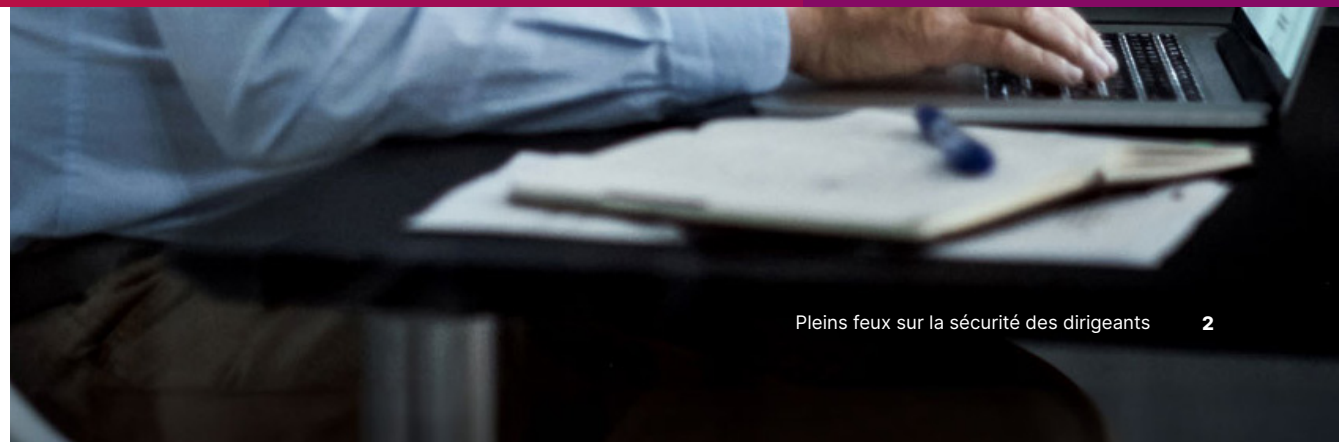
Pourtant, le risque que les dirigeants adoptent des comportements dangereux est bien supérieur à ce que pensent les équipes de sécurité.

Selon leurs propres déclarations, **les dirigeants sont 5 fois plus** susceptibles d'avoir demandé et obtenu un accès non autorisé aux informations sensibles d'un client ou de l'entreprise.

Plus d'un dirigeant sur 3 a déjà cliqué sur un lien d'hameçonnage, un taux 4 fois supérieur à celui des autres collaborateurs de bureau.

Ils sont 4 fois plus susceptibles de partager un mot de passe d'entreprise avec des personnes extérieures à l'entreprise.

Comment protéger les dirigeants (le groupe de collaborateurs le plus ciblé), alors qu'ils disent soutenir les décisions de votre entreprise mais contournent souvent les protocoles de sécurité ? Une nouvelle étude Ivanti dévoile la triste vérité.



ivanti

Points clés du rapport :

L'écart important entre les priorités annoncées par les dirigeants (notamment leur adhésion aux stratégies de sécurité) et leur comportement au travail.

Le lien fort entre les habitudes de sécurité des dirigeants et le degré de risque élevé de cyberattaque et de violation de données, quand les habitudes des autres collaborateurs posent des risques bien moindres.

Le manque actuel de confiance entre les dirigeants et les équipes chargées de les sécuriser… qui peut conduire les dirigeants à chercher un support IT en externe au lieu de demander de l'aide en interne.

Des façons pratiques de sécuriser votre entreprise grâce à des implémentations silencieuses dans les coulisses, tandis que vous et votre équipe restaurez la confiance mutuelle nécessaire pour que les dirigeants soutiennent réellement votre programme de sécurité.

Les responsables de sécurité savent déjà que les hauts responsables dotés d'un accès de haut niveau présentent une vraie menace pour la sécurité. La nouvelle étude d'Ivanti attire l'attention sur l'*échelle* du problème et sur les risques disproportionnés que ces exceptions aux règles de sécurité font peser sur l'entreprise.

« Il peut être tentant de dispenser les dirigeants des mesures de cybersécurité les plus strictes en raison de leur petit nombre, en sous-estimant le danger potentiel qu'ils représentent.

Cependant, de récentes études dissipent ces idées fausses. Les dirigeants montrent un comportement au travail qui leur est propre et disposent d'un accès et d'une influence incomparables.

Ces études montrent sans contestation possible qu'il est impératif de traiter et de corriger leurs habitudes et leurs comportements. »

Giuliano Liguori,
PDG de Kenovy

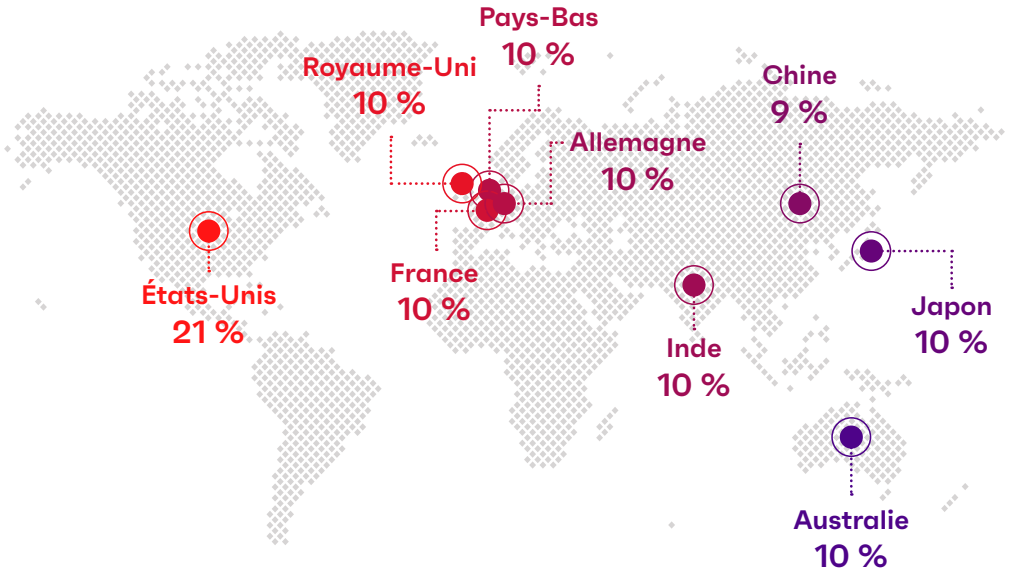
Sommaire :

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 menaces d'aujourd'hui et savoir comment les entreprises se préparent aux menaces futures encore inconnues.

Dans ce rapport, nous mettons l'accent sur les hauts dirigeants, notamment sur les attitudes et comportements qui en font un danger pour la sécurité.



Collaborateurs de bureau
5 202

Professionnels de sécurité
902

Dirigeants
454

01

Écarts de conduite des dirigeants :

Différence entre ce que les dirigeants disent de la sécurité... et ce qu'ils ont tendance à faire

ivanti

Problème actuel

Ce que les dirigeants disent est très différent de ce qu'ils font

Les dirigeants se disent optimistes quant à la cybersécurité ; presque tous se déclarent de fervents soutiens de la mission de sécurité de leur entreprise. Pourtant, notre étude montre un large écart entre ce que les dirigeants affirment et leurs pratiques. C'est ce que nous appelons les écarts de conduite.

Les écarts de conduite : différence entre la perception et le comportement des dirigeants

	Ce que DISENT les dirigeants :	Ce que FONT les dirigeants :
Culture de sécurité	96 % des dirigeants affirment que les cadres sont au moins modérément en faveur ou impliqués dans les mesures de cybersécurité de leur entreprise.	**49 % des dirigeants (CXO) ont demandé à contourner** une ou plusieurs mesures de sécurité au cours de l'année écoulée.
Formation	78 % disent que leur entreprise dispense une formation obligatoire à la cybersécurité.	**77 % utilisent des astuces pour créer des mots de passe faciles à mémoriser,** par exemple en incluant des dates d'anniversaire ou des noms d'animaux de compagnie. **En outre, les dirigeants sont 3 fois plus susceptibles** de partager leurs périphériques professionnels avec des utilisateurs non autorisés, comme des amis, de la famille et des indépendants externes.
Hameçonnage	88 % des dirigeants se disent prêts à reconnaître et à signaler les menaces comme les malwares et l'hameçonnage.	Parmi les personnes visées par un hameçonnage, **35 % admettent avoir cliqué** — sur le lien... ou même, avoir envoyé de l'argent.

Parce qu'ils manquent de temps pour la procédure normale, se sentent au-dessus des règles ou autre, les dirigeants tendent à se comporter différemment des autres collaborateurs de bureau. En clair, ils prennent plus de risques.

24 %

des cadres affirment avoir gardé le mot de passe initialement fourni lors de leur intégration pour accéder aux applications de l'entreprise.

14 %

des autres collaborateurs de bureau n'ont pas non plus changé le mot de passe d'origine.

Pourquoi c'est important

Ces comportements à haut risque des dirigeants ne constituent pas un simple contournement des règles

La plupart des professionnels de la sécurité ont connaissance de ces comportements à risque, mais ils préfèrent mettre en avant d'autres priorités stratégiques que l'hygiène de cybersécurité des cadres supérieurs.

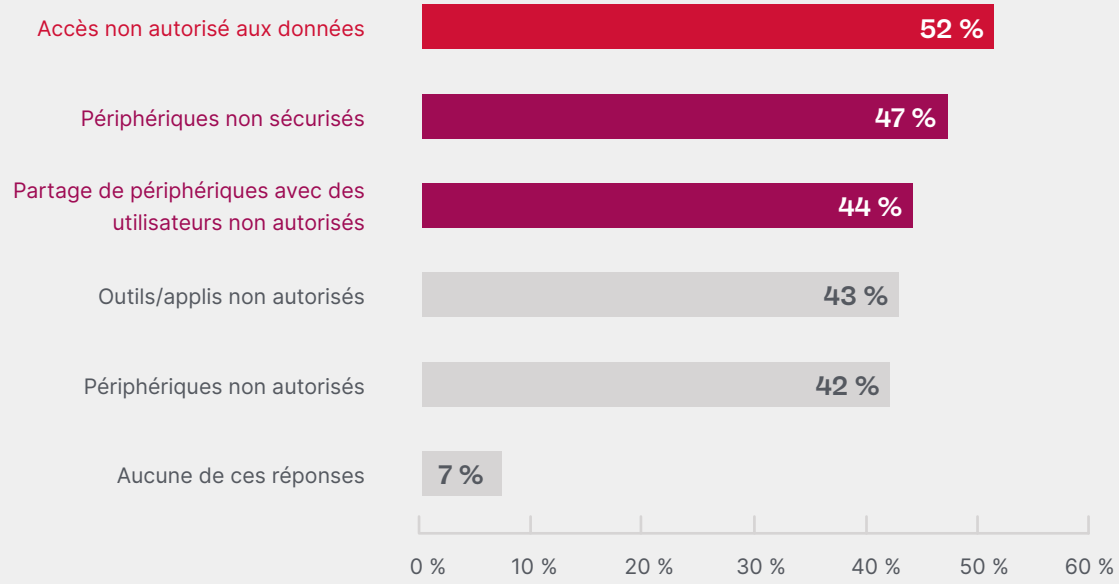
Les responsables de la sécurité doivent utiliser leur temps et leurs ressources (limités) de manière à protéger l'entreprise contre les risques les plus fréquents et les plus importants. Le raisonnement est le suivant : pourquoi les équipes de sécurité devraient-elles passer plus de temps à protéger les dirigeants qui disent avoir adhéré au programme… et ont même octroyé le budget pour ce programme ?

Les études d'Ivanti le confirment : les mauvaises pratiques de sécurité des dirigeants s'avèrent un problème systémique qui affecte la plupart des entreprises..

En fait, les facteurs de risque élevé pour la sécurité de leur entreprise que citent les professionnels eux-mêmes correspondent directement aux comportements que les dirigeants reconnaissent avoir.

Q: Parmi les éléments suivants, lesquels représentent un risque de sécurité élevé pour votre entreprise ?

Remarque : les professionnels de la sécurité interrogés pouvaient choisir plusieurs options.



1/3 des dirigeants

admettent avoir accédé à des fichiers et données non autorisés.

Les dirigeants sont 3 fois

plus susceptibles de partager leurs périphériques professionnels avec leurs proches et amis que les autres collaborateurs de bureau.

Influence de la dynamique du pouvoir sur les comportements de sécurité des dirigeants

Les inégalités de pouvoir entre les équipes de sécurité et les hauts dirigeants accentuent malheureusement le problème.

Combien de fois les équipes de sécurité ont-elles tenté d'implémenter des stratégies de sécurité basées sur les meilleures pratiques pour se retrouver confrontées aux récriminations et aux comportements de Shadow IT de la part des utilisateurs de première ligne, premiers bénéficiaires de cette protection ?

Comment peut-on attendre des équipes de sécurité qu'elles renforcent l'hygiène et les pratiques de sécurité chez les dirigeants qui approuvent leur budget (et leur travail) sur un marché du travail incertain ?

Par manque de temps, épuisement ou burnout, les professionnels de la sécurité cèdent souvent à la pression des dirigeants.

Pourquoi les équipes de sécurité ont-elles du mal à impacter le comportement des dirigeants ?

Burnout

Les RSSI sont surchargés et en burnout : 60 % d'entre eux déclarent avoir connu un burnout ces 12 derniers mois et 61 % se plaignent des attentes excessives envers les RSSI/DSI[1].

Culture

Quand le patron (ou le patron du patron) demande un passe-droit ou un contournement du protocole de sécurité, les équipes Sécurité, on le comprend, hésitent à refuser.

Sans une solide culture privilégiant la sécurité, les collaborateurs et les pros de la sécurité risquent tout simplement d'accepter cette demande dangereuse d'une personne en position d'autorité.

Juste pour cette fois

La rationalisation ne manque pas d'attrait : *« juste pour cette fois »* ou *« juste pour vous »*.

Sur le moment, les pros de la sécurité peuvent se sentir gênés d'imposer les règles au PDG… surtout si des exceptions ont été accordées par le passé.

Ce que l'on fait « juste pour cette fois » se répète presque toujours, ce qui accentue le danger des pratiques de contournement des dirigeants et crée un précédent sur lequel il est dur de revenir.

02

Cyberrisques démesurés des cadres dirigeants :

Impact des mauvaises habitudes des dirigeants sur leur cybersécurité

ivanti

Problème actuel

Les comportements risqués des dirigeants ont des conséquences dramatiques

Certes peu nombreux, les dirigeants jouissent d'un niveau exceptionnellement élevé d'accès automatique alors même qu'ils ont des comportements de sécurité inquiétants, bien plus dangereux pour l'entreprise que les actions des autres employés.

Connexions non protégées des relations proches des dirigeants

45 % des dirigeants

laissent leur famille et leurs amis utiliser leurs périphériques professionnels au moins une fois par mois.

Près d'un dirigeant sur 5

a partagé son mot de passe professionnel avec des personnes extérieures à l'entreprise.

C'est 3 fois plus que tout le reste du personnel de bureau !

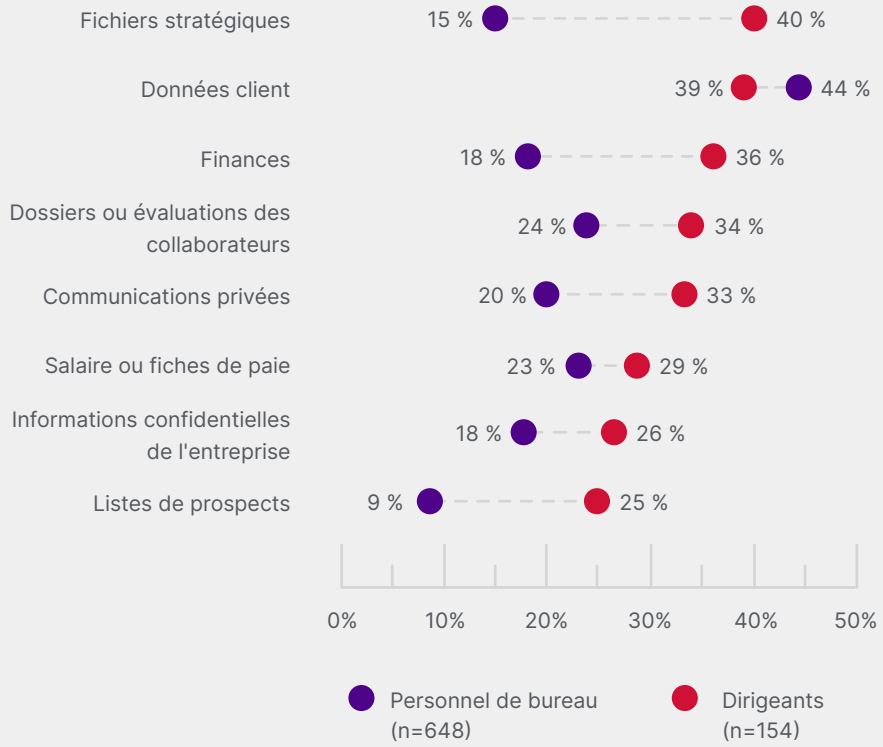
Ces contacts personnels ne sont pas formés à la sécurité et ne sont pas partie prenante de la protection de votre entreprise, alors même qu'ils utilisent les appareils de l'entreprise avec un accès étendu aux fichiers et au réseau.

ivanti

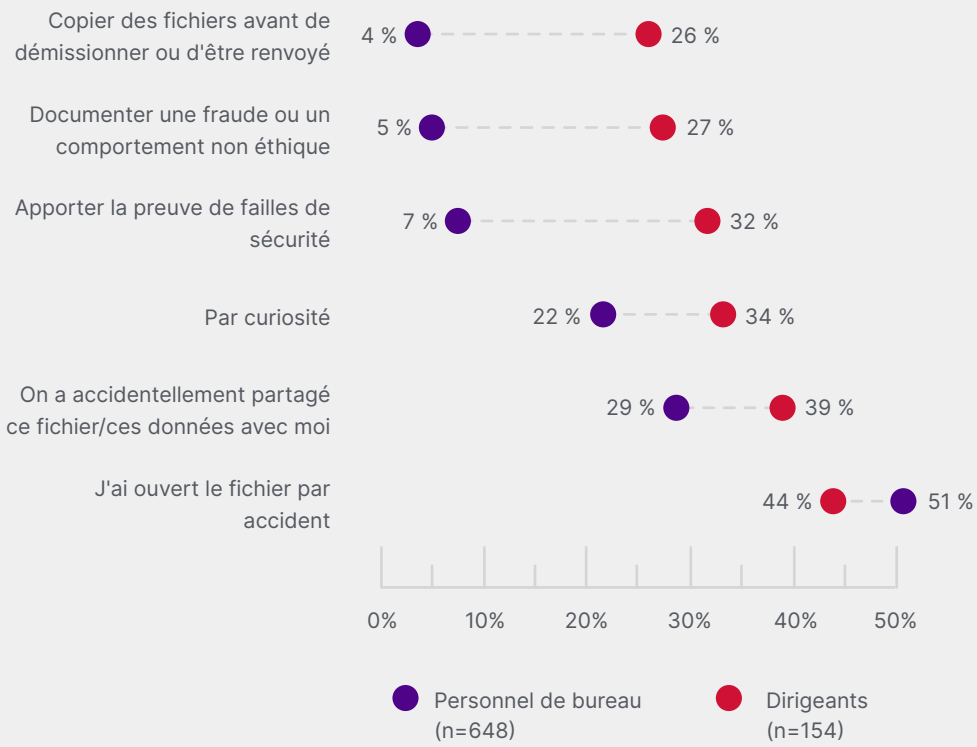
Accès non autorisé des dirigeants

Plus d'1 dirigeant sur 3 (34 %) admet avoir accédé à des informations non autorisées au bureau. Et près de 2 sur 3 disent qu'ils auraient pu modifier ces fichiers/données en y accédant.

Q: À quels fichiers avez-vous eu accès ?



Q: Pourquoi avez-vous accédé à des informations non autorisées ?



Remarque : pour chaque graphique, toutes les personnes interrogées avaient précédemment confirmé avoir accédé à des fichiers inutiles à leur travail.

Pourquoi c'est important

Les exceptions de sécurité des dirigeants augmentent les risques

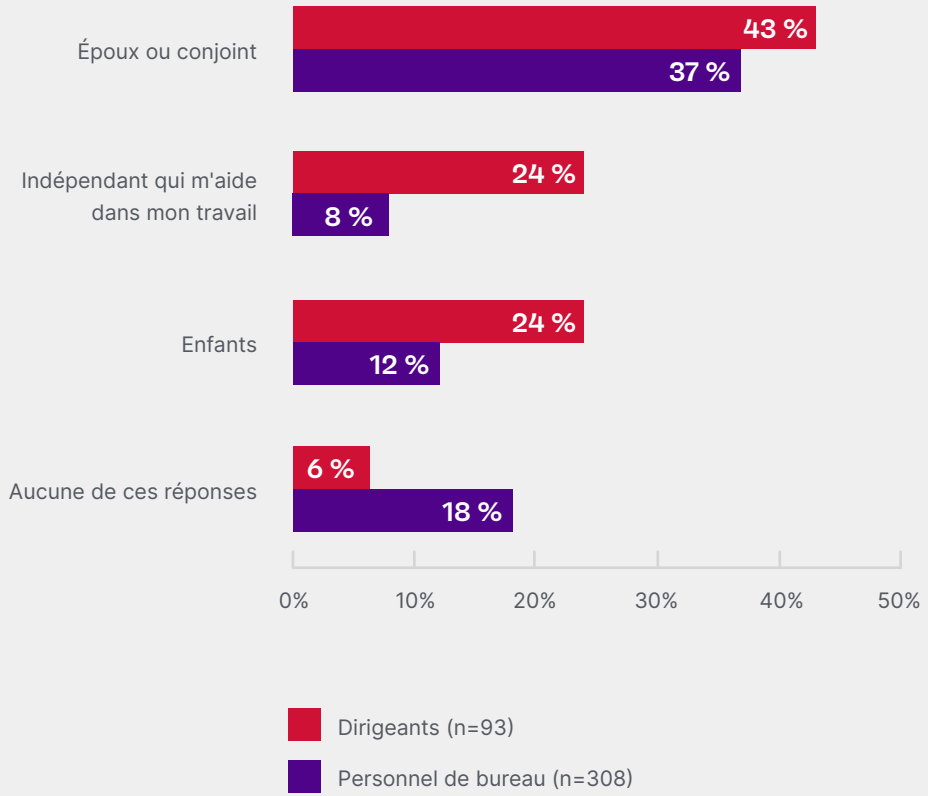
De nombreux dirigeants prennent des raccourcis pour gagner du temps ou parce que c'est plus pratique. Cependant, les études d'Ivanti montrent que le risque est plus systémique qu'on ne le pensait jusque-là.

Les dirigeants pensent, avec raison, que leur temps est précieux et limité. Partager des mots de passe et des périphériques avec la famille, les collègues et un support technique tiers par exemple, peut être considéré comme un gain de temps sans risque.

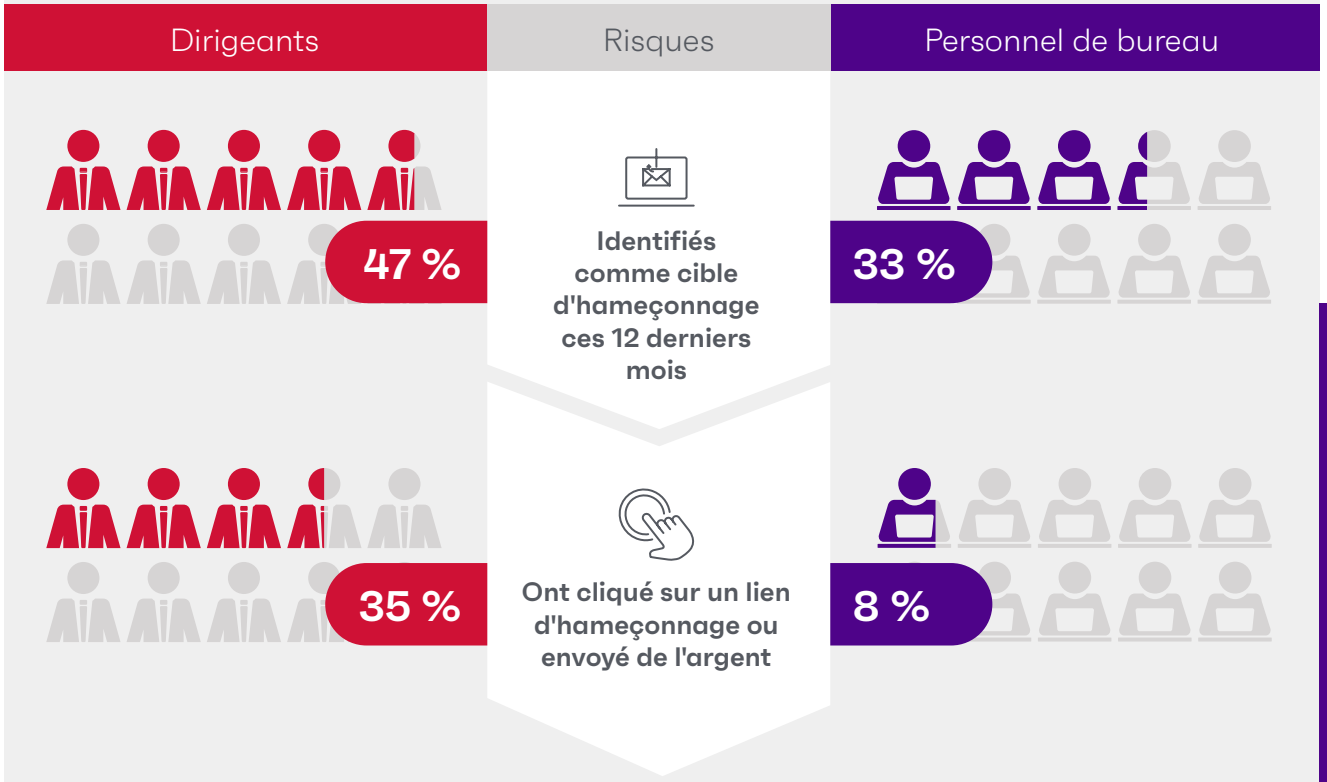
27 %

des dirigeants interrogés disent laisser des proches utiliser leurs périphériques professionnels au moins une fois par mois... contre seulement 6 % des autres collaborateurs de bureau.

Q: Avec qui avez-vous partagé votre mot de passe ?



Dirigeants plus exposés à l'hameçonnage que le personnel de bureau



Ces taux plus élevés peuvent être dus à un pic dans les attaques par « spearphishing » ou harponnage pour chasser les « baleines », à savoir des cibles à forte valeur. Pour les pirates, cela vaut la peine de consacrer du temps et des efforts supplémentaires pour toucher une cible à haut niveau d'accès et de privilèges.

Les acteurs malveillants, membres de gangs de ransomwares à la motivation financière ou de groupes APT (menaces avancées persistantes), ciblent explicitement les dirigeants. En effet, ces cadres hyperconnectés à des sources de données précieuses et à des actifs en réseau manquent de vigilance dans leur hygiène de cybersécurité.

Après tout, pourquoi lancer un large filet pour voler les permissions d'un employé de bureau lambda, quand une seule « baleine » vous donne un accès exceptionnel à des actifs de bien plus grande valeur ?

« **Il y a 100 % de risque que votre** entreprise ait subi un hameçonnage au cours de l'année écoulée. C'est la méthode n° 1 des pirates pour prendre pied dans votre réseau.

Nous devons absolument en tenir compte, et ne pas partir du principe que les gens sont “plus malins que ça“ ou que la tentative de fraude est évidente. »

Daniel Spicer
Chief Security Officer chez Ivanti

Répercussions dans le monde réel

Le turnover des cadres favorise l'hameçonnage

En 2015, Mattel a été victime d'un « spearphishing » (harponnage) qui a fait les gros titres. L'entreprise a perdu 3 millions de dollars au profit de cybercriminels basés en Chine.

L'étude de cas menée après cela par Infosec[2] a montré que la décision de Mattel d'embaucher un nouveau PDG avait créé les conditions idéales pour cette exploitation :

« Ils ont attendu le moment idéal, qui s'est présenté quand Mattel a décidé de nommer un nouveau PDG, Christopher Sinclair, pour remplacer Bryan Stockton en janvier 2015. L'arrivée du nouveau PDG impliquait des changements au plus haut niveau de la Direction, qui allaient provoquer de nouvelles luttes de pouvoir dans la hiérarchie de l'entreprise.

Autrement dit, les cybercriminels ont même pris en compte la vie de l'entreprise et les relations humaines chez Mattel pour planifier leur e-mail de pêche à la baleine. »

Étude de cas Infosec[2]

03

Frictions dans la sécurité :

Les relations tendues entre les dirigeants et leur équipe de sécurité à la loupe

ivanti

Problème actuel

Une médiocre hygiène de cybersécurité, conséquence directe des expériences des dirigeants avec la Sécurité

Les enquêtes d'Ivanti montrent que les dirigeants ont 2,5 fois plus tendance à faire appel à l'équipe Sécurité que le collaborateur moyen (et c'est bon signe) mais qu'ils sont aussi bien plus enclins à trouver ces échanges *négatifs*.

Les dirigeants sont :

2 fois

plus susceptibles de dire que leurs interactions passées avec l'équipe Sécurité étaient peu satisfaisantes

4 fois

plus susceptibles de faire appel à un support technique externe non approuvé

33 %

plus susceptibles d'appréhender de signaler une erreur de sécurité comme un clic sur un lien d'hameçonnage. (C'est plus d'un dirigeant sur 10 !)

2 fois

plus susceptibles de dire que ces interactions étaient embarrassantes

5 fois

plus susceptibles de partager un mot de passe d'entreprise avec des personnes extérieures à l'entreprise

Comment éliminer les entraves à la communication entre les dirigeants, qui appréhendent de signaler des erreurs, et les équipes de sécurité chargées de les protéger ?

Les violations de données se sont clairement hissées à la première place des préoccupations des dirigeants. Une protection robuste doit désormais exploiter toute la puissance de l'IA dans la détection des menaces en temps réel pour renforcer les défenses des actifs de l'entreprise.

Ronald van Loon
PDG et Principal Analyst chez Intelligent World

Remarque : ces statistiques comparent les collaborateurs de niveau Direction avec tous les autres collaborateurs de bureau.

Pourquoi c'est important

Les entreprises ont besoin d'un programme de cybersécurité des *dirigeants* robuste

Les pratiques de contournement des dirigeants créent certes de graves vulnérabilités, mais au-delà, la tolérance aux passe-droits pour les cadres s'inscrit dans une culture d'entreprise où les erreurs sont moins signalées.

Pour les équipes de sécurité, la priorité est de réinstaurer la confiance et d'emporter l'adhésion des dirigeants afin de créer un espace de dialogue et d'assistance, sans jugement ni condescendance.

Les hauts dirigeants

soutiennent la culture de sécurité lorsqu'ils comprennent le rôle stratégique de la cybersécurité au sein de l'entreprise et appuient visiblement les efforts en ce sens.

Les équipes Sécurité

soutiennent la culture de sécurité en maintenant un style de communication ouvert visant à éduquer (plutôt qu'à punir ou humilier) les personnes qui font des erreurs.

Atténuer les risques de sécurité des dirigeants est encore plus urgent en cas de licenciement

Comme le montre notre étude, le déprovisionnement des informations d'authentification est un problème généralisé : les professionnels de la sécurité confient en effet que leurs recommandations sont ignorées dans un tiers des cas… un aveu étonnant au vu de l'exposition.

De plus, 26 % des dirigeants interrogés déclarent encore disposer de mots de passe valables de leur ancien employeur. C'est ce que nous appelons des *informations d'authentification zombies*.

Les menaces liées aux informations d'authentification zombies s'intensifient dans les périodes de licenciement, quand les collaborateurs sont plus enclins à emporter des données ou à en vouloir à leur ancien employeur.

Jeff Pollard, analyste chez Forrester, confirme cette conclusion : « Nous savons que les licenciements ou les pertes d'emploi sont des facteurs prédictifs de risques en interne, ce qui augmente la probabilité d'événements de sécurité. Nous voyons cela se produire depuis plusieurs années. »[3]

« Avant, c'était difficile [de réussir une attaque interne] ; maintenant, c'est facile. Par le passé, vous pouviez emporter ce qui tenait dans votre attaché-case. Aujourd'hui, vous pouvez transporter plusieurs téraoctets. »

Pete Nicoletti
Field CISO zone Amériques chez Check Point Software[3]

04

Comment réagir :

Corriger les écarts de conduite des dirigeants dans votre entreprise

ivanti

Comment réagir

Regarder le problème en face

L'enquête d'Ivanti confirme ce que beaucoup d'entre nous savent depuis longtemps : les dirigeants représentent une menace unique et importante pour la sécurité d'une entreprise. Nous avons désormais les données pour régler ce problème.

1. ### Mener des audits
   pour évaluer les écarts de conduite actuels de vos dirigeants.

2. ### Éliminer d'abord les risques les plus faciles et les moins gênants
   pour éviter les conflits directs avec la Direction quand c'est inutile.

3. ### Organiser un exercice sous forme de jeu
   pour obliger les cadres à faire le lien entre l'hygiène de cybersécurité de base et l'impact d'une future fuite de données sur leur propre département.

4. ### Implémenter un programme de sécurité haut de gamme
   Certes, la multitude des collaborateurs de bureau dépasse souvent largement le petit nombre de membres de l'équipe dirigeante. Mais le retour sur investissement de vos ressources limitées dans l'attention personnelle à ce petit groupe d'acteurs est sans commune mesure.

« Vous devez créer une culture (je dis que c'est facile, mais c'est vrai) où vous pouvez défier la Direction et construire un processus auquel tout le monde est soumis. »

AJ Nash
VP et Distinguished Fellow of Intelligence chez ZeroFox

20 %

des fuites de données mondiales sont liées à des attaques venant de l'intérieur.[3]

Le saviez-vous ?

Les hauts dirigeants sont 6,5 fois plus susceptibles de copier des fichiers avant de démissionner ou d'être renvoyés que le reste de la main-d'œuvre intellectuelle.

1 Mener un audit

Pour dresser le tableau des comportements des dirigeants au sein de votre entreprise, envisagez un audit. Le but n'est pas de les punir ou de leur faire honte, mais bien de garantir que les stratégies de gouvernance de sécurité s'appliquent à tout le personnel, à tous les postes.

Audit interne

Faites l'inventaire des interactions entre votre équipe de sécurité et les dirigeants (de niveau Directeur ou supérieur) sur les 12 derniers mois, et recherchez les problèmes de communication récurrents et les comportements risqués... aussi bien chez les dirigeants que chez les membres de votre équipe de sécurité.

Par exemple, extrayez un échantillon aléatoire des enregistrements d'appels et des messages de ticket archivés. Recherchez des indices sur le ton et le choix de mots des deux parties.

- L'échange a-t-il créé un malaise autour d'une erreur d'inattention ?
- A-t-il fait redouter les conséquences d'un oubli ?
- A-t-il dérangé ou mis en colère l'une des parties ?

Audit externe

Envisagez d'embaucher un cabinet externe pour lui confier aussi un audit des risques des dirigeants.

Lorsqu'une entreprise envisage de modifier les privilèges des dirigeants ou d'imposer un contrôle plus strict à l'équipe de direction, c'est toujours une bonne idée d'avoir un point de vue extérieur.

Un chargé d'audit externe peut superviser une évaluation impartiale des risques posés par les dirigeants et, si nécessaire, annoncer de mauvaises nouvelles à l'équipe de direction et au conseil d'administration.

Répercussions dans le monde réel

La stratégie interne d'une école déjoue une escroquerie par hameçonnage de 100 000 dollars[4]

Jan McGee, alors cheffe d'un établissement scolaire en Floride, signe un chèque de 100 000 dollars à tirer sur le compte de l'école après plusieurs mois de correspondance avec quelqu'un qu'elle pensait être le milliardaire Elon Musk ou son représentant.

Jan McGee n'était pas autorisée à signer de chèque pour plus de 50 000 dollars sur les fonds de l'école sans l'approbation du conseil d'administration. Heureusement, le responsable commercial de l'école, Brent Appy, a réussi à faire opposition à ce chèque avant que les escrocs ne puissent le toucher.

« Je suis une femme intelligente. J'ai fait des études. Et je suis tombée dans le piège.

Le *grooming,* c'est quand vous parlez à quelqu'un en qui vous avez confiance, et qu'il vous amène à croire tout ce qu'il dit. Et je suis tombée dans le panneau. »

Dr. Jan McGee
Ancienne cheffe d'établissement scolaire en Floride

2 Éliminer d'abord les risques les plus faciles et les moins gênants

Après l'audit, quand vous avez une meilleure idée de vos vulnérabilités de sécurité, il est temps d'élaborer un plan d'action… et de le faire d'une manière qui ne soit pas trop envahissante.

Identifiez la faille ou l'exposition la plus courante dans votre entreprise en fonction de vos audits des écarts de conduite des dirigeants, et priorisez-la pour y remédier en premier.

Parmi les éléments les plus simples à mettre en œuvre :

Élaborer et mettre à jour votre stratégie de confidentialité et de classification des données : qui est autorisé à accéder à quoi, dans quelles circonstances et pendant combien de temps, et pourquoi certaines permissions ne sont pas octroyées. Ce qui est autorisé et ce qui ne l'est pas, et *pourquoi*, doit être transparent et évident pour tout le monde.

Actualiser les stratégies de communication interne pour mettre en place des stratégies AUP (stratégie d'utilisation acceptable) et de confidentialité des données lors de l'onboarding de chaque collaborateur, avec des rappels réguliers. Vous ne pouvez pas compter sur un seul document « officiel » de stratégie sur l'intranet de l'entreprise pour éduquer toutes vos parties prenantes internes, et surtout pas des dirigeants très occupés !

Documenter et implémenter des procédures standard d'approbation et d'octroi des accès pour garantir que les stratégies de contrôle d'accès s'appliquent bien à tout le personnel, et que toutes les activités sont entièrement documentées et vérifiables. (Si vos traces d'audit ne peuvent pas confirmer l'accès ou les activités réseau, c'est le moment de changer !)

Examiner l'expérience collaborateur numérique (DEX) actuelle de vos dirigeants. Les mesures de sécurité punitives ou inhibitrices qui interfèrent avec le workflow régulier des dirigeants renforcent la méfiance. Choisissez plutôt des outils de sécurité qui s'exécutent en coulisses, afin d'assurer la sécurité des dirigeants sans provoquer des centaines de questions et/ou de tickets signalant des déconnexions fréquentes.

3 Organiser un exercice sous forme de jeu pour la direction

Le jeu est un excellent moyen de former les dirigeants sans connaissances techniques à la sécurité et d'affermir leur soutien. En effet, ces sessions leur permettent d'appréhender par eux-mêmes les impacts des violations de sécurité sur leur service… avec l'aide de l'équipe Sécurité pour les orienter dans la bonne direction.

Essayez de commencer doucement, avec un simple exercice « trouvez l'hameçonnage ».

Vous pouvez commencer votre prochaine réunion de direction par une simple série de « trouvez l'hameçonnage », dans laquelle vous montrez à votre équipe des exemples de messages d'hameçonnage, et demandez au groupe lesquels sont réels et lesquels sont de l'hameçonnage.

Il suffit de deux diapos et de moins de trois minutes pour ce jeu interactif simple qui montre des cyberattaques réelles !

Astuces pour rendre ludique la formation à la sécurité des dirigeants

Faire court

Préférez les sessions plus courtes et plus fréquentes avec un animateur sur place ou à distance aux ateliers d'une demi-journée ou plus. Consacrez cinq minutes au début des réunions de direction régulières pour un jeu ou une session de sécurité rapide !

Ajouter une part de hasard

Choisissez au hasard les menaces et les scénarios de vos sessions. Vous pouvez utiliser une méthode très simple (comme lancer un dé à 20 faces pour choisir un risque dans une liste numérotée) ou une plus complexe, comme un générateur pondéré en fonction des risques les plus réalistes pour votre entreprise, région ou secteur d'activité spécifique.

Être créatif

Encouragez vos dirigeants à proposer des solutions créatives pour bloquer une attaque ou pour exploiter les risques des scénarios présentés ; ne ralentissez pas la session en expliquant pourquoi une idée est irréaliste, peu pratique ou inexacte.

Jouer collectif

Ne nommez jamais vos collaborateurs (actuels ou anciens) parmi les risques ou les menaces même dans des exercices fictifs ! Les dirigeants et l'équipe de sécurité doivent toujours être du même côté, pour que tout le monde réussisse ou échoue, en tant que groupe.

Matérialiser l'exercice

Préparez des kits de formation à la sécurité incluant divers scénarios, matériaux, accessoires, outils ou même des Legos, pour accélérer les exercices de formation tout en offrant des opportunités d'engagement uniques et créatives.[5]

Recycler des jeux de société

Récupérez un jeu de société par ex. un Monopoly ou un plateau de jeu Serpents et Échelles, pour en faire un jeu de sécurité prêt à l'emploi.

Remettre des prix

Récompensez les meilleurs participants, les plus créatifs avec des cadeaux d'entreprise !

Utiliser la langue courante

Évitez le jargon et les acronymes de la sécurité, ainsi que toute remarque, même voilée, sur les habitudes de sécurité actuelles des dirigeants.

Des cas d'usage de la vie réelle pour faire le lien

Pensez aussi à souligner l'impact des attaques sur la vie personnelle et professionnelle à l'aide d'études de cas dans un secteur, un poste de direction ou un profil de risque proches. N'oubliez pas de montrer à la fois les bonnes et les mauvaises réactions !

Exemple d'étude de cas : Levitas Capital[6]

Incident :

En 2020, l'un des fondateurs de Levitas Capital a cliqué sur un lien Zoom falsifié qui a installé un logiciel malveillant sur le réseau de l'entreprise. Les pirates ont volé 800 000 dollars avant que la ruse ne soit découverte.

Ce qui a mal tourné :

En bref ? Les circuits normaux d'approbation des transferts financiers ont été rompus, les pirates ont pris le contrôle du système d'e-mail de l'entreprise et, à deux reprises, ils se sont fait passer pour un cofondateur du fonds auprès d'un administrateur tiers.

Conséquences :

Le plus gros client de Levitas a perdu confiance et les a quittés, et le fonds spéculatif a fermé deux mois après l'événement ... Une chute très médiatisée pour les deux fondateurs du fonds, Michael Brookes et Michael Fagan.

« Les très nombreux signaux d'alerte ont tous été ignorés. »

Michael Fagan
Cofondateur de Levitas Capital

4 Envisager la mise en place d'un service haut de gamme de sécurité pour la direction

Leur profil et l'étendue de leurs accès rendent les dirigeants dignes d'une attention toute particulière de la part des équipes de sécurité, une sorte de service haut de gamme.

De fait, les cadres dirigeants sont deux fois plus susceptibles de déclarer leurs interactions insatisfaisantes avec l'équipe Sécurité et quatre fois plus de faire appel à une assistance technique extérieure. Pour renverser la tendance, un programme premium va viser à renforcer la confiance et à faire tomber les obstacles au signalement des erreurs ou aux questions de sécurité.

Pour créer votre programme de sécurité haut de gamme, vous pouvez :

Désigner un interlocuteur unique (autre que le RSSI !) pour les dirigeants. Vous pourrez ainsi rétablir la confiance tout en consolidant et en normalisant la communication.

Repenser l'onboarding des collaborateurs de Direction, avec des permissions d'accès personnalisées et la configuration d'un gestionnaire de mots de passe personnalisé. Si les dirigeants eux-mêmes n'ont pas toujours le temps de suivre toute une procédure pour appliquer les configurations appropriées, votre entreprise risquerait de payer très cher l'absence de ces garde-fous.

Appliquer les stratégies de déprovisionnement via l'automatisation, sans omettre les vérifications manuelles de l'offboarding pour éviter les informations d'authentification zombies.

Développer une formation individuelle et sur mesure à la sécurité, qui ne soit pas une présentation générique facile à ignorer ignorer. Utilisez les exercices sur table précédents et sélectionnez des études de cas dont les incidents font écho au rôle ou au département du nouveau dirigeant.

Quelles que soient les mesures que vous choisirez, il s'agit pour vous et votre équipe d'impulser une culture de sécurité positive et non punitive, et d'amener la Direction vers plus de conformité par des actions de formation et de sensibilisation engageantes et des partages d'information.

Les études de cas citées dans ce rapport le prouvent : les erreurs humaines existent. Et elles *vont* se produire dans votre entreprise. Elles sont inévitables et impossibles à éliminer totalement.

Dès lors, seules les entreprises fortes d'une véritable adhésion de leurs dirigeants pourront restaurer les systèmes et la confiance, et se forger un avenir au-delà de la crainte d'une violation.

Retrouvez toute la série d'études et de rapports d'Ivanti sur la cybersécurité !

Références

1. Proofpoint. (2022, May). 2022 Voice of the CISO: Global Insights Into CISO Challenges, Expectations and Priorities. From Proofpoint: https://go.proofpoint.com/en-voice-of-the-ciso-2022.html

2. Yip, K. N. (2016, May 21). Whaling Case Study: Mattel's $3 Million Phishing Adventure. From Infosec: https://resources.infosecinstitute.com/topic/whaling-case-study/

3. Pratt, M. K. (2023, February 28). Economic pressures are increasing cybersecurity risks; a recession would amp them up more. From CSO Online: https://www.csoonline.com/article/3689008/economic-pressures-are-increasing-cybersecurity-risks-a-recession-would-amp-them-up-more.html

4. Metz, C. (2023, March 29). Florida principal resigns after sending $100K to scammer posing as Elon Musk. From CBS News Miami: https://www.cbsnews.com/miami/news/florida-principal-resigns-after-sending-100k-to-scammer-posing-as-elon-musk/

5. Garzón, G., & Garzón, F. (2020, June 30). Cybersecurity Incident Response: Tabletop Exercises Using the Lego Serious Play Method. From ISACA: https://www.isaca.org/resources/isaca-journal/issues/2020/volume-4/cybersecurity-incident-response

6. SecureWorld News Team. (2020, November 23). Hedge Fund Closes Down After Cyber Attack. From SecureWorld: https://www.secureworld.io/industry-news/hedge-fund-closes-after-bec-cyber-attac

Pleins feux sur la sécurité des dirigeants en 2023

Dans une nouvelle étude, Ivanti dévoile les risques réels qui pèsent sur les hauts dirigeants.

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

ivanti

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