Avec les compliments de :

MetaCompliance®

Sensibilisation à la cybersécurité

pour les nuls®

Changez la culture de sécurité du personnel

Créez un personnel plus soucieux de la sécurité

Suivez ce guide pour les campagnes de cybersécurité

Robert O'Brien

Geraldine Strawbridge

Édition spéciale MetaCompliance

À propos de MetaCompliance

MetaCompliance possède plus de 14 ans d'expertise dans le domaine de la formation et de la sensibilisation du personnel à la sécurité. Travaillant avec des clients de tous les secteurs, la société aide les organisations à protéger leurs données, à former leur personnel et à gérer les risques liés à la réputation et à la réglementation. Au cours de cette période, le défi réglementaire auquel sont confrontées les organisations a augmenté, tout comme le paysage des menaces associées à leurs actifs numériques.

L'entreprise est un leader d'opinion dans « l'aspect humain » de la cybersécurité et de la conformité. L'équipe de MetaCompliance travaille quotidiennement avec des clients des secteurs public et privé pour mettre en œuvre les meilleures pratiques en matière de campagnes de sensibilisation à la sécurité pour le personnel, qui mobilisent réellement les gens et modifient les comportements.

Sa plateforme SaaS au graphisme convivial offre aux clients une suite intégrée et multilingue de fonctionnalités comprenant la simulation de phishing, la formation en ligne sur la cybersécurité et la conformité, la gestion des stratégies, la gestion de la confidentialité et la gestion des incidents. Les organisations bénéficient d'une meilleure protection réglementaire grâce à un système unique pour la gestion des projets relatifs à la confidentialité, à la conformité et à la cybersécurité, ce qui permet au personnel de s'acquitter plus facilement de ses obligations en matière de conformité.

L'architecture cloud innovante MyCompliance de MetaCompliance est conçue sur la plateforme Microsoft Azure, offrant ainsi une solution professionnelle globale. MetaCompliance est basée à Londres, au Royaume-Uni, à Dublin, en Irlande et à Atlanta, en Géorgie, et compte une clientèle croissante dans les secteurs public et privé.

Sensibilisation à la cybersécurité

pour les nuls®

Sensibilisation à la cybersécurité

Édition spéciale MetaCompliance

par Robert O'Brien, expert en cybersécurité et conformité
Geraldine Strawbridge, rédactrice dans le domaine de la cybersécurité

pour les nuls®

Sensibilisation à la cybersécurité pour les Nuls®, édition spéciale MetaCompliance

Édité par : **John Wiley & Sons, Ltd.,** The Atrium, Southern Gate

Chichester, West Sussex, www.wiley.com

Siège social

John Wiley & Sons, Ltd., The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, Royaume-Uni

ISBN 978-1-119-89963-1 (pbk) ; ISBN 978-1-119-89964-8 (ebk)

Imprimé en Grande-Bretagne

10 9 8 7 6 5 4 3 2 1

Table des matières

Introduction

Au cours des dix dernières années, le paysage de la cybersécurité a changé de façon spectaculaire. Selon Cybersecurity Ventures, d'ici 2021, le coût mondial de la cybercriminalité devrait atteindre 6 000 milliards de dollars : c'est une activité encore plus rentable que l'ensemble du commerce mondial de drogues illégales. Les organisations de toutes tailles et dans tous les secteurs sont devenues des cibles potentielles pour les cybercriminels. De nouvelles menaces apparaissent en permanence et les organisations ne peuvent plus se contenter de compter sur leurs défenses technologiques pour assurer leur sécurité.

Les cybercriminels ciblent le point le plus faible des défenses d'une organisation et, trop souvent, il s'agit de vos employés. Une énorme proportion de toutes les violations de données, soit 90 %, peut être attribuée à une erreur humaine. C'est pourquoi les organisations doivent s'engager dans un programme de sensibilisation à la cybersécurité qui permet à l'ensemble du personnel de reconnaître et d'accepter le rôle important qu'il joue dans la protection des données sensibles de l'entreprise.

À propos de ce livre

L'ouvrage Sensibilisation à la cybersécurité pour les Nuls, édition spéciale MetaCompliance, se compose de six chapitres qui explorent le paysage moderne de la cybersécurité (chapitre 1), la nécessité d'une sensibilisation à la cybersécurité (chapitre 2), l'adoption de campagnes de cybersécurité pour promouvoir le changement (chapitre 3), l'intégration de la gestion des politiques dans les programmes de sensibilisation à la sécurité (chapitre 4), les moyens de développer une stratégie de cybersensibilisation conforme aux meilleures pratiques (chapitre 5) et les bonnes pratiques de sensibilisation à la sécurité (chapitre 6).

Chaque chapitre est indépendant du reste de l'ouvrage. Si un sujet vous intéresse, vous pouvez donc passer directement au chapitre qui s'y rapporte. Vous pouvez lire cet ouvrage dans le sens qui vous convient (même si nous vous déconseillons de le lire à l'envers ou de droite à gauche).

Quelques suppositions idiotes

Lorsque nous avons rédigé ce livre, nous sommes partis du principe que vous étiez un professionnel de la cybersécurité ou de l'informatique, par exemple un directeur de l'information (DPI), un directeur des technologies (CTO), un directeur de la sécurité de l'information (CISO), un directeur de la confidentialité (CPO), un responsable de la protection des données, un directeur informatique, un responsable informatique, un responsable des ressources humaines (RH), un responsable de la formation, un responsable du changement ou même un cadre supérieur.

Si l'une de ces hypothèses vous correspond, alors ce livre est pour vous. Si aucune de ces hypothèses ne vous concerne, poursuivez quand même votre lecture. Lorsque vous aurez terminé cet ouvrage, vous aurez une conscience accrue de la cybersécurité.

Icônes employées dans ce livre

Nous utilisons occasionnellement des icônes spéciales pour attirer l'attention du lecteur sur des informations importantes. Voici à quoi vous attendre :

RAPPEL

Cette icône signale des informations importantes à inscrire obligatoirement dans votre mémoire non volatile, votre matière grise ou votre crâne, à côté des dates d'anniversaire.

CONSEIL

Nous espérons que vous apprécierez ces informations utiles.

ATTENTION

Ces alertes donnent des conseils pratiques pour vous permettre d'éviter des erreurs potentiellement coûteuses ou frustrantes.

Au-delà de ce livre

Ce sujet est tellement vaste qu'il est impossible de tout aborder dans ces pages. Donc, s'il vous arrive de penser, en refermant ce livre : « Oh, ce livre était génial ; où puis-je en savoir plus ? », rendez-vous sur `www.metacompliance.com`.

DANS CE CHAPITRE

- Analyse de l'évolution du paysage des menaces
- Identification des motivations d'un cybercriminel
- Intégration de la sensibilisation à la sécurité dans la transformation numérique
- Explication des cadres de sécurité et de la protection des données
- Examen des mandats de conformité aux normes en vigueur

Chapitre 1
Comprendre le paysage moderne de la cybersécurité

Dans ce chapitre, vous découvrirez comment des cybermenaces sophistiquées, ainsi que des niveaux de gouvernance plus élevés, des réglementations en matière de protection des données et le besoin de sécurité dès la conception ont augmenté la nécessité de sensibilisation à la cybersécurité dans l'organisation moderne.

Examen des cybermenaces ciblant les personnes

La cybercriminalité est rapidement devenue l'une des plus grandes menaces pesant sur les organisations du monde entier. Les vecteurs d'attaque changent, les cybercriminels utilisant toute une série de tactiques différentes pour accéder aux précieuses données des entreprises.

Si les organisations veulent minimiser le risque de violation de la sécurité, elles doivent comprendre les différents types de cybermenaces qui pourraient être utilisées pour les cibler :

- **Phishing :** le *phishing* est un type d'attaque d'ingénierie sociale qui vise à inciter les victimes à divulguer des informations sensibles ou à installer des logiciels malveillants. En utilisant le courrier électronique, les médias sociaux, les appels téléphoniques et les SMS, les cybercriminels se font passer pour une entité de confiance afin de manipuler leur victime pour qu'elle effectue une action spécifique, comme par exemple cliquer sur un lien malveillant, télécharger une pièce jointe, visiter un site Web frauduleux ou divulguer volontairement des informations sensibles. Ces informations peuvent ensuite être utilisées pour accéder à des comptes personnels ou commettre un vol d'identité.
- **Malware :** un *malware* est un type de logiciel malveillant conçu pour endommager un système informatique ou y accéder à l'insu de l'utilisateur. Les virus, les vers, les chevaux de Troie, les logiciels espions, les logiciels publicitaires et les ransomwares sont des exemples de malware. Les logiciels malveillants sont généralement installés sur un ordinateur lorsqu'un utilisateur clique sur un lien, télécharge une pièce jointe malveillante ou ouvre un logiciel fictif. Une fois installé, le logiciel malveillant peut voler, supprimer ou chiffrer des données sensibles. Il peut également bloquer les fonctions informatiques essentielles, en rendant ainsi un système inopérant.
- **Menace interne :** une *menace interne* est un incident de sécurité qui trouve son origine au sein d'une organisation et non pas dans une source externe. Il peut s'agir d'un employé ou ex-employé, d'un sous-traitant, d'un fournisseur tiers ou de tout autre partenaire commercial ayant accès aux données et aux systèmes informatiques de l'organisation. Les attaques internes peuvent être particulièrement dangereuses car, contrairement aux acteurs externes qui tentent d'infiltrer un réseau, les acteurs internes ont généralement un accès légitime aux systèmes informatiques d'une organisation.
- **Attaques de la chaîne logistique :** une attaque de la chaîne logistique, également appelée *attaque par un tiers*, tente de nuire à une organisation en exploitant les vulnérabilités de son réseau de chaîne logistique. Les *attaques de la chaîne logistique* peuvent potentiellement infiltrer un réseau entier par le biais d'une seule compromission. Elles peuvent être plus difficiles à détecter que les attaques traditionnelles de logiciels malveillants.

ATTENTION

La nature humaine constitue une vulnérabilité majeure et les cybercriminels savent comment l'exploiter.

Comprendre les profils et les motivations des pirates

La culture populaire a dépeint les pirates informatiques de diverses manières, souvent sous la forme d'un personnage portant un sweat à capuche dans une cave ou d'un adolescent mécontent désireux de mettre le monde à sac. L'un des exemples les plus notables au cinéma est la pirate informatique fictive Lisbeth Salander, héroïne du film *Millénium : Les Hommes qui n'aimaient pas les femmes* (The Girl with the Dragon Tattoo) de Stieg Larsson. Lorsqu'elle est présentée pour la première fois, elle utilise ses compétences de hacker pour le compte d'une société de sécurité privée. Mais à mesure que l'intrigue se complique, ses talents de pirate informatique sont motivés par la vengeance, ce qui lui permet finalement de prendre sa revanche sur l'un des principaux « méchants » en réalisant une audacieuse fraude financière. Cela montre que les personnes impliquées dans la cybercriminalité sont animées par de nombreuses motivations différentes.

Il est important pour votre organisation de comprendre leurs motivations afin de savoir comment faire face aux pirates informatiques. Voici quelques-unes des raisons qui motivent les pirates dans leurs activités criminelles :

- **L'argent :** l'argent est le principal facteur de motivation de toute activité criminelle, et la cybercriminalité ne fait pas exception. Il s'agit tout simplement d'un vol à l'ère numérique, et c'est beaucoup plus facile à réaliser que de braquer une banque avec une arme à feu. Malgré les piratages très médiatisés des grandes marques, les attaques ciblent de plus en plus les petites et moyennes entreprises dont les pratiques de sécurité sont moins sophistiquées. En réalité, il est beaucoup plus lucratif pour un pirate informatique de s'attaquer à une myriade de petites organisations qu'à une entreprise du classement Fortune 100 qui a investi des millions dans le renforcement de ses défenses technologiques.
- **L'espionnage :** les pirates informatiques ont souvent recours au cyberespionnage pour voler des informations confidentielles, de la propriété intellectuelle ou des secrets commerciaux. Qu'il s'agisse d'une attaque d'un État-nation ou de l'espionnage d'une entreprise, l'espionnage constitue désormais une menace importante pour toutes les organisations.

  Toutes ces violations montrent à quel point les pirates informatiques ont redoublé d'activité dans deux domaines clés qui les motivent : la politique et le secteur industriel.

RAPPEL

Les infrastructures stratégiques comme les transports, l'eau, les télécommunications et les services publics font également l'objet d'une attention particulière de la part des entités soutenues par un État. La militarisation des logiciels malveillants par des entités gouvernementales étrangères va mettre à mal toutes les organisations, à l'exception des plus grandes et des mieux dotées en ressources, et le principal facilitateur de ces vecteurs d'attaque est l'homme, ce qui peut surprendre. L'ingénierie sociale et l'exploitation de pratiques de sécurité inadéquates sont les premiers domaines qu'un cybercriminel tentera d'exploiter. C'est pourquoi il est impératif que les organisations mobilisent leur propre personnel pour se défendre contre ces menaces. La mise en œuvre d'un programme de sensibilisation du personnel adapté est fondamentale pour défendre votre organisation.

- **Le divertissement :** de nombreux pirates sont motivés par le plaisir et l'excitation à l'idée d'infiltrer le système informatique d'une entreprise. Par exemple, lors du concours de piratage éthique Pwn2Own de cette année, les organisateurs ont fourni une Tesla Model 3 aux participants pour qu'ils la piratent. En l'espace d'une journée, deux pirates ont découvert un bug de sécurité qui leur a permis de pirater le navigateur Web interne de la voiture. Loin de faire face à des poursuites judiciaires, le duo est reparti avec sa propre Tesla Model 3, la somme de 375 000 dollars $ et, surtout, la reconnaissance de ses pairs, ce qui est très recherché dans la communauté des hackers.
- **L'hacktivisme :** *l'hacktivisme* est le fait de pirater un système ou un réseau informatique à des fins politiques ou sociales. Il y a toujours eu et il y aura toujours des personnes qui se tournent vers l'activisme pour une cause spécifique allant à l'encontre des institutions. Ce qui est nouveau, c'est la technologie omniprésente.

  La technologie est désormais une arme, de plus en plus utilisée pour promouvoir des objectifs idéologiques. L'une des raisons de cette croissance est que lancer une cyberattaque revient beaucoup moins cher qu'une action militaire directe.
- **Le vol de ressources :** siphonner les ressources informatiques du grand public pour miner du bitcoin est devenu une activité rentable. Le minage du bitcoin est une activité gourmande en électricité et en puissance de traitement, et les pirates informatiques exploitent toutes les opportunités qui s'offrent à eux pour voler ces ressources. Même des multinationales comme Starbucks en ont été victimes. Par exemple, un magasin de Buenos Aires a récemment découvert que son réseau Wi-Fi avait été piraté et que des fraudeurs l'utilisaient pour miner du bitcoin sur les appareils de clients peu méfiants.

- **Autre :** on peut ranger dans cette catégorie les menaces internes, les fuites de données involontaires, les erreurs de configuration, les erreurs des utilisateurs et toute une série d'autres menaces sans rapport avec les efforts de piratage de tiers. Les méthodes les plus probables pour une compromission sont les logiciels non corrigés et l'ingénierie sociale. Ces menaces représentent le plus grand risque pour la plupart des organisations.

Cadres de sécurité et protection des données

Les questions les plus importantes que votre organisation doit se poser sont les suivantes : ***Quelle est la meilleure façon de mettre en œuvre un système de gestion de la sécurité pour mon organisation, et quelles sont les parties impliquées ?***

La norme ISO 27001, qui définit une approche des meilleures pratiques en matière de management de la sécurité des systèmes d'information, peut apporter une réponse.

ISO 27001 – La norme mondiale en matière de cybersécurité

La confidentialité et la protection des données sont des initiatives importantes pour les organisations modernes. Les activités de préparation et de maintien de la confidentialité sont une tâche d'envergure pour n'importe quelle organisation. Il importe donc que les employés disposent du temps et de la formation nécessaires pour comprendre quelles sont leurs obligations quotidiennes en matière de confidentialité dans le cadre de leur travail.

La norme ISO 27001 est une véritable norme de sécurité mondiale, et c'est aussi la seule qui soit soumise à un audit externe. Elle permet aux organisations d'adopter une approche uniforme pour démontrer qu'elles appliquent les meilleures pratiques en matière de processus de sécurité des systèmes d'information. Les avantages de la norme ISO 27001 sont notamment liés au fait que le certificat montre que l'organisation est préparée à faire face en cas de problème. Le certificat ISO 27001 est devenu un atout commercial de plus en plus précieux, car les clients demandent à leur chaîne logistique des assurances en matière de cyberrisques.

Tirer parti des avantages de la norme ISO 27001

Les efforts et l'implication de la direction nécessaires pour obtenir l'accréditation ISO 27001 sont garants d'une plus grande maturité de

l'organisation en matière de cybersécurité. De plus, cette norme apporte d'autres avantages :

- Résilience accrue de l'entreprise et protection contre les défaillances de sécurité
- Confiance renforcée des clients
- Fiabilité et sécurité accrues des systèmes de base et du matériel informatique
- Plus de focalisation sur les risques et leur impact sur l'entreprise

Un programme de sensibilisation du personnel adapté est requis pour obtenir la certification ISO 27001. Plus précisément, les clauses 7.2, 7.3 et 7.4 de la norme ISO IEC 27001 portent sur la connaissance et la compréhension du système de management de la sécurité des systèmes d'information (SMSI) en cours de certification. Une formation générale à la cybersécurité ne répondra pas nécessairement aux exigences de conformité de la norme ISO 27001, d'autant plus que le système SGSI de chaque organisation est propre à l'ensemble des risques et des systèmes qui sous-tendent ses activités.

Il est essentiel que les membres du personnel soient sensibilisés au fonctionnement des processus de sécurité au sein de leur organisation, ce qui implique généralement une formation sur mesure portant sur le SMSI de l'organisation. Une campagne de sensibilisation aux meilleures pratiques couvrira les principales cybermenaces, allant du phishing à la sécurité physique, et favorisera également la participation et la bonne connaissance de l'initiative ISO 27001. Une formation spécifique relative au SMSI de l'organisation est également requise, qui peut prendre la forme d'un simple séminaire en ligne organisé à l'échelle de l'organisation pour donner un aperçu de son fonctionnement.

CONSEIL

En faisant de votre SMSI le point de départ de votre campagne de cybersensibilisation, vous vous concentrerez sur les cybermenaces spécifiques qui concernent votre organisation et votre personnel, en évitant ainsi tout phénomène de lassitude de la part des utilisateurs. Au fur et à mesure de l'évolution du paysage des menaces, la réponse apportée par votre SMSI évoluera elle aussi. L'essentiel est d'accompagner votre personnel dans cette démarche et de veiller à ce qu'il soit informé de tout changement.

Un autre cadre très respecté, largement utilisé par les organisations du monde entier pour normaliser les processus, réduire les risques et améliorer les opérations de cybersécurité, est le cadre de cybersécurité du NIST (voir encadré).

CADRE DE CYBERSÉCURITÉ DU NIST

Le National Institute of Standards and Technology (NIST) des États-Unis a créé un cadre de cybersécurité (CSF) pour fournir aux organisations des conseils sur la manière de prévenir, de détecter et de répondre aux cyberincidents. Ce cadre, reconnu au niveau international, présente un ensemble de bonnes pratiques, de normes et de recommandations qui aident une organisation à améliorer sa politique de cybersécurité.

Initialement conçu pour améliorer les services d'infrastructure stratégiques, le NIST CFS a depuis été adopté dans divers secteurs et aidé les organisations à adopter une attitude plus proactive en matière de gestion des risques.

Ce cadre est divisé en trois parties :

- **Le cadre de base** définit un ensemble d'activités permettant d'atteindre des résultats spécifiques en matière de cybersécurité. Il repose sur cinq opérations :
- **Identification :** développer la connaissance organisationnelle afin de gérer les risques de cybersécurité pour les systèmes, les actifs, les données et les capacités.
- **Protection :** élaborer et mettre en œuvre les précautions appropriées pour assurer la fourniture des services d'infrastructure essentiels.
- **Détection :** développer et mettre en œuvre les activités appropriées pour identifier l'occurrence d'un événement de cybersécurité.
- **Réponse :** élaborer et mettre en œuvre les activités appropriées pour intervenir en réponse à un événement de cybersécurité ayant été détecté.
- **Récupération :** élaborer et mettre en œuvre les activités appropriées pour maintenir les plans de résilience et restaurer les capacités ou les services qui ont été altérés en raison d'un événement de cybersécurité.

Ces fonctions sont sous-divisées en 22 catégories et 98 sous-catégories.

- **Les niveaux de mise en œuvre du cadre** fournissent un contexte sur la façon dont les organisations considèrent le risque et les processus qui peuvent être mis en place pour atténuer ce risque.
- **Le profil du cadre** décrit les résultats souhaités, en fonction des catégories et sous-catégories du cadre.

L'importance de sensibiliser le personnel aux projets de transformation numérique

Les projets de transformation numérique sont des initiatives passionnantes au sein des organisations modernes. Ils représentent une opportunité pour l'entreprise d'exploiter de nouvelles technologies et d'adopter des produits qui réduisent les coûts et entraînent une augmentation des revenus.

Les projets de transformation numérique sont généralement des stratégies ambitieuses visant à modifier la manière dont une entreprise exerce ses activités en s'appuyant sur les technologies numériques.

Ce sont des initiatives majeures de gestion du changement, et nécessitent un investissement important dans la communication avec le personnel. Ces communications visent à susciter le soutien et l'enthousiasme du personnel. Souvent, ces initiatives ne mettent pas l'accent sur le risque posé par le manque de prudence et de diligence nécessaires en matière de sécurité informatique et de conformité. Or, c'est exactement ce qu'il faut pour trouver un équilibre entre obtenir la transformation à tout prix et assurer un contrôle et des précautions appropriés. Consultez le chapitre 3 pour découvrir comment communiquer de la façon la plus efficace avec le personnel.

DANS CE CHAPITRE

- Comprendre le profil de risque
- Reconnaître les défis que représente la création d'un personnel plus vigilant
- Être conscient des risques et veiller à ce que la cybersécurité reste pertinente

Chapitre 2
Déterminer le besoin de sensibilisation à la cybersécurité

Très peu de guides pratiques ou de manuels fournissent les conseils nécessaires pour planifier, développer et mettre en œuvre un programme de sensibilisation du personnel à la cybersécurité. En partie, cela vient du fait que le secteur de la sécurité informatique a été obsédé par les technologies traditionnelles comme les pare-feux et les solutions anti-malware. Ces défenses technologiques ont apporté un semblant de sécurité en faisant croire que le périmètre est défendu.

Malgré cet investissement important dans la sécurité du périmètre, il existait, et il existe toujours, un niveau de « déni plausible » selon lequel les actions d'un seul employé peuvent contourner totalement ces contrôles.

Vu les violations de données se produisant régulièrement dans les organisations de premier ordre, il est reconnu dans le monde entier que les conséquences de ces incidents sont trop graves pour être ignorées. C'est pourquoi ce problème figure à l'ordre du jour des conseils d'administration de la plupart des organisations modernes. En outre, les régulateurs ont de plus en plus recours à des sanctions et à des amendes pour inciter les entreprises à respecter les nouvelles réglementations en matière de

protection des données. Ces facteurs, ainsi que d'autres influences macroéconomiques, ont nécessité un changement radical dans la manière dont les employés accomplissent leurs tâches et minimisent les risques.

Le fait que le conseil d'administration reconnaisse l'importance du risque de cybersécurité comme une responsabilité légitime de l'entreprise est une étape majeure dans la maturation d'une organisation. La principale restriction de tout projet de sensibilisation à la cybersécurité est la mesure dans laquelle les dirigeants de l'organisation reconnaissent le cyberrisque et lui accordent la même importance et les mêmes ressources que le risque financier. Le chapitre 5 aborde plus en détail la question du soutien de la direction à votre campagne.

Ce chapitre explique plus en détail ce que vous pouvez faire pour que votre entreprise soit sensibilisée à la cybersécurité.

Comprendre le profil de risque

Que se passerait-il si votre organisation était piratée ? Est-ce probable et quel en serait l'impact ? Pour comprendre les réponses à ces questions, vous devez connaître le profil de risque unique auquel votre organisation est confrontée. La mesure dans laquelle les cybermenaces concernent votre organisation détermine le niveau de vulnérabilité de cette dernière. La compréhension de ces vulnérabilités et la mise en place de plans de remédiation constituent une approche des meilleures pratiques pour réduire l'exposition de votre organisation au risque de cybersécurité. Cela est particulièrement pertinent lorsqu'il s'agit de votre personnel et de vos chaînes logistiques, car ce sont des voies d'attaque courantes pour les tiers malveillants.

Les sections suivantes fournissent des informations pratiques pour aider votre organisation à réduire ses risques.

Mise en œuvre d'une campagne de sensibilisation aux risques

Il est important de s'attaquer aux comportements du personnel concernant les risques liés à la cybersécurité et à la protection des données. Une campagne de sensibilisation vise à remédier aux risques qui découlent de l'aspect humain de la cybersécurité.

Cependant, les campagnes de sensibilisation à la sécurité qui se concentrent uniquement sur la formation rapide du personnel à la cybersécurité ont un succès limité. Un véritable changement de comportement nécessite une formation continue associée à un effort

important de la part de l'organisation. Il faut aussi du temps, car les personnes sont naturellement réfractaires au changement.

Identifier la compréhension du risque par votre personnel

Votre organisation dispose de plusieurs moyens pour déterminer rapidement la compréhension des risques de sécurité par votre personnel. Par exemple :

- **Envoyez à tout le personnel une simulation de phishing et voyez combien d'employés tombent dans le piège.** Portez une attention particulière aux utilisateurs qui étaient prêts à saisir des informations d'identification ou des informations réelles après avoir reçu une invitation provenant d'un e-mail frauduleux. Ce taux de clics vous fournira un point de départ.
- **Effectuez une analyse rapide des incidents survenus au cours des 12 mois précédents.** Existe-t-il des incidents similaires qui ressemblent à une tendance ou à une récurrence ? Définissez les priorités de votre programme de sensibilisation en fonction de ces risques.

Ces informations sont également cruciales pour expliquer au personnel pourquoi la formation à la cybersécurité est si importante. Exemple : « l'année dernière, 20 ordinateurs portables ont été perdus dans cette entreprise. Veuillez améliorer votre compréhension des meilleures pratiques de gestion des appareils en suivant la formation en ligne ci-jointe. »

Axer la formation uniquement sur les personnes qui en ont besoin

La sensibilisation à la cybersécurité avec contexte et segmentation a renforcé l'efficacité. Par exemple, la formation de l'ensemble du personnel sur le contrôle des ordinateurs portables et des appareils est inefficace si seul un petit nombre d'employés possède un ordinateur portable. Seuls les employés disposant d'un appareil ont besoin de ce type de formation. Il est contre-productif de faire suivre à l'ensemble des employés une formation générique sur la sécurité. Dans la mesure du possible, votre organisation doit cibler la formation de sensibilisation en fonction du rôle et du risque spécifiques d'une personne.

Les campagnes de sensibilisation à la cybersécurité ont plus d'impact si elles portent sur des risques compréhensibles et si les gens peuvent identifier les conséquences réelles qui résultent de pratiques négligentes en matière de cybersécurité.

CONSEIL

Organisez les risques liés à la sécurité des systèmes d'information en fonction des ressources humaines et technologiques. Ces dernières concernent les systèmes métiers stratégiques d'une organisation et les données qui résident sur ces systèmes. Du point de vue de la sensibilisation, il est important de veiller à ce que les bons messages parviennent aux personnes qu'il faut et au bon moment. Reconnaissez également que les utilisateurs et les données ne sont pas tous égaux face aux risques.

Par exemple, le service financier est plus exposé à une cyberattaque qu'un membre du personnel de la cafétéria. La prise en compte des différents rôles au sein de l'organisation est importante pour élaborer une campagne de sensibilisation efficace, car vous pourrez ainsi vous concentrer sur vos employés à haut risque au lieu de cibler tout le monde de manière globale.

Identifier les employés ayant besoin d'une formation plus approfondie

Consacrer du temps à élaborer des communiqués spécifiques ou à fournir une formation pertinente à ces groupes d'employés est extrêmement efficace, en particulier si vous utilisez un langage qu'ils connaissent bien.

L'identification des groupes vulnérables de votre personnel prend du temps. Cependant, les trois groupes les plus importants devant recevoir une formation supplémentaire sur les risques sont les suivants :

- **Le service financier :** ce service est généralement le plus à risque d'être ciblé dans une organisation parce qu'il contrôle les fonds de l'entreprise.
- **Les utilisateurs techniques privilégiés :** ces utilisateurs sont ciblés, car ils peuvent être utilisés pour intensifier une cyberviolation en raison de leur accès privilégié à des systèmes sécurisés.
- **Les cadres supérieurs de la société :** les cadres supérieurs sont visés parce qu'ils disposent d'une autorité qui peut être utilisée pour intensifier une cyberviolation.

N'oubliez pas l'ensemble de votre chaîne logistique et votre réseau de partenaires. Ceux-ci représentent également une grande partie de votre profil de risque. Le chapitre 3 examine plus en détail la manière dont vous pouvez identifier les tiers les plus exposés, le risque qu'ils représentent dans une organisation agile moderne et les moyens de les inclure dans vos activités de cybersécurité.

En outre, moins les employés ont de l'ancienneté dans l'organisation, plus il est facile de modifier leur comportement. En effet, les nouveaux utilisateurs peuvent accepter les politiques et apprendre volontiers de nouvelles méthodes de travail, car ils ont un état d'esprit plus souple. En revanche, les membres du personnel employés depuis plus longtemps peuvent s'avérer plus récalcitrants à l'apprentissage de nouvelles méthodes.

De plus, l'identification du nombre de langues couramment parlées dans votre organisation est également importante dans la cartographie de votre profil de risque. Non seulement une variété de langues peut rendre plus difficile la mise en place d'un programme de sensibilisation du personnel, mais elle augmente aussi le nombre de vecteurs de menaces auxquels votre organisation doit faire face.

Par exemple, une organisation qui exerce son activité au Brésil doit s'inquiéter des e-mails de phishing en portugais comme en anglais. L'identification de vos principaux profils culturels et linguistiques est importante pour rendre le programme de sensibilisation à la sécurité pertinent pour votre personnel.

Hiérarchisation des risques de sécurité

Dans de nombreuses organisations, la sécurité n'a pas été considérée par le personnel comme une priorité au même titre que le risque financier. La sécurité n'était pas considérée comme un aspect incontournable au bon déroulement des affaires et, par conséquent, les utilisateurs ont pris de mauvaises habitudes pendant plusieurs années. Il est donc plus difficile de mettre en œuvre une campagne de sensibilisation à la sécurité. Votre campagne doit former les utilisateurs à la sécurité, mais elle doit aussi surmonter les mauvaises habitudes qui se sont accumulées au fil du temps. Ce n'est qu'en étant cohérent et en répétant le message de votre campagne que votre organisation pourra convaincre vos employés.

Les systèmes existants difficiles à modifier sont souvent utilisés comme un prétexte pour éviter de changer les comportements. Vous avez déjà peut-être entendu quelqu'un dire : « notre système fonctionne de cette façon, il est donc inutile d'essayer de changer ». Surmonter ce type d'attitude peut être difficile.

Les problèmes de sécurité liés aux systèmes existants peuvent conduire à un sentiment d'impuissance face aux menaces pour la sécurité. Par exemple, lorsqu'un système de contrôle d'accès est géré sur un système d'exploitation Windows obsolète, on peut comprendre que le remplacement de toutes les serrures électroniques d'une organisation par un système qui fonctionne par ailleurs parfaitement bien n'est peut-être pas le meilleur investissement.

Cependant, ces types de systèmes existants doivent être remplacés dès que possible. Le personnel a besoin de savoir que l'organisation a identifié ces défis et qu'elle tente activement de les résoudre. Bien que ces activités soient réalisées en arrière-plan et en dehors du cadre d'un programme de sécurité destiné au personnel, il est essentiel de progresser sur ces questions afin d'assurer l'intégrité de toute campagne de sensibilisation des employés.

Faire de la cybersécurité une réalité pour les membres de votre organisation

Il est peu probable que les programmes de sensibilisation à la cybersécurité suscitent l'enthousiasme du personnel et de la direction.

RAPPEL

Lorsque vous envisagez de mettre en place un programme visant à sensibiliser le personnel à la sécurité des systèmes d'information, gardez à l'esprit que la plupart des gens ne passent que très peu de temps, voire aucun, à réfléchir à cette question. Il est difficile de rendre la cybersécurité intéressante. Cependant, il incombe à l'organisation de rendre ses communications sur la sécurité acceptables et même agréables, si possible, pour ses employés.

L'obtention de la participation des utilisateurs à vos programmes de sensibilisation à la cybersécurité est l'une des principales mesures du succès. Par exemple, si vous envoyez une évaluation des risques ou un document d'apprentissage en ligne et que seulement 50 % de votre personnel y participe, vous avez un gros problème. Une partie importante de votre personnel ne se sent pas impliquée dans votre programme. Plus important encore, votre organisation ne peut pas démontrer sa conformité. Il est également probable que les récalcitrants à votre programme de cybersécurité se trouvent parmi les 50 % du personnel qui n'ont pas répondu à la communication ni suivi la formation.

Votre organisation peut répondre à cette situation de trois façons différentes :

- La direction peut ignorer les personnes qui n'ont pas participé et espérer que tout ira bien. Cette approche est peut-être populaire mais, en fin de compte, elle est vouée à l'échec. Les régulateurs attendront des preuves de vos efforts pour faire participer ces utilisateurs au programme de sensibilisation.
- La direction peut commencer à solliciter sans cesse les utilisateurs pour qu'ils remplissent leurs obligations de sensibilisation à la cybersécurité. Cette opération gourmande en main-d'œuvre n'est pas la

bienvenue pour la direction et relègue la sécurité des systèmes d'information au fin fond des préoccupations organisationnelles.

- Les solutions technologiques peuvent avoir un impact significatif sur les utilisateurs afin de les inciter à remplir leur mission de sécurité.

En définitive, la campagne de sensibilisation à la cybersécurité doit susciter l'intérêt de l'utilisateur, ce qui implique l'utilisation de supports, de graphismes et de contenus de formation en ligne appropriés. Choisissez donc la meilleure formation en ligne possible, couvrez les principales langues de votre organisation et laissez les utilisateurs déterminer eux-mêmes la langue dans laquelle ils se sentent le plus à l'aise pour consommer le contenu.

Gérer les risques et garantir la pertinence

Presque toutes les organisations sont confrontées à une forme de projet de transformation numérique. À mesure que l'on explore les possibilités de gains d'efficacité et de revenus, de nouveaux modèles métiers deviennent disponibles en raison de l'évolution des marchés et de l'adaptation de technologies comme le cloud, la gestion des données et les plateformes mobiles. Ces projets sont très médiatisés dans chaque organisation et bénéficient généralement de l'attention et du soutien du conseil d'administration et de l'équipe de direction.

La législation sur la protection des données, comme le règlement général sur la protection des données (RGPD), a placé le respect de la confidentialité des données personnelles dès la conception et la sécurité dès la conception au cœur des nouvelles initiatives numériques. Dans certains pays, les organisations sont tenues d'entreprendre une analyse d'impact pour évaluer l'incidence sur la protection des données d'un nouveau système, d'un nouveau processus ou d'un nouveau modèle métier. Les professionnels de la protection des données et de la sécurité des systèmes d'information ont un rôle très important à jouer pour s'assurer que les équipes chargées de la transformation numérique sont conscientes de cette exigence et que le nouveau système ou la nouvelle approche dispose de contrôles adéquats et de communications appropriées avec le personnel.

RAPPEL

Inclure les communications relatives à un projet de transformation numérique dans le cadre de votre projet annuel de sensibilisation à la cybersécurité augmentera sa pertinence pour l'entreprise et contribuera aux efforts visant à accroître le profil de la sécurité au sein de l'équipe dirigeante. En outre, en anticipant ces nouveaux projets numériques, les employés peuvent voir la sécurité des systèmes d'information comme un catalyseur plutôt que comme un élément bloquant qui suit

inévitablement l'arrivée tardive des contrôles de sécurité dans ce type d'initiative.

Lorsque les cadres supérieurs s'interrogent sur la validité d'un projet de transformation numérique, ils évaluent déjà les différents risques commerciaux ainsi que les avantages potentiels. Le défi consiste à aborder le projet sous l'angle des risques et à s'assurer que les risques liés à la sécurité et à la protection des données sont placés au même niveau que les risques financiers et autres risques commerciaux. Les projets de transformation numérique offrent des possibilités de sensibilisation à la cybersécurité qui viennent s'ajouter à une initiative d'entreprise beaucoup plus large.

DANS CE CHAPITRE

- Utiliser une communication efficace
- Combattre l'apathie
- S'appuyer sur le personnel de votre entreprise pour diffuser votre message
- Prendre en compte les relations avec des tiers

Chapitre 3

Changer la culture organisationnelle grâce à des campagnes de sensibilisation à la cybersécurité

Votre organisation peut être tentée de s'occuper de son programme de sensibilisation à la sécurité et d'envoyer des formations en ligne et des simulations d'attaques de phishing aux utilisateurs. Cependant, ces approches sont vouées à l'échec si elles ne tiennent pas compte de l'objectif principal, à savoir changer les comportements des employés par rapport au cyberrisque. Dès que vous commencez à envisager de modifier les comportements, vous entrez dans le domaine de la gestion du changement. Comme toutes les organisations le savent, les programmes de gestion du changement sont notoirement difficiles. Les meilleurs programmes de sensibilisation à la sécurité abordent la tâche de la même manière que les autres projets de changement organisationnel. Ils réunissent un groupe multidisciplinaire pour tirer parti des connaissances de l'organisation, notamment des experts de la gestion de projets, du marketing interne, des RH et de la sécurité informatique.

Le changement ne va pas de soi ; il demande du temps et une quantité importante de volonté et d'efforts. La direction ressentira

inévitablement un certain désespoir, se demandant si le projet de sensibilisation est même nécessaire et s'il prendra fin un jour.

Ce désagrément survient normalement lorsque la campagne de sensibilisation coïncide avec d'autres initiatives de communication d'entreprise. Il est courant que les utilisateurs se rebiffent dans ces circonstances. Au stade de la planification, l'organisation peut contrer ces tensions en réduisant le nombre et la fréquence des communications de sensibilisation pendant une période limitée. L'essentiel est de ne pas arrêter le programme. Si vous l'arrêtez, vous ne pourrez plus jamais le redémarrer.

Ce chapitre vous aide à assurer le succès de la campagne de sensibilisation en vous donnant des conseils sur la manière d'utiliser une communication efficace, de ne pas vous décourager lorsque vous rencontrez de l'apathie, de compter sur les personnes de votre organisation pour diffuser votre message et de faire appel à vos sous-traitants.

Communiquez de façon sérieuse

Votre campagne de sensibilisation doit être adaptée spécifiquement à votre organisation. Suivez ces quelques conseils pour vous assurer que votre campagne communique bien votre message :

- **Assurez-vous d'y intégrer visiblement votre logo afin de lui donner l'envergure nécessaire dans l'esprit de vos utilisateurs.** Votre personnel consomme beaucoup de contenus audiovisuels dans sa vie privée. Vous devez donc vous assurer que votre formation a l'apparence d'un contenu important et pertinent. Ceci étant dit, n'importe quelle formation de sensibilisation à la cybersécurité vaut mieux que rien du tout.
- **Adaptez votre message aux menaces auxquelles votre personnel est confronté au quotidien.** Évitez les formations fantoches qui ne serviront qu'à dire que vous avez un programme de sensibilisation.

  S'ils comprennent les risques et les conséquences personnelles et professionnelles, la grande majorité des membres de votre personnel réagiront positivement et changeront de comportement. Prenez le temps de bien définir votre message. Si ce n'est pas une compétence que vous ou votre équipe possédez, demandez l'aide de votre équipe marketing. Sinon, faites appel à une agence externe.

RAPPEL

CONSEIL

Votre population d'utilisateurs ne peut supporter qu'une quantité limitée de communications sur ce sujet. Commencez doucement et développez votre campagne sur 12 mois. Pensez-y, combien de cours de formation en ligne voudriez-vous suivre en un mois, même s'ils sont

courts ? Si vos employés n'ont pas reçu ce type de formation auparavant, publiez-en une par mois au cours des six premiers mois pour ne pas les lasser.

RAPPEL

En outre, avant d'augmenter le nombre de formations, demandez-vous combien de politiques de cybersécurité, d'attaques de phishing simulées et d'évaluations des risques vos utilisateurs peuvent supporter au cours des six premiers mois ? Tous ces éléments s'ajoutent les uns aux autres. Pour s'assurer que la campagne de sensibilisation ne se termine pas prématurément, discutez avec l'équipe de direction des moyens nécessaires pour pousser les utilisateurs à consulter ce contenu. L'expérience prouve qu'en règle générale, moins vous en faites, mieux c'est. Vous devez obtenir l'adhésion de votre personnel dans cette campagne.

De nombreuses campagnes de sécurité négligent d'expliquer aux utilisateurs pourquoi la sécurité est importante pour eux et pourquoi le système de management de la sécurité de l'information (SMSI) est en place pour atténuer les risques de cybermenaces. Assurez-vous de communiquer cette initiative globale aux utilisateurs pour leur permettre de comprendre que la cybersécurité est un élément essentiel du statu quo dans le monde numérique d'aujourd'hui.

Maintenir la dynamique face à l'apathie

Il est généralement simple d'obtenir le soutien de la direction pour sensibiliser votre public d'utilisateurs dans le cadre d'un projet de sensibilisation à la sécurité. Les cadres supérieurs ne sont que trop conscients des menaces qui pèsent sur l'organisation en termes d'amendes et d'atteinte à la réputation. Toutefois, il n'est pas rare qu'une campagne soit lancée, mais que l'inertie de l'entreprise la fasse échouer six mois plus tard et que les résultats soient médiocres. Souvent, les projets de sensibilisation ne parviennent pas à établir et à gérer un cycle de communication prévisible.

La plupart des employés et des cadres supérieurs doivent être informés dès le début que la campagne de sécurité s'inscrit dans une stratégie à long terme visant à améliorer les cyberdéfenses de l'organisation. Il est essentiel que les gens ne s'attendent pas à une initiative ponctuelle. Par conséquent, vous devez établir des communications reproductibles afin que les utilisateurs connaissent l'importance de la campagne grâce à des notifications régulières des messages clés, des formations et des évaluations. En outre, intégrez une boucle de rétroaction dans vos communications afin que la direction reçoive en temps utile les avis du personnel. La direction peut utiliser ce retour d'information pour améliorer l'initiative de sensibilisation globale au fil du temps et déterminer la cadence de vos campagnes de sensibilisation en cours.

Il est difficile pour la direction d'essayer de maintenir la sensibilisation du personnel en tête des préoccupations tout au long de l'année, en raison de la fréquence permanente des cybermenaces actives. La cybersécurité implique une lutte permanente contre les attaques. Il est donc pratiquement impossible de trouver le temps de définir un message pour le programme de sensibilisation.

RIEN DE TEL QU'UNE VIOLATION POUR CATALYSER LE CHANGEMENT

Personne ne souhaite faire l'objet d'une cyberattaque ciblée qui aboutit à une violation de données. C'est un événement qui ne fait pas bonne figure sur votre C.V. si vous êtes un professionnel de la sécurité. Cela dit, l'expérience de la gestion d'un cyberincident majeur est un événement important pour tout cadre impliqué dans la gestion de la sécurité de l'information.

La différence entre une organisation qui a subi une violation de données (ou un incident évité de justesse) et une organisation expérimentée est que cette dernière dispose d'un plan de réponse aux incidents prêt à être mis en œuvre, alors que l'organisation non initiée adopte souvent une approche attentiste. Si des gestionnaires chevronnés sont employés, une planification adéquate de l'incident a probablement eu lieu.

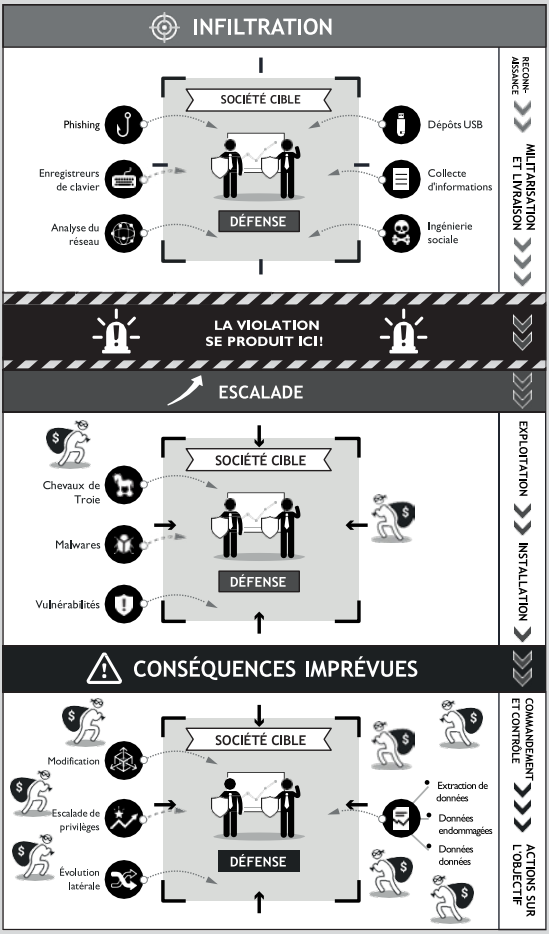
Voici la seule bonne chose qui peut découler d'une violation ou d'un quasi-accident de données : la direction ne peut plus se permettre de prendre ses désirs pour des réalités ou de prétendre à un déni plausible. Elle doit s'impliquer.

Bien que chacun soit conscient des menaces et partage la conviction que les risques que son organisation soit victime d'une cyberattaque sont élevés, l'investissement dans la sensibilisation à la cybersécurité reste impopulaire et les cadres supérieurs sont tentés de fournir une solution minimale. Le secteur de la sécurité doit assumer une part de responsabilité dans la promotion de la dernière technologie périmétrique comme étant la panacée pour tous les problèmes de sécurité, en oubliant toujours que le moyen le plus facile de contourner les défenses est de passer par la personne qui se trouve derrière le pare-feu.

En tant que groupe, les professionnels de la protection des données, de la conformité et de la sécurité de l'information ne devraient pas essayer d'effrayer les cadres dirigeants en les menaçant d'amendes. Mettez plutôt en avant les avantages commerciaux qu'il y a à se démarquer des organisations moins conformes ou moins sûres. La valeur concurrentielle du

marché qui en résulte doit être promue en interne comme la raison de l'investissement, en particulier dans le domaine du changement de culture du personnel.

La direction a une occasion unique, peu de temps après une violation ou un quasi-accident, et avant que la peur n'ait été rationalisée, de lier l'équipe de direction à la mission de sécurité de l'information et d'obtenir le soutien nécessaire. Cet investissement porte généralement sur les personnes et les solutions, mais c'est le temps consacré par ce groupe qui s'avère finalement le plus précieux. La figure ci-dessous présente une chronologie typique d'une violation de données.



Recruter des champions de la cybersécurité

Il est extrêmement important de veiller à ce que les membres de l'organisation ne considèrent pas le service informatique comme le seul responsable de la sensibilisation à la sécurité de l'information et à la protection des données. Au lieu de cela, l'organisation doit accepter que sa sécurité numérique relève de la responsabilité de *chacun*.

Une campagne de sensibilisation à la cybersécurité a besoin d'autant d'alliés que possible. Votre organisation compte déjà des personnes actives dans ce domaine. Elles signalent les incidents, simulent des attaques de phishing et fournissent des informations en retour. Elles comprennent les dommages que le cyberrisque fait subir à l'organisation. Faites volontiers appel à ces utilisateurs. Appuyez-vous sur eux dans votre organisation pour vous assurer que chacun comprend sa responsabilité. Ces *champions* savent communiquer, ont de l'entregent et sont doués pour les relations humaines. Ils représentent un atout précieux pour votre campagne. Demandez à vos collègues d'autres services de vous aider à identifier des membres potentiels du personnel.

CONSEIL

En d'autres termes, la direction doit créer un programme d'ambassadeurs qui s'appuie sur ces champions, c'est-à-dire les personnes les plus ambitieuses et les plus intéressées de votre organisation. Votre programme d'ambassadeurs doit être soutenu par l'ensemble de l'organisation et recevoir l'aval de la direction. Vous pouvez utiliser ce soutien de la direction pour lancer officiellement votre programme d'ambassadeurs afin de reconnaître leur contribution, ce qui est toujours très apprécié.

Vous avez peut-être déjà des personnes qui sont en première ligne de vos opérations de sécurité de l'information et de protection des données personnelles. Ces personnes peuvent avoir été identifiées comme propriétaires d'actifs informationnels dans une perspective ISO 27001, ou comme propriétaires d'une activité de traitement des données. Elles peuvent déjà avoir suivi une formation sur la protection des données ou la sécurité de l'information.

Essayez de reconnaître chaque réussite. Développez votre campagne en misant sur la positivité. Célébrez la recertification réussie de la norme ISO 27001 ainsi que toute autre réalisation dans ce domaine.

CONSEIL

Si possible, votre programme de champions de la cybersécurité doit disposer d'un canal de communication distinct sur un outil de messagerie interne, tel que Microsoft Teams ou Slack, afin d'assurer un flux régulier de commentaires sur l'état de votre projet de cybersensibilisation. Utilisez au moins ce canal de communication pour informer les

champions de tout incident de violation de données et de tout incident évité de justesse.

Le lancement d'un programme de champions de la cybersécurité est un élément satisfaisant d'une campagne de sensibilisation réussie. Il permet d'obtenir un réel soutien à votre initiative de changement dans toute l'organisation. Il fait également office de système d'alerte précoce lorsque la campagne commence à s'essouffler ou a raté son but.

Ces champions peuvent montrer, par leurs actions et leur plaidoyer, que les programmes de sensibilisation à la cybersécurité exigent de l'ensemble de l'organisation qu'elle intègre ces meilleures pratiques dans son approche habituelle.

Étendre les initiatives de sensibilisation à la cybersécurité aux relations avec les tiers

La gestion des risques liés aux fournisseurs et aux tiers a souvent été difficile pour la plupart des organisations au cours des 20 dernières années. Au fur et à mesure que les organisations se sont transformées et ont évolué, elles ont externalisé des spécialités et des activités non essentielles à des partenaires de confiance. Dans certaines organisations modernes, jusqu'à 50 % du personnel peut ne pas être employé à temps plein. Le recours à la sous-traitance permet d'obtenir une organisation évolutive et agile. Cependant, cela a des répercussions sur le déploiement d'une campagne de sensibilisation à la sécurité. Les sections suivantes traitent des sous-traitants à inclure dans votre plan de sensibilisation à la sécurité et des défis technologiques qu'ils peuvent rencontrer.

Savoir qui inclure

Le niveau d'intégration des sous-traitants dans votre organisation détermine dans quelle mesure ils doivent participer à votre programme de sensibilisation. Les relations avec les tiers qui sont en contact avec vos actifs informationnels, vos activités de traitement des données et votre réseau doivent au moins faire partie du processus de planification de votre campagne de sensibilisation. Le cas échéant, votre organisation doit identifier les relations avec les tiers particulièrement difficiles ou à haut risque, puis déterminer la communication nécessaire pour chaque segment. Au minimum, toutes les personnes qui accèdent à vos systèmes internes doivent signer votre politique d'utilisation acceptable. Vous élaborerez, à partir de là, des exigences supplémentaires en termes de politiques et de formation.

Par exemple, les conseillers professionnels et les professionnels techniques de tiers de confiance peuvent avoir accès à des données confidentielles et avoir besoin d'accéder à des systèmes clés, en particulier les banques de données financières, de ressources humaines et d'entreprise. Veillez à ce qu'une formation sur les obligations nécessaires en matière d'accès à vos actifs numériques soit dispensée à ces types de personnel tiers.

Comme pour les employés permanents, la direction doit segmenter les sous-traitants tiers en fonction du risque qu'ils représentent pour l'organisation. Plus le risque est élevé, plus les contrôles doivent être nombreux. Veillez à convenir de ces contrôles, qu'il s'agisse d'attestation de formation ou de politique, avec le sous-traitant au moment de la signature du contrat. Ces conditions préalables doivent faire partie de vos conditions générales et doivent être un élément essentiel des relations avec les fournisseurs qui ont accès à vos systèmes informatiques.

Prise en compte des défis technologiques potentiels

Parfois, votre organisation peut avoir à surmonter de véritables défis technologiques en faisant participer des tiers à votre initiative de sensibilisation. Par exemple, des tiers éloignés peuvent ne pas être en mesure d'accéder à un système de gestion de l'apprentissage (LMS) sur site afin de suivre la formation en ligne nécessaire. Il en va de même lorsqu'il s'agit d'adhérer aux politiques clés qui régissent la relation entre l'organisation, le fournisseur et la personne qui fournit effectivement le service. Par le passé, les organisations ont souvent négligé d'impliquer des tiers dans ce type d'initiatives de sécurité. Or, la gestion des fournisseurs et le cyberrisque associé aux interactions avec les tiers sont devenus une source de préoccupation pour les responsables informatiques et un domaine de focalisation pour les lois internationales sur la protection des données personnelles.

Sensibilisation progressive des tiers à la cybersécurité

Une approche progressive d'intégration de tiers dans vos campagnes de sensibilisation à la cybersécurité est la méthode la plus judicieuse pour faire mûrir votre relation avec vos fournisseurs. Trouvez d'abord un moyen de gérer vos principales politiques et un moyen fiable d'obtenir une attestation ; dans l'idéal, une solution de gestion électronique des politiques pouvant automatiser ce processus. Le papier est un support déconseillé dans ce cas, surtout lorsque vous essayez de remettre les documents signés dans un dossier central. Déterminez les principaux

risques qu'un sous-traitant peut représenter, puis proposez une formation appropriée, idéalement par le biais d'un LMS basé sur le cloud auquel le sous-traitant peut accéder à distance ou par le biais de vos systèmes avant son arrivée sur le site.

ATTENTION

Vous pouvez également retrouver chez vos fournisseurs tous les mauvais comportements de vos employés. Par exemple, un sous-traitant est tout aussi susceptible de faciliter le talonnage qu'un membre de votre propre personnel. Pourtant, votre campagne de sensibilisation interne couvre la sécurité physique via des politiques et de la formation. Assurez-vous que vos sous-traitants sont également formés sur ces sujets.

Étendez la couverture de votre campagne de sensibilisation pour évaluer le niveau de formation à la sensibilisation et de gestion de la politique des employés qu'un fournisseur adopte dans son propre environnement. Cette évaluation fait partie de la diligence raisonnable de votre fournisseur ; et fait partie intégrante du processus d'intégration des fournisseurs de votre organisation. De nombreuses organisations envoient aux fournisseurs une évaluation des risques avant la signature du contrat. Dans le cadre de cette procédure, évaluez le niveau de sensibilisation à la cybersécurité des fournisseurs en leur posant des questions sur la sécurité générale de l'information, notamment sur leur pare-feu et leurs défenses antivirus. Un fournisseur qui ne peut pas fournir de preuves de l'existence d'une politique ou d'un régime de formation en matière de sécurité de l'information aura du mal à satisfaire aux exigences de votre campagne de sensibilisation.

DANS CE CHAPITRE

- Comprendre l'importance des politiques dans une campagne de sensibilisation à la sécurité
- Faciliter l'identification des risques
- Former le personnel vétéran et les nouveaux employés aux politiques
- Considérer les avantages d'une architecture technologique centralisée

Chapitre 4
Intégrer la gestion des politiques dans votre programme de sensibilisation à la sécurité

Une politique est un ensemble d'idées ou un plan de ce qu'il faut faire dans des situations particulières qu'un groupe de personnes, une entreprise, une organisation, un gouvernement ou un parti politique ont officiellement accepté.

Les politiques planifient la marche à suivre dans des situations particulières. Votre campagne de sensibilisation à la sécurité nécessite des politiques claires mises en œuvre par la direction pour le personnel. Les politiques doivent être communiquées au personnel, car si vous ne leur indiquez pas la marche à suivre dans certaines situations, comment pouvez-vous compter sur eux pour agir de la bonne manière ?

Ce chapitre insiste sur l'importance du rôle des politiques pour renforcer la campagne de sensibilisation à la sécurité de votre organisation.

Comprendre le rôle des politiques dans une campagne

On peut comparer les politiques d'une organisation à l'ensemble des lois qui permettent à un gouvernement de gérer un pays. Elles constituent l'épine dorsale de la réponse de l'organisation aux menaces de cybersécurité (politiques en matière de médias sociaux, de mots de passe, de réseaux, etc.) et de la protection réglementaire (politique d'utilisation acceptable, politiques de confidentialité, codes de conduite, etc.) Elles sont incontournables dans un processus de communication avec le personnel fondé sur les meilleures pratiques. Les activités de formation et les politiques sont plus efficaces lorsqu'elles sont alignées. Si elles sont traitées séparément, elles s'accumulent, augmentent les communications aux employés et finissent par provoquer la lassitude des utilisateurs.

RAPPEL

Considérez les politiques comme les lois de votre organisation. Aucun gouvernement ne permettrait que ses lois soient inventées à la volée ni que l'exécutif n'exerce pas un contrôle strict sur l'approbation des lois, des politiques et des communications. Or, dans de nombreuses organisations, la gestion des politiques pour la fonction de sécurité de l'information et de protection des données est souvent ignorée par la direction.

Lors de l'élaboration d'un programme de sensibilisation, assurez-vous d'examiner tous les éléments clés qui doivent être communiqués au personnel : politiques, apprentissage en ligne, évaluations des risques, les attaques de phishing simulées, etc. L'enjeu est de trouver le bon équilibre entre ces éléments pour atteindre les objectifs de la stratégie de sensibilisation.

RAPPEL

Comme c'est le cas de toute initiative de sensibilisation, les personnes jouent un rôle essentiel. Encouragez l'adhésion du personnel aux politiques pour qu'il accepte qu'on lui dicte la marche à suivre dans des situations particulières. Cette adhésion crée chez les membres de votre personnel une responsabilité personnelle et contribue grandement à un changement de comportement.

Les politiques sont des normes organisationnelles documentées auxquelles les personnes sont tenues de se conformer. Il est essentiel que le personnel puisse accéder facilement aux politiques via un portail central faisant office de source infaillible pour l'organisation. Ce portail doit être inviolable afin de fournir à l'organisation une « force probante » si les politiques sont contestées devant un tribunal.

En outre, les politiques doivent faire l'objet d'un contrôle strict des révisions afin que les modifications et les changements apportés aux politiques au fil du temps soient enregistrés et puissent être examinés dans une piste d'audit. Les politiques changent constamment pour répondre aux besoins de l'organisation. Par conséquent, le processus de gestion des changements de politique au sein de l'organisation doit être revu pour s'assurer que l'approche de la politique est adaptée à l'objectif. L'essentiel est que les politiques soient communiquées aux employés d'une manière qui favorise la cyberconformité et la conformité réglementaire. La méthode optimale passe par la création d'un plan de communication des politiques, comme le montre la figure 4-1.

FIGURE 4-1 : Les éléments essentiels d'un plan de communication (Source : OCEG et GRC 20/20).

Gestion des politiques : former votre personnel à l'identification des risques

Une organisation élabore des politiques pour atténuer les risques identifiés dans les domaines de la conformité ou de la sécurité de l'information. Les politiques sont élaborées lorsque les risques sont suffisamment importants pour nécessiter une politique écrite formelle. En outre, une politique détaillera les contrôles nécessaires pour gérer le risque. Cependant, la politique n'est qu'une étape dans le processus de sensibilisation. Le personnel doit également être formé au contenu de la politique.

La formation associée à la politique peut adopter une vue plus abrégée du contenu de la politique. Laissez au document de politique le soin de couvrir la multitude d'éventualités entourant l'élimination des risques.

La formation doit couvrir les principaux points que les employés sont censés connaître et ne pas être une répétition mot à mot du document.

RAPPEL

Les politiques jouent un rôle important dans le changement de la culture organisationnelle. Il ne fait aucun doute que lorsqu'un membre du personnel est appelé à faire état d'une politique, que ce soit par voie électronique ou en signant un document papier, il confirme qu'il est conscient de la portée de ses actions. Les politiques contribuent à accroître l'importance de la cybersécurité sur le lieu de travail. Elles permettent d'aligner la responsabilité personnelle sur les risques, les procédures et les règlements de l'organisation.

Les sections suivantes fournissent plus de détails sur la formation du personnel actuel ainsi que des nouvelles recrues.

Former le personnel aux politiques

Bien que la politique contienne des orientations pour les personnes, le personnel a souvent besoin d'une formation sur la manière de la mettre en œuvre. Le risque que la politique vise à traiter, et le niveau de risque qui a été évalué sont directement liés à la quantité d'instructions dont l'utilisateur aura besoin. Plus les risques sont élevés, plus les politiques nécessiteront des niveaux de formation élevés pour garantir la compréhension et l'application du contrôle correspondant. En outre, vous devrez éventuellement adopter une approche hybride associant politiques, contenus d'apprentissage en ligne et formations en présentiel pour les risques plus élevés afin de garantir une adoption et une compréhension maximales. (Le chapitre 5 traite plus en détail cette approche hybride.)

Il existe une corrélation claire entre le temps et l'énergie consacrés à la politique, à la formation et à la sensibilisation et leur impact réel sur l'organisation. Les activités de mise en conformité qui ont une grande visibilité et le soutien des dirigeants ont tendance à être mieux perçues par les employés, ce qui se traduit par une plus grande adoption des politiques, l'achèvement des formations et des tests connexes.

Reportez-vous à la figure 4-2 pour connaître les questions importantes à poser lors de la formation de votre personnel aux nouvelles politiques.

Identifier pourquoi les politiques sont importantes pour la sensibilisation du nouveau personnel

Dans de nombreuses organisations, l'approche adoptée à l'égard des nouveaux employés leur impose de signer des politiques et de suivre des formations en ligne jusqu'à trois heures par jour pendant la première semaine suivant le recrutement. Ce n'est pas une utilisation efficace du temps du nouvel employé. Ce type d'apprentissage revient à boire dans un tuyau d'arrosage.

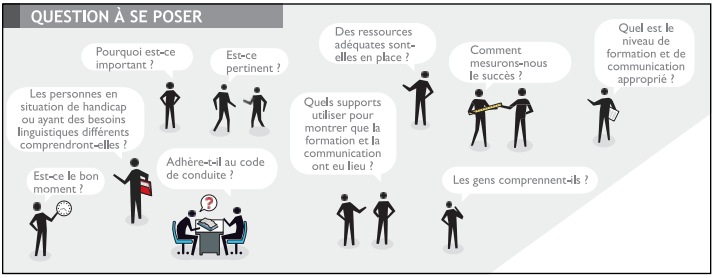


FIGURE 4-2 : Questions à poser (Source : OCEG et GRC 20/20).

Toutes les organisations ont du mal à gérer les nouveaux employés au cours des premières semaines d'embauche, alors qu'ils sont en phase d'apprentissage. Il convient d'élaborer un programme d'initiation adapté à leurs besoins. Imaginez avoir à suivre deux ou trois heures de formation par jour. Cela risque de devenir pénible. Le problème avec les nouveaux employés est qu'ils ont une quantité de choses à apprendre. Lorsque vous les formez à la cybersécurité, tenez compte de leurs capacités d'attention et d'assimilation.

RAPPEL

Planifiez de manière réfléchie les politiques importantes pour les nouveaux employés ainsi que l'apprentissage en ligne correspondant. Fixez des limites à la quantité de formation en ligne que le nouvel employé doit suivre au cours du premier mois. Dans l'idéal, visez un maximum de trois heures par semaine au cours du premier mois. Ce laps de temps permettra au nouvel employé d'assimiler les politiques clés et de suivre les éléments de formation en ligne nécessaires pour apprendre l'approche organisationnelle, mais sans se lasser. Après le premier mois, réduisez le nombre de politiques et de formations en ligne pour permettre à l'employé de devenir productif dans son nouveau rôle.

Reconnaître l'importance d'une architecture technologique centralisée pour vos politiques

Dans une organisation moderne, la gestion efficace des politiques et l'apprentissage en ligne sont devenus trop compliqués pour être gérés manuellement par des personnes. Un système centralisé de gestion des politiques peut permettre de répondre aux demandes en constante évolution de l'organisation, des exigences réglementaires et de l'environnement commercial.

Il est difficile de gérer le cycle de vie des politiques sur des feuilles de calcul et des systèmes de partage de fichiers. Cela démontre un manque de maturité globale de la conformité au sein d'une organisation et une approche ad hoc de la gestion de la sécurité et de la conformité.

Les sections suivantes expliquent comment un système centralisé de gestion des politiques peut aider votre organisation et qui, dans votre organisation, peut utiliser ce système.

Identifier les avantages d'un système centralisé

Voici quelques-uns des principaux avantages de l'utilisation d'un système centralisé :

- **Garantit une participation à 100 %.** S'assurer que chacun reçoit, comprend et atteste de la politique est un avantage essentiel d'un système centralisé de gestion des politiques.
- **Permet de rendre la formation et les politiques accessibles en un seul endroit.** La possibilité de lier une formation pertinente à vos politiques est importante pour tous les employés.
- **Réduit la charge de la direction.** L'automatisation des politiques peut éviter la nécessité d'une surveillance importante de la part de la direction en automatisant la mise en application. C'est la technologie, et non la direction, qui notifie et rappelle aux utilisateurs qu'ils doivent remplir leurs obligations en matière de politique et de formation.
- **Toutes les politiques et formations sont regroupées en un seul endroit.** Le principal avantage d'une solution technologique est le fait de disposer d'une source infaillible pour vos activités de conformité, notamment en ce qui concerne les politiques, la formation et l'interaction avec vos employés.

La figure 4-3 démontre davantage comment votre organisation peut tirer parti d'une technologie centralisée.

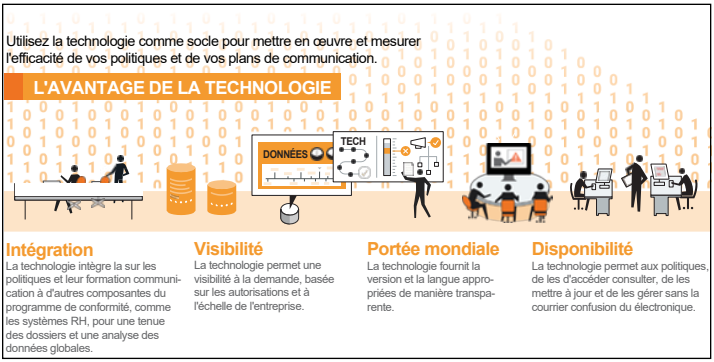


FIGURE 4-3 : Les avantages de la technologie (Source : OCEG et GRC 20/20).

Comprendre qui utilise ce système

Trois groupes principaux utilisent ce type de système de gestion des politiques tout-en-un :

- **Les administrateurs qui mettent en place le système et diffusent les politiques et les formations :** ils disposent de leur propre interface d'administration pour créer, cibler, publier et gérer les politiques organisationnelles.
- **Les utilisateurs qui suivent la formation et assimilent les politiques :** ils peuvent s'acquitter de leurs obligations, à savoir signer des politiques, suivre des formations, autogérer leur interaction avec le contenu et y accéder s'ils ont besoin de rafraîchir leurs connaissances.
- **La vue de gestion ou de supervision du système :** ici, la direction peut examiner le système pour s'assurer que les employés suivent les campagnes de communication nécessaires à la conformité. Les auditeurs et les régulateurs peuvent accéder au système pour vérifier que l'organisation a respecté son devoir de diligence et de surveillance.

DANS CE CHAPITRE

- Assurer le soutien de la direction
- Élaborer un plan de campagne
- Créer une base de référence pour votre stratégie
- Savoir à quoi ressemble votre réussite
- Envisager une approche hybride

Chapitre 5
Élaborer une stratégie de meilleures pratiques en matière de cybersensibilisation

Pour que votre campagne de cybersensibilisation soit un succès, votre organisation a besoin d'un plan d'action clair. Ce chapitre vous donne des conseils pour élaborer ce plan, tout en vous assurant du soutien des dirigeants de votre organisation. Une fois votre plan mis en place, vous devez être en mesure de mesurer son efficacité. Si nécessaire, votre organisation doit envisager une approche hybride.

Assurer le soutien de la direction

La réussite d'un programme de sensibilisation dépend souvent du soutien apporté par la direction de l'organisation. Sans ce soutien de la direction, il est difficile d'obtenir un financement et des ressources adéquats et un projet de sensibilisation à la sécurité est limité dans ce qu'il peut accomplir.

Les programmes de cybersensibilisation visent à modifier les comportements du personnel, ce qui implique un élément de psychologie. Si vous avez le soutien de l'équipe dirigeante, vous pouvez démanteler les obstacles et les décisions peuvent être prises rapidement. Il est important de savoir dès le départ quel est le ton donné par la direction. Par exemple, quelle est l'approche face à un mauvais comportement en matière de cybersécurité ? Une approche « allégée » ou, au contraire, zéro tolérance ? À combien d'exercices de simulations de phishing un employé peut-il échouer avant que des mesures disciplinaires soient prises ? Si le ton n'est pas donné, chaque manager et chaque directeur peuvent potentiellement interpréter la mise en œuvre de la campagne de sensibilisation.

La modification des comportements du personnel fait intervenir un élément de psychologie. Par exemple, les collaborateurs aiment être dirigés par leurs leaders. Lancer une campagne de sensibilisation avec un message venant du sommet est donc très efficace. Cela peut prendre la forme d'un e-mail ou d'une simple vidéo.

CONSEIL

Lorsque vous préparez votre campagne de sensibilisation, assurez-vous d'avoir le soutien total de votre équipe dirigeante. Il peut être judicieux de prévoir quelques heures de formation spécifique pour la direction. Cette formation sur mesure, en face à face, doit être complétée par une formation en ligne pour les cadres.

Élaborer un plan de campagne

L'adoption d'un processus de planification fondé sur l'atténuation des risques constitue le meilleur moyen d'élaborer une campagne de cybersensibilisation adaptée aux objectifs. En élaborant votre plan, assurez-vous qu'il est adapté au calendrier (généralement 12 mois) et qu'il inclut les principaux risques auxquels l'organisation est confrontée à ce moment précis. Soyez prêt à réévaluer vos risques, car ils changent et évoluent avec le temps.

ATTENTION

Les organisations font souvent appel à un professionnel de la sécurité de l'information pour organiser la planification d'un plan de communication de sensibilisation. Il importe de soutenir cette fonction par une expertise en communication d'entreprise. Cela dit, les professionnels de

la sécurité de l'information et de la confidentialité des données sont essentiels au succès d'une campagne de sensibilisation à la cybersécurité. Leurs connaissances peuvent guider et éclairer le programme. Le risque est au cœur de toute campagne de sensibilisation. Ces intervenants peuvent identifier et hiérarchiser les différents types de risques auxquels il faut remédier.

RAPPEL

Toutefois, un collaborateur issu de la gestion de projets ou de la communication d'entreprise devra peut-être intégrer cette équipe pour s'assurer que le message est partagé de manière efficace. Cette équipe a besoin de plusieurs compétences pour élaborer une campagne de sensibilisation réussie.

Vous pouvez être tenté d'envoyer quelques e-mails de phishing simulés en croyant que cela suffira à remplir l'exigence de sensibilisation à la cybersécurité. Il ne fait aucun doute que cette méthode met en évidence le risque d'ingénierie sociale pour le personnel. Toutefois, le programme de sensibilisation doit prendre en compte l'ensemble des menaces qui pèsent sur l'organisation. Un programme de sensibilisation doit également enregistrer les exercices de remédiation et documenter les activités de suivi. Ces dossiers sont essentiels pour remplir les exigences de conformité et de gouvernance.

La création d'un cahier des charges (voir la figure 5-1) ou d'une campagne d'activités pour l'année à venir est essentielle à la réussite d'un projet de cybersensibilisation. Ce type d'exercice oblige à identifier les principaux risques. L'organisation doit déterminer la capacité des personnes à assimiler les messages de conformité et de sécurité. La direction doit décider du type et du nombre de communications qui peuvent être diffusées par semaine, par mois et finalement par an. L'enjeu est de trouver un équilibre entre le risque et la lassitude des utilisateurs. L'équipe qui met en œuvre cette campagne doit éviter d'être trop ambitieuse dans l'exécution du programme de sécurité.

RAPPEL

Il faut beaucoup de temps pour changer les comportements et améliorer la résilience du personnel face aux menaces de cybersécurité.

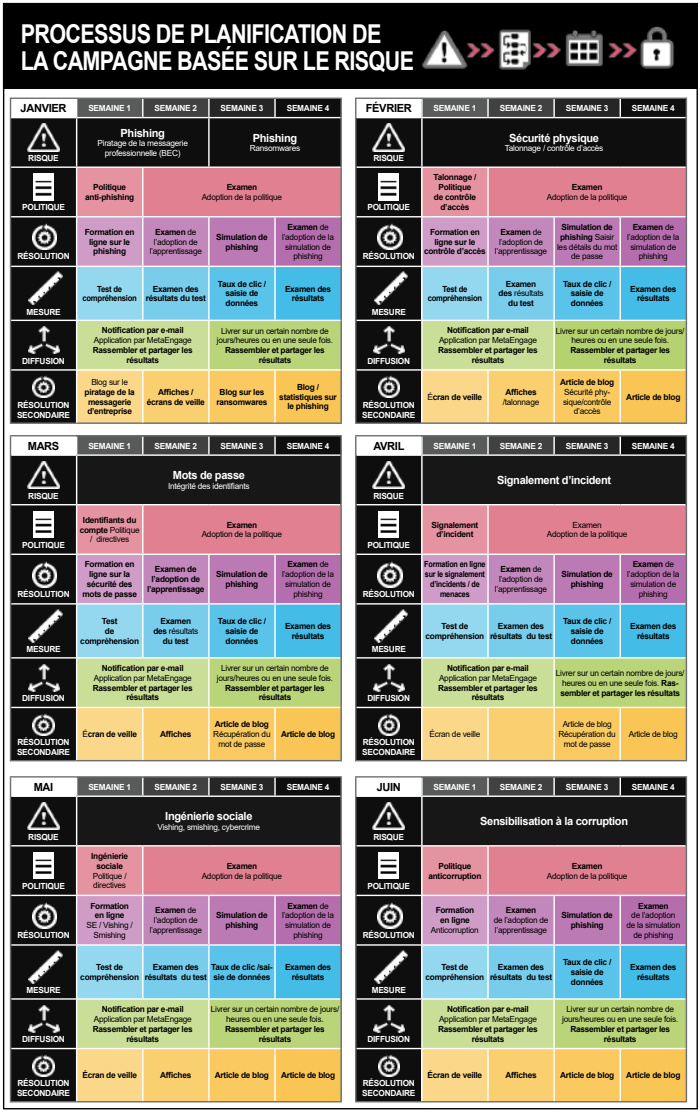


FIGURE 5-1 : Un planning de sensibilisation à la sécurité sur 12 mois.

Établir une base de référence

Les indicateurs clés de performance (ICP) indiquent si un projet est réussi ou non. Vous devez gérer votre sensibilisation à la sécurité de l'information de la même manière. Mettez en évidence les ICP que vous avez identifiés pour déterminer une base de référence. Vous pouvez ensuite utiliser ces données pour mesurer les progrès accomplis.

Vos programmes de sensibilisation doivent être basés sur les risques actuels auxquels votre organisation est confrontée. Comme point de départ, les incidents récents qui ont été enregistrés constituent un excellent guide pour les questions que le programme aborde et les risques qui doivent être corrigés.

CONSEIL

La meilleure façon de savoir dans quelle mesure vos utilisateurs connaissent ces risques est de les interroger au moyen d'un questionnaire ou d'une enquête en ligne. Basez les questions de l'enquête sur les risques auxquels l'entreprise est confrontée. Faites en sorte que l'enquête soit aussi courte et concise que possible.

Les résultats de cette enquête influenceront ensuite tout programme de formation ultérieur. Par exemple, si l'enquête met en évidence des lacunes dans les connaissances en matière de sécurité physique, vous devrez alors mettre en place une formation ou un communiqué de politique pour combler ces lacunes. Nous recommandons à votre organisation de s'attaquer à un risque clé chaque mois. L'enquête doit également vérifier les connaissances de votre personnel sur un minimum de 12 questions/risques.

RAPPEL

Un autre moyen rapide d'établir une base de référence est de simuler une attaque de phishing pour les employés. Vous pourrez ainsi déterminer le degré de sensibilité de l'entreprise aux e-mails frauduleux de phishing et connaître ainsi, en temps réel, quel pourcentage du personnel aurait été victime d'une attaque réelle. Il vous sera également possible d'identifier les utilisateurs plus risqués qui ont soumis leurs informations d'identification après avoir reçu ces e-mails.

Les politiques font partie intégrante de la sensibilisation du personnel à la sécurité. Dès le départ, lancez un exercice pour identifier les politiques essentielles que le personnel est tenu de respecter. N'oubliez pas qu'une politique ne doit exister que si elle est liée à un risque. Par conséquent, chacun de vos risques clés doit faire l'objet d'une politique organisationnelle. Déterminez bien quand vos politiques ont été révisées pour la dernière fois et si elles sont toujours adaptées à leur objectif.

ATTENTION

Veillez à éviter une révision massive de la politique de l'organisation, car cela a tendance à ralentir les campagnes de sensibilisation. La meilleure pratique consiste à réviser la politique pertinente au moins un mois avant que le risque ne figure dans votre calendrier de sensibilisation.

Définir et mesurer votre réussite

Après avoir convenu d'une base de référence et l'avoir documentée, il est important de suivre vos ICP chaque mois afin de mesurer le succès du plan de sensibilisation. Les domaines à examiner sont les suivants :

- Pourcentage d'utilisateurs adhérant aux principales politiques
- Pourcentage d'utilisateurs qui cliquent sur une attaque de phishing simulée
- Nombre d'évaluations des risques liés aux fournisseurs
- Nombre d'activités de traitement des données
- Nombre d'enquêtes menées auprès du personnel
- Nombre d'incidents de sécurité
- Nombre d'attaques par phishing signalées par le personnel

Les trois derniers paramètres sont importants, car ils concernent la sensibilisation du personnel aux principaux défis de l'organisation en matière de sécurité. ***Remarque :*** le nombre d'incidents de sécurité signalés peut augmenter à mesure que le personnel est sensibilisé aux différents risques.

Ces paramètres constituent la base du rapport soumis au comité directeur de la gouvernance de l'information et contribueront à l'informer sur les mesures correctives pour les risques et l'avancement de la campagne de sensibilisation.

Adopter une approche hybride en matière de sensibilisation

Les bonnes campagnes de marketing utilisent de nombreuses méthodes différentes pour attirer l'attention des clients sur leur produit ou service. Elles combinent plusieurs canaux numériques, e-mails et médias sociaux, ainsi que des méthodes traditionnelles comme les promotions et les cadeaux en magasin. À l'instar des campagnes de marketing, votre programme de sensibilisation à la sécurité doit donc utiliser une approche hybride pour attirer et retenir l'attention de vos utilisateurs.

Une fois que vous avez retenu leur attention, vous devez à l'étape suivante obtenir un changement de comportement.

Les sections suivantes expliquent comment vous pouvez utiliser le partage d'expériences et décrivent d'autres moyens de communiquer efficacement votre message.

Intégrer le partage d'expériences dans votre programme

Il n'existe pas de solution universelle en matière de marketing ou de sensibilisation à la sécurité. Dans le domaine de la communication organisationnelle, différents acteurs internes se battent pour attirer l'attention des collaborateurs. Un bon programme de sensibilisation prend en compte cet état de fait. Cela signifie que vous devez adopter de multiples canaux de communication pour attirer l'attention de votre public, y compris les supports physiques ou numériques et le partage d'expériences.

RAPPEL

Les êtres humains ont une tradition orale. Exploitez cette tradition et racontez une histoire, ou utilisez une thématique à laquelle les personnes puissent s'identifier afin de faire passer votre message. Exemple de thématique : vos employés sont des agents gouvernementaux essayant de déjouer des machinations criminelles. Pensez à James Bond ou à Wonder Woman !

Innover dans vos communications

Les méthodes physiques de communication avec le personnel emploient diverses approches inventives. Voici quelques moyens de communiquer avec votre organisation au sujet de la campagne :

- **Affiches :** moyen le plus économique et le plus efficace, une campagne d'affichage renforce vos messages et thèmes clés. Vous pouvez utiliser tous les types d'affiches, y compris les panneaux numériques à la réception et les petites affiches dans les ascenseurs. Veillez à aligner vos affiches sur le risque dont vous faites la promotion et changez les affiches toutes les quatre à six semaines, afin que les gens ne s'habituent pas au message.
- **Méthodes numériques :** les méthodes numériques sont l'approche la plus courante pour communiquer et résoudre le risque associé à un manque de formation du personnel. Certaines organisations disposent de systèmes autonomes de formation en ligne sur la simulation d'une attaque par phishing ou la gestion des politiques ou la cybersécurité, qui permettent de diffuser des messages clés aux employés.

AUTOMATISER VOTRE CAMPAGNE

Automatisez l'ensemble de votre campagne de sensibilisation à la sécurité sur 12 mois et gérez la diffusion appropriée des principaux éléments au bon public et au bon moment. Ces éléments doivent combiner formations en ligne adaptées, politiques essentielles, articles de blogs pertinents, e-mails de phishing simulés, évaluations des risques et enquêtes.

Une approche automatisée de la sensibilisation à la sécurité permet d'enregistrer les informations d'audit à l'appui d'une éventuelle défense réglementaire pouvant être requise en cas de violation ou d'audit.

DANS CE CHAPITRE

- Donner le ton depuis le sommet
- Impliquer votre public
- Se préparer à une violation de données
- Passer en revue vos initiatives de sensibilisation

Chapitre 6
Dix bonnes pratiques en matière de sensibilisation à la cybersécurité

Voici dix bonnes pratiques conseillées pour vous aider à créer la campagne de sensibilisation à la cybersécurité la plus efficace qui soit pour votre organisation.

Commencez par le leadership du PDG

La cybersécurité reçoit enfin l'attention qu'elle mérite dans les conseils d'administration. Le nombre de violations de données très médiatisées ne cessant d'augmenter, l'accent est mis sur la gestion des cyberrisques afin de réduire les risques d'attaque.

La cybersécurité est la responsabilité de tous, mais les organisations résilientes ont besoin d'un leadership fort de la part du PDG. Un PDG engagé mettra en œuvre les mesures de sécurité correctes nécessaires pour protéger les actifs numériques, les employés, les clients et la réputation de l'organisation. Si le PDG prend la cybersécurité au sérieux, cela

se répercutera dans toute l'organisation et contribuera à instaurer une culture de sensibilisation accrue à la cybersécurité.

Reportez-vous au chapitre 5 pour découvrir comment obtenir le soutien de vos dirigeants.

Apprenez à connaître les tolérances de votre organisation

Pour créer un programme efficace de sensibilisation à la sécurité, votre organisation doit évaluer le paysage des menaces et identifier vos principaux risques. Ce faisant, vous pourrez mieux comprendre les menaces réelles susceptibles de compromettre la sécurité de votre organisation.

Votre tolérance au risque doit être définie dès le départ, afin que vous puissiez mettre en œuvre les mesures de sécurité appropriées en fonction des menaces réelles auxquelles vous êtes confronté. Vous éviterez ainsi de consacrer des ressources à des menaces peu susceptibles de se produire ou qui n'auront que peu ou pas d'impact sur votre entreprise.

Vous devez procéder à des évaluations régulières des risques pour vous assurer que votre approche en matière de cybersécurité est conforme aux cadres réglementaires, aux normes de sécurité de l'information et aux lois comme le règlement général sur la protection des données (RGPD).

Prenez le temps d'identifier correctement les risques pour affiner le message, la diffusion et le ciblage efficace de votre programme de sensibilisation à la cybersécurité.

Protégez vos actifs informationnels

Pour élaborer une stratégie globale de cybersécurité et identifier efficacement les risques, vous devez procéder à un audit complet des actifs informationnels de votre organisation.

Un actif informationnel est un élément d'information qui a de la valeur pour votre organisation. Il peut s'agir d'informations personnelles identifiables (PII), d'informations financières, de propriété intellectuelle ou de toute autre information importante pour votre entreprise.

Vous devez déterminer quels sont les actifs informationnels les plus précieux, où ils se trouvent et qui y a accès. Chaque actif doit être catégorisé (par exemple, public, privé ou confidentiel) et protégé en fonction de sa valeur. Cette démarche est cruciale pour identifier les risques et classer par ordre de priorité les zones qui doivent être défendues.

Après avoir identifié ces domaines, vous pouvez vous concentrer sur la manière dont chaque actif informationnel risque d'être compromis. Qu'il s'agisse d'une violation du système, d'un logiciel malveillant ou même d'une menace interne, vous pouvez prendre des mesures éclairées pour améliorer ces processus et réduire la probabilité qu'un cybercriminel accède à des systèmes stratégiques.

Concentrez-vous sur les groupes à haut risque

La clé d'un programme efficace de sensibilisation à la sécurité est de s'assurer que la formation judicieuse cible les personnes qu'il faut. Tous les utilisateurs sont sensibles aux cybermenaces. Toutefois, certains employés sont plus exposés aux menaces que d'autres. Par exemple, vos services RH et financier seront fréquemment visés en raison de leur accès privilégié à des données sensibles.

Le PDG, le directeur financier et les cadres supérieurs sont également des cibles privilégiées en raison de leur accès à de précieuses informations sur l'entreprise. Ils sont souvent la cible d'escroqueries sophistiquées via des attaques par piratage de la messagerie d'entreprise. Dans ce type d'attaque par phishing, les cybercriminels se font passer pour un cadre de haut niveau afin de convaincre un employé, un client ou un vendeur de transférer de l'argent sur un compte frauduleux ou de divulguer des informations sensibles. Si un cadre supérieur tombe dans le piège, les résultats risquent d'être dévastateurs et de mettre en péril la sécurité de votre organisation.

Reportez-vous au chapitre 2 pour plus d'informations sur les groupes les plus vulnérables et sur la manière dont vous pouvez leur proposer des formations.

Rendez votre campagne intéressante grâce au partage d'expériences

Le *partage d'expériences* est l'un des moyens les plus puissants de donner vie à votre campagne de sensibilisation à la cybersécurité. La cybersécurité peut être un sujet rébarbatif, mais il est essentiel de trouver des moyens d'impliquer votre personnel si vous voulez avoir un impact positif sur les comportements au sein de votre organisation. Le message est tout simplement trop important pour se perdre dans les communications formelles de l'entreprise.

Raconter une histoire permet aux apprenants d'assimiler des contenus. Les histoires créent une réponse émotionnelle qui permet de se souvenir plus facilement de ce qui est enseigné. Vous pouvez donner vie aux messages de cybersécurité, en les rendant plus accessibles aux personnes dans leur vie quotidienne. En rendant l'histoire pertinente pour l'utilisateur, vous augmentez considérablement les chances que cette personne retienne l'information, améliorant ainsi la politique de sécurité globale de votre organisation. Le chapitre 5 explique plus en détail comment vous pouvez inclure le partage d'expériences dans votre campagne.

Mettez à jour votre gestion des politiques

Les politiques sont essentielles pour fixer les limites du comportement des individus, des processus, des relations et des transactions au sein de votre organisation. Elles fournissent un cadre de gouvernance, identifient les risques et permettent de définir la conformité, ce qui est important dans le paysage réglementaire de plus en plus complexe d'aujourd'hui.

Un système de gestion des politiques efficace dispose d'une méthode cohérente de création des politiques, structure les procédures de l'entreprise et facilite le suivi de l'attestation et des réponses du personnel. Par conséquent, ce système peut vous aider à rationaliser les processus internes, à démontrer votre conformité aux exigences réglementaires et à cibler efficacement les domaines qui présentent le plus grand risque pour la sécurité des données.

Préparez-vous dès maintenant à une violation de données

Si vous n'avez pas commencé à vous préparer à une violation de données, c'est le moment de le faire. Des milliards de données confidentielles ont été exposées et, selon IBM, le coût moyen mondial d'une violation de données a atteint le chiffre stupéfiant de 3,92 millions de dollars.

Il ne s'agit plus de savoir « si » votre organisation va être attaquée, mais « quand ». Vous devez commencer à vous préparer à l'inévitable et mettre en place un plan garantissant une réaction appropriée en cas d'atteinte à la sécurité.

La mise en place d'un plan de réponse efficace permet de former et d'informer le personnel, d'améliorer les structures organisationnelles,

de renforcer la confiance des clients et des parties prenantes, et de réduire tout dommage financier ou de réputation potentiel à la suite d'une violation.

CONSEIL

Vous devez tester régulièrement votre plan de réponse en cas de violation des données afin d'identifier les points faibles et de vous assurer que chaque membre de votre équipe comprend ses responsabilités, tant dans la préparation que dans la réaction en cas de violation.

Recrutez des champions de la cybersécurité

La cybersécurité n'est pas seulement une question de technologie. Vos collaborateurs jouent un rôle essentiel dans la défense de votre organisation et dans l'identification des menaces susceptibles de mettre en danger votre sécurité.

Désigner des champions de la cybersécurité est un excellent moyen de responsabiliser le personnel et de le doter des compétences nécessaires pour prévenir une cyberattaque. Selon le National Cyber Security Centre du Royaume-Uni, la moitié des entreprises victimes d'une cyberattaque ont constaté que les menaces les plus perturbatrices étaient signalées directement par le personnel, au lieu d'être détectées automatiquement par un logiciel.

Les champions de la cybersécurité n'ont pas besoin d'être des experts techniques ; il s'agit d'ajouter une touche humaine à votre stratégie de sécurité et de rallier du personnel qui s'engage à faire connaître et à mettre en œuvre les bonnes pratiques en matière de cybersécurité.

Le chapitre 3 fournit des conseils spécifiques sur la manière d'identifier et d'utiliser les champions de votre organisation.

Tenez compte de votre chaîne logistique

Pour de nombreuses organisations, la chaîne logistique constitue le maillon le plus faible de leurs défenses dans le domaine de la cybersécurité. Plutôt que de cibler directement une entreprise, les cybercriminels tenteront de compromettre les réseaux et systèmes stratégiques d'une organisation en exploitant des failles dans les processus et systèmes de sa chaîne logistique.

Les chaînes logistiques constituent un élément essentiel des opérations commerciales, mais ces réseaux sont souvent vastes et diversifiés et s'étendent sur plusieurs pays. Ces fournisseurs n'ont généralement pas

mis en place de solides mesures de protection en matière de cybersécurité, ce qui signifie qu'ils présentent de nombreux points faibles que les cybercriminels peuvent exploiter.

Certaines des plus grandes violations de données de l'histoire récente sont le résultat d'attaques visant la chaîne logistique. La violation de Target aux États-Unis en 2014, qui a exposé les données personnelles de plus de 70 millions de clients, en est un bon exemple. En lançant une attaque de phishing sur l'un des fournisseurs de services de l'entreprise, les cybercriminels ont pu accéder aux lecteurs de cartes de paiement des points de vente (POS) de Target.

Chaque fournisseur qui se connecte à votre entreprise représente un risque potentiel. Il est donc essentiel que vous procédiez à des évaluations détaillées des risques liés aux tiers afin de résoudre tous les problèmes susceptibles de menacer votre sécurité. Vous pourrez ainsi déterminer les mesures de sécurité à mettre en place pour assurer la sécurité de vos données.

Le chapitre 3 examine comment vous pouvez étendre votre campagne aux fournisseurs tiers.

Mettez en place une surveillance adéquate et des examens réguliers

Le paysage des menaces évolue en permanence. Votre programme de sensibilisation à la cybersécurité doit donc évoluer avec lui. Il est important de procéder à des examens réguliers de l'état de préparation du personnel pour identifier les points faibles et déterminer si les politiques et les formations actuelles doivent être mises à jour.

Pour la conformité du point de vue réglementaire, les bonnes pratiques consistent à consigner les résultats de tous les examens et à donner suite à toute recommandation de correction des risques. Sans ces audits réguliers, votre programme de sensibilisation à la cybersécurité risque de ne pas refléter le paysage des menaces et de laisser votre organisation vulnérable aux attaques.

UNE SENSIBILISATION À LA CYBERSÉCURITÉ QUE VOTRE PERSONNEL APPRÉCIERA

www.metacompliance.com

Créez une culture de sensibilisation accrue à la sécurité

Les menaces pour la sécurité évoluent et deviennent de plus en plus sophistiquées. Les défenses technologiques traditionnelles ne suffisent pas à sécuriser une organisation contre sa plus grande faille de sécurité : l'élément humain. La nature humaine constitue une vulnérabilité majeure et les cybercriminels savent comment l'exploiter. L'ouvrage « Sensibilisation à la cybersécurité pour les Nuls » est un guide décrivant les stratégies, les défis et les meilleurs moyens de modifier le comportement des utilisateurs au sein d'une organisation afin d'identifier et de traiter les menaces de cybersécurité et de protéger les informations et les actifs précieux.

À l'intérieur…

- Découvrez comment mettre en œuvre avec succès un programme de sensibilisation à la cybersécurité
- Respectez les exigences réglementaires strictes
- Engagez le personnel dans une formation pertinente et spécifique à son rôle
- Intégrez la gestion des stratégies dans les programmes de sensibilisation à la sécurité
- Assurez le soutien de la direction pour les campagnes de sensibilisation à la sécurité

Allez sur Dummies.com®
pour voir des vidéos, des exemples pas à pas, des articles pratiques, ou pour faire des achats !

ISBN: 978-1-119-89963-1

pour les nuls®

WILEY END USER LICENSE AGREEMENT

Go to www.wiley.com/go/eula to access Wiley’s ebook EULA.