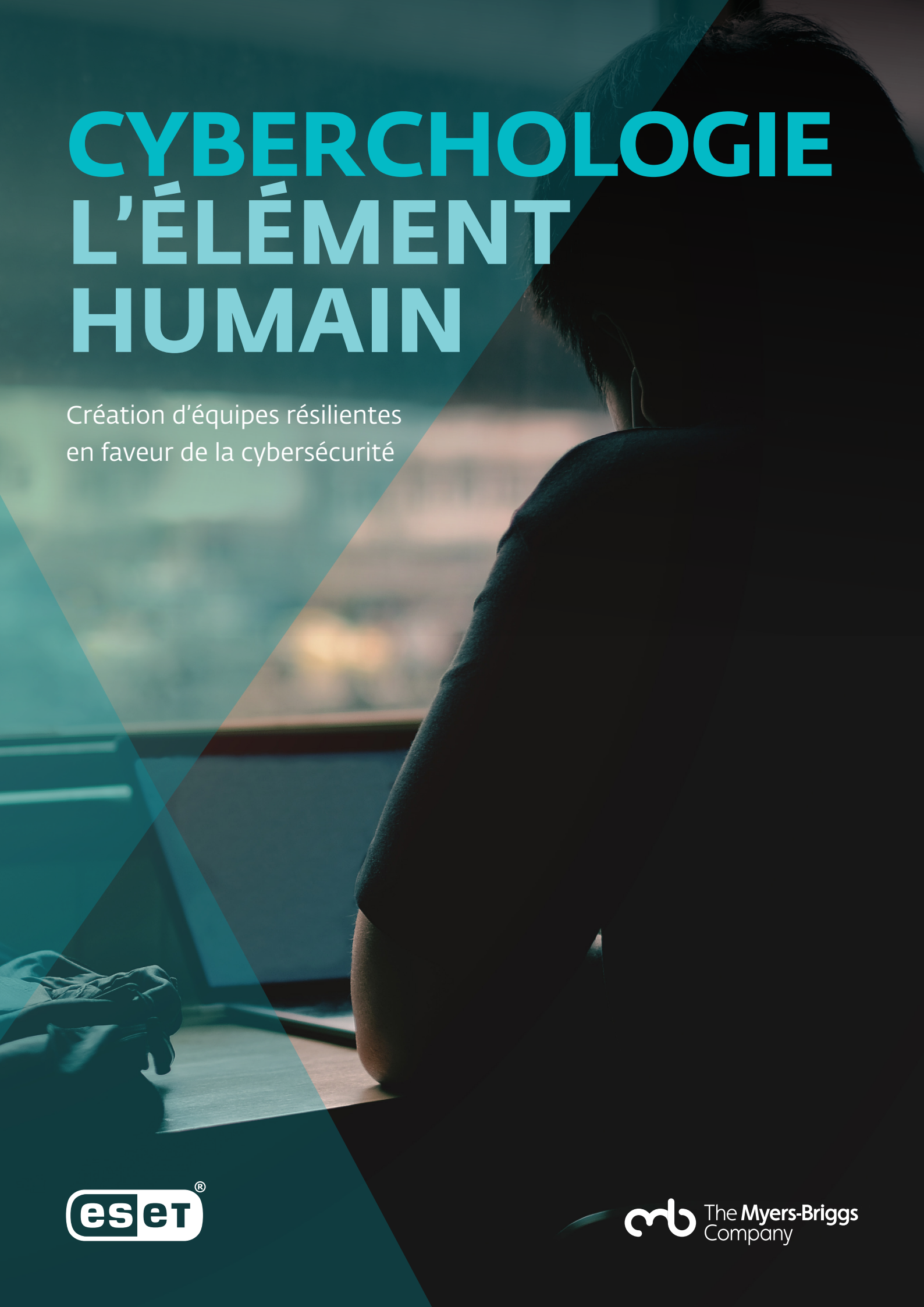


CYBERCHOLOGIE
L'ÉLÉMENT HUMAIN

Création d'équipes résilientes
en faveur de la cybersécurité

ESET®

The Myers-Briggs Company

La cybersécurité est devenue la considération la plus importante pour toute entreprise moderne. La majorité des entreprises ont une présence en ligne sous une forme ou une autre, et la technologie est au cœur de la plupart des fonctions métiers. La pandémie de COVID-19 agissant comme un catalyseur, la numérisation s'est accélérée dans presque tous les secteurs, et la nécessité d'être résilient et dynamique face au changement s'est accrue.

Dans le cadre de ce livre blanc de cyberchologie, **ESET**, le 1er éditeur Européen de solutions de sécurité, s'est associé à **The Myers-Briggs Company**, l'organisme leader en psychologie des entreprises, pour confirmer le rôle essentiel des salariés dans la protection des entreprises contre les menaces en ligne, en étudiant le lien entre le type de personnalité et les vulnérabilités face à la cybercriminalité. Le document examine également les attitudes et les expériences de plus de 100 responsables de la sécurité de l'information quant à la cybersécurité pendant les confinements dus au COVID-19.

Depuis que les gouvernements du monde entier ont mis en place des mesures de confinement en raison de COVID-19, le monde du travail a considérablement changé, d'une manière que la plupart des gens n'auraient pas pu imaginer : recours en masse au télétravail, qui s'appuie encore plus fortement que jamais sur la technologie, ainsi que des bouleversements dans les infrastructures technologiques de nombreuses entreprises. Les systèmes informatiques centraux ont été remplacés par un réseau d'individus disparates, tous ayant une plus grande responsabilité quant à leur propre utilisation de la technologie et leurs besoins en matière de sécurité. Non seulement un système de sécurité défaillant laisse les entreprises vulnérables, mais la confiance des salariés dans la gestion de la cybersécurité est également un risque sérieux.

Le paysage de la cybersécurité évolue constamment pour atténuer la sophistication croissante des cyberattaques. Le COVID-19 n'a fait qu'exacerber ce phénomène. Les études d'ESET ont révélé que depuis le début des confinements, la cybercriminalité a augmenté de 63 %, et les entreprises sont dans leur ligne de mire en raison de leurs effectifs désormais dispersés. Comme nous le verrons dans ce livre blanc, le télétravail est amené à se prolonger. Les entreprises doivent adapter leurs stratégies de cybersécurité en conséquence. La cybersécurité d'une entreprise est entre les mains de chaque salarié muni d'un ordinateur. Il ne s'agit plus d'un problème destiné uniquement aux dirigeants et aux équipes informatiques.

À une époque où les entreprises comptent sur la résilience, des acteurs malveillants exploitent les vulnérabilités de sécurité qui accompagnent le télétravail. Des mesures simples, telles que l'utilisation d'une interface de bureau virtuel ou l'obligation de chiffrer les fichiers sensibles, peuvent réduire la probabilité de réussite d'une attaque. Les recherches effectuées par ESET pour ce rapport ont révélé que plus de la moitié des entreprises n'avaient pas mis en place de mesures de continuité pour une éventuelle pandémie avant celle liée au COVID-19. Et parmi elles, 80 % ont déclaré avoir mis en place une stratégie de télétravail, seul un quart des entreprises considérerait que leur stratégie de télétravail et leur stratégie opérationnelle sont efficaces.

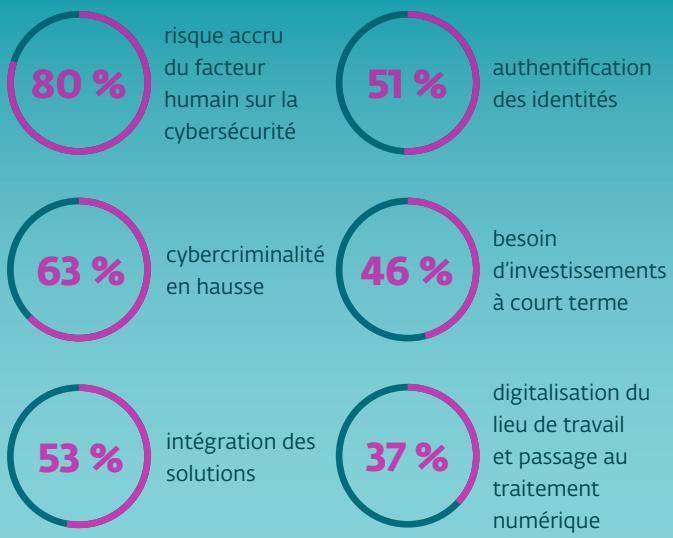
Pour que les entreprises ne se contentent pas de survivre, mais bien de prospérer, il est essentiel de mettre en place une stratégie de cybersécurité globale qui tienne compte des personnalités individuelles, ainsi qu'une solution logicielle complète pour les endpoints. Avec une telle responsabilité reposant sur des salariés travaillant tous à partir de différents lieux, appareils et réseaux, suivre de bonnes habitudes de cybersécurité et une formation personnalisée à la cybersécurité sont essentielles. Ce livre blanc examine pourquoi et comment les équipes de RH et techniques devraient travailler ensemble pour développer des stratégies, des équipes et des systèmes informatiques résilients, pour favoriser la résilience de l'entreprise.

Les défis de la cybersécurité

Avant l'épidémie de COVID-19, le nombre de cyberattaques était déjà en hause. La pandémie et les confinements qui en ont résulté n'ont fait qu'accroître ce risque. Les cybercriminels ont utilisé des tentatives d'hameçonnage et des malwares sur le thème du COVID-19 pour tirer parti des vulnérabilités innées de la main-d'œuvre dispersée et de ses systèmes informatiques. Les RSSI ont signalé une augmentation de 63 % de la cybercriminalité pendant les confinements, tandis que de nombreuses entreprises luttaient pour survivre, ou adaptaient rapidement leurs modèles économiques et opérationnels pour survivre. La pandémie a transformé le monde du travail tel que nous le connaissons, et les entreprises devront adapter leurs stratégies de cybersécurité en conséquence.

Outre les coûts d'une attaque proprement dite sur les opérations et la réputation, les amendes infligées par les organismes de réglementation augmentent. Avant la pandémie, le bureau du commissaire à l'information (ICO) **a infligé deux amendes de plusieurs millions d'euros** contre British Airways et Marriott, en vertu du règlement général sur la protection des données (RGPD). Même si les grandes entreprises ont les moyens de faire face aux ramifications d'une attaque, les petites entreprises, elles, risquent d'être paralysées.

Principaux défis signalés par les entreprises pendant les confinements dus à COVID-19



L'étude d'ESET a révélé que pour 75 % des entreprises, la moitié de leur activité est assurée par des salariés qui télétravaillent alors que ce n'était pas le cas avant le COVID-19. À l'inverse, moins de 25 % des entreprises ont déclaré être dans l'incapacité de travailler parce qu'elles ne pouvaient pas réaliser leurs projets à distance. Même si les employés finiront par revenir au bureau, le télétravail, sous une forme ou une autre, est là pour durer. De nombreuses entreprises ont été en mesure de fonctionner en télétravail pendant les confinements, mais avec des systèmes et des processus adaptés. Avec cette transition soudaine, les entreprises ont été obligées d'innover, ce qui montre qu'il est en fait possible d'effectuer une grande partie de notre travail à distance.

Le télétravail a permis une certaine flexibilité, mais il a également modifié considérablement les systèmes et les processus métiers afin de répondre aux besoins d'une main-d'œuvre dispersée. L'accès des salariés aux services informatiques, et vice versa, a changé. La collaboration et le travail d'équipe sont facilités virtuellement, et l'absence de communication en face à face peut entraver les canaux de communication directs. Certaines des mesures de sécurité courantes dans un bureau doivent être compensées à domicile, notamment l'obligation pour les employés à distance d'utiliser une authentification multifacteur ou un VPN pour accéder aux réseaux internes. Rappeler aux télétravailleurs d'activer les mises à jour automatiques et vérifier la sécurité de leurs propres réseaux Wifi est une première ligne de défense cruciale contre les cybercriminels.

Lors de l'évaluation des défis associés aux salariés qui travaillent à domicile, 80 % des entreprises ont déclaré qu'un risque accru causé par des facteurs humains constituait une sorte de défi pour la cybersécurité. De plus, 37 % des entreprises ont déclaré que la numérisation du lieu de travail et le passage au traitement en ligne ont constitué un défi. Avec la combinaison de systèmes informatiques fragmentés et d'un manque de sécurité centrale, le passage soudain au télétravail et un climat mondial de stress et d'inquiétude constituent le terreau idéal pour une cyberattaque réussie.

L'impact du stress sur les habitudes de cybersécurité

La crise du coronavirus a ajouté une couche supplémentaire de stress et d'inquiétude à notre vie quotidienne. Il peut être difficile de se concentrer et de rester motivé au travail, ce qui rend les salariés plus vulnérables aux cybermenaces. Dans son rapport « **Personnalité et stress dans un monde virtuel** », The Myers-Briggs Company a constaté que 47 % des personnes interrogées étaient assez ou très inquiètes quant à leur capacité à gérer le stress pendant la crise du coronavirus. L'économie entrant en récession ainsi que la santé de la famille et des amis étant les principales préoccupations. Ce courant sous-jacent persistant de stress affecte les différents types de personnalité de diverses manières, et se manifeste dans la façon dont les gens gèrent le stress et réagissent à certaines situations. Des salariés déjà anxieux peuvent être plus enclins à paniquer et cliquer sur un lien malveillant, ou un manque d'attention aux détails peut faire qu'une faille de sécurité ne soit pas correctement signalée au service informatique.

Mieux connaître votre type MBTI peut vous aider. Voici quelques éléments qui détaillent les contours de chaque profil, en fonction de la partie la plus utilisée de leur personnalité, le cœur de leur caractère, et leur comportement sous pression.

Activiste (ESTP et ESFP)

Facteurs de stress

- Manque de stimulation et d'enthousiasme
- Tâches théoriques et abstraites sans application pratique immédiate
- Être physiquement confiné, par ex. en raison d'une maladie ou de circonstances particulières

Stress quotidien et comportement

- Recherche de plus en plus de stimulation externe
- Peut se comporter de manière dangereuse ou à la recherche de sensations fortes et d'excès
- Ne vit que dans le moment présent et ne prend aucune décision

Explorateur (ENTP et ENFP)

Facteurs de stress

- Les gens qui disent « ça ne marchera jamais »
- Trop de détails apparemment non pertinents
- Manque de variété, ne pas pouvoir faire quelque chose de nouveau

Stress quotidien et comportement

- Partage des idées de plus en plus irréalisables avec de plus en plus de personnes
- Incapable de prendre les choses au sérieux, devient destructeur par « jeu »
- Ne sera pas contraint par des décisions

L'impact du stress sur les habitudes de cybersécurité

Directeur (ESTJ et ENTJ)

Facteurs de stress

- Personnes, systèmes ou entreprises inefficaces
- Situations ambiguës, impossibilité de prendre des décisions, blocages
- Devoir se concentrer sur les sentiments des gens, plutôt que sur la tâche à accomplir

Stress quotidien et comportement

- Devient excessivement directif, énergique, voire agressif
- Prend des décisions rapides et les impose aux autres
- Rejette les preuves/autres opinions qui ne correspondent pas à son point de vue

Éducateur (ESFJ et ENFJ)

Facteurs de stress

- Conflit avec les autres et entre les autres
- Manque de chaleur, absence de réciprocité de l'amabilité
- Injustice dans le monde en général

Stress quotidien et comportement

- Devient expansif et trop amical
- Exigeant dans la satisfaction de ses propres besoins et de ceux des autres
- Interprète les situations en fonction de ses valeurs, en ignorant toute preuve

Conservateur (ISTJ et ISFJ)

Facteurs de stress

- Agir sans informations ni plans détaillés et pratiques
- D'autres personnes qui rejettent les leçons de l'expérience passée du conservateur
- Changer des choses qui fonctionnent déjà

Stress quotidien et comportement

- Recherche de façon obsessionnelle la seule information importante
- Se met en retrait du monde extérieur
- Impossibilité de prendre une décision avant d'avoir trouvé toutes les informations

L'impact du stress sur les habitudes de cybersécurité

Visionnaire (INTJ et INFJ)

Facteurs de stress

- Ne pas avoir le temps de réfléchir aux possibilités avant de répondre
- Voir ses idées mûrement réfléchies rejetées ou ignorées
- Personnes désorganisées ou ayant des opinions arrêtées

Stress quotidien et comportement

- Se met en retrait, pour échafauder des idées de plus en plus complexes dans leur tête
- Ce type peut se dissocier de la réalité
- Incapable d'agir avant d'avoir étudié toutes les possibilités

Analyste (INTP et ISTP)

Facteurs de stress

- Voir ses solutions soigneusement raisonnées rejetées ou ignorées
- Des décisions illogiques qui n'ont pas été réfléchies
- Manifestations excessives d'approbation ou d'émotion de la part des autres

Stress quotidien et comportement

- Se met en retrait pour résoudre les problèmes par ses propres moyens
- Se focalise sur la recherche de la solution unique et correcte
- Ignore les autres, prend des décisions sans les informer

Conscience (ISFP et INFP)

Facteurs de stress

- Les personnes qui ignorent, rejettent ou contreviennent à leurs valeurs
- Avoir un emploi en contradiction avec ses valeurs
- Personnes ou entreprises inflexibles et irréfléchies

Stress quotidien et comportement

- Se met en retrait dans un dialogue intérieur
- Travaille de manière obsessionnelle à des décisions qui correspondent à ses valeurs
- Ignore les faits qui ne cadrent pas avec ses idées

Résilience

Alors que nous sommes aux prises avec un changement de paradigme dans nos vies professionnelles et familiales, la résilience est plus importante que jamais. Plus de 50 % des entreprises prévoient de maintenir en place, d'une manière ou d'une autre, les changements survenus depuis le début de la crise de COVID-19. Aujourd'hui plus que jamais, les sociétés doivent placer la résilience au coeur de leurs systèmes et de leurs équipes informatiques.

Des salariés confiants et formés aux bonnes pratiques de cybersécurité constituent le fondement d'une stratégie résiliente. Dans son **étude sur le catphishing**, ESET a examiné et découvert les habitudes de cybersécurité de 2 000 salariés au Royaume-Uni. 69 % de ces Britanniques se disent préoccupés par leur cybersécurité mais ne savent pas quoi faire, quand 68 % des 25-54 ans et 55 % des plus de 55 ans admettent être préoccupés par la cybersécurité. Même si les salariés de la tranche d'âge des 16-24 ans sont moins inquiets, cela ne signifie pas nécessairement qu'ils sont moins susceptibles d'être victimes d'une attaque, car la complaisance, le manque de compétences et de formation peuvent rendre les entreprises vulnérables.

« L'étude Catphishing d'ESET, qui s'est penchée sur les habitudes de cybersécurité de 2 000 salariés au Royaume-Uni, a découvert que 69 % des Britanniques sont préoccupés par leur cybersécurité mais n'ont aucune idée de ce qu'ils peuvent faire, 68 % des 25-54 ans et 55 % des plus de 55 ans admettant être préoccupés ou inquiétés par la cybersécurité. »

Malgré une nette augmentation des menaces et un manque de compétences des salariés, 40 % des RSSI ont déclaré que le COVID-19 n'avait eu aucun impact sur la taille de leur budget de sécurité informatique, par rapport au budget initialement prévu. Cette négligence peut exposer les entreprises à de futures cyberattaques et les priver des ressources nécessaires pour y remédier. Les équipes informatiques doivent repenser le mode de fonctionnement de la sécurité organisationnelle, le télétravail devenant la norme et non plus l'exception.

L'écrasante majorité des cyberattaques aboutissent non pas grâce à l'habileté des pirates, mais à cause d'une erreur humaine ou d'un oubli. En effet, 80 % des entreprises ont déclaré que l'un des principaux défis entraînés par le COVID-19 était l'augmentation du risque entraîné par le facteur humain sur la cybersécurité. La façon dont les gens préfèrent assimiler les informations et communiquer peut jouer un rôle dans la manière dont les différents membres d'une équipe abordent la cybersécurité, car tous les types de personnalité ont des faiblesses et des points forts différents qui peuvent avoir une incidence sur le résultat d'une attaque.

Le modèle de personnalité MBTI (indicateur du type Myers-Briggs) s'intéresse à quatre domaines de la personnalité : Extraversion ou Introversion, Sensation ou Intuition, Pensée ou Sentiment, Jugement ou Perception, et à leur combinaison dynamique pour décrire la personne dans son ensemble. Par exemple, les personnes ayant une personnalité extravertie (celles qui élaborent des idées en les vocalisant) ont tendance à être plus vulnérables à la manipulation, à la tromperie et à la persuasion des cybercriminels, tandis que les personnes ayant une préférence pour la sensibilité (celles qui observent et se souviennent des détails) sont plus susceptibles de repérer les attaques d'hameçonnage, mais de prendre également des risques pour la sécurité. Bien que les différentes préférences des personnalités ne garantissent pas une sensibilisation ou des connaissances en matière de cybersécurité, l'intégration d'une conscience de soi et d'une compréhension de la personnalité dans la formation à la cybersécurité est un point de départ pour comprendre où se situent les faiblesses en matière de cybersécurité.

Si l'erreur humaine est responsable de la majorité des cyberattaques, les entreprises ne peuvent ignorer l'impact des caractéristiques et des traits humains sur les habitudes de cybersécurité des salariés. La sécurité numérique a longtemps été considérée comme relevant de la seule responsabilité des départements informatiques, mais pour élaborer une stratégie de cybersécurité holistique qui tienne compte du facteur humain, les départements informatiques et RH doivent travailler ensemble. À l'aide de tests psychométriques et d'outils de connaissance de

Résilience

soi, les RH peuvent identifier la composition des équipes et repérer les vulnérabilités potentielles. Les équipes informatiques peuvent utiliser ces informations pour créer des protocoles de sécurité complets et une cyberstratégie proactive afin de conserver une longueur d'avance sur les menaces potentielles.

La prise en compte des préférences de la personnalité peut également rendre la formation à la cybersécurité plus attrayante et plus efficace. En dispensant une formation plus étendue lors de l'intégration, et en la poursuivant par des vérifications et des actualisations régulières adaptées à la personnalité des salariés, les bonnes habitudes de cyberhygiène et de sécurité ont plus de chances d'être respectées. Ce point est particulièrement important si l'on considère le passage de nombreuses entreprises au télétravail. Les équipes informatiques ayant moins de visibilité et d'accès physique aux salariés individuels, il est essentiel de veiller à ce que votre personnel soit correctement formé aux bonnes pratiques de cybersécurité pour protéger l'ensemble de l'entreprise.

Le paysage de la cybersécurité a considérablement évolué au cours des 12 derniers mois. Certaines menaces ont évolué et ont refait surface sous différentes formes. La plupart d'entre elles sont généralement des malwares ou des tentatives d'hameçonnage. Les entreprises peuvent éviter les attaques malveillantes sur leurs systèmes lorsque les gens sont conscients du type d'attaque auquel ils peuvent être vulnérables, et peuvent ainsi être proactives dans l'atténuation des cyber-risques.

Hameçonnage

Couramment effectué via email, l'hameçonnage est une escroquerie en ligne par laquelle un cybercriminel se fait passer pour une entité digne de confiance afin d'obtenir les données sensibles de la victime.

Le groupe Sednit, également connu sous les noms d'APT28, Fancy Bear, Sofacy ou STRONTIUM, opère depuis au moins 2004 et a souvent fait la une des actualités ces dernières années. Le 20 août 2019, une nouvelle campagne a été lancée par le groupe, ciblant ses victimes habituelles : les ambassades et les ministères des Affaires étrangères des pays d'Europe de l'Est et d'Asie centrale. **La dernière campagne** a commencé par un email d'hameçonnage contenant une pièce jointe malveillante qui déclenche une longue chaîne de téléchargements, se terminant par une porte dérobée. Les types de personnalité tels que les ENFP et les ENTP peuvent être vulnérables aux attaques d'hameçonnage, telles que celles utilisées par le groupe Sednit via un format d'email simple. Même si les ENFP et les ENTP peuvent avoir des affinités pour les technologies de l'information, la meilleure pratique pour ces types de personnalité consiste à prendre le temps de vérifier la validité des emails qu'ils reçoivent avant d'y répondre, et se méfier de ceux comportant un contenu intrigant ou qui font appel à l'émotion.

ENFP

- Les ENFP sont parmi les premiers à se rendre compte de la mise en place d'un nouveau processus de sécurité
- Ils prennent la sécurité informatique très au sérieux si elle devient une de leurs valeurs

Conseils en matière de cybersécurité :

- Méfiez-vous des emails chargés émotionnellement
- Réfléchissez avant de cliquer

ESFP

- Les ESFP prennent des mesures rapides lorsqu'ils remarquent des anomalies
- Ils suivent en général les règles et les politiques de sécurité informatique

Conseils en matière de cybersécurité :

- Ne faites pas confiance à un réseau public pour les données sensibles, même s'il est accessible via un mot de passe
- Ne considérez pas les choses comme acquises ; il est utile d'être vigilant, voire même méfiant

ISTJ

- Les ISTJ sont susceptibles de repérer les incohérences et les erreurs dans les emails d'hameçonnage
- Ils suivent en général les règles et les politiques de sécurité informatique

Conseils en matière de cybersécurité :

- N'utilisez pas seulement des variations du ou des mêmes mots de passe
- Restez vigilant. L'expérience passée ne doit pas être votre seul guide

ENTP

- Les ENTP, férus d'informatique, s'efforceront d'être compétents et d'éviter les erreurs « stupides »
- Ils sont désireux de faire bouger les choses (même si cela peut impliquer de contourner les règles)

Conseils en matière de cybersécurité :

- Si vous compromettez la sécurité, les autres peuvent vous considérer comme incompétent
- Prenez le temps de lire vos emails, vous pourriez repérer quelque chose

ESTP

- Lorsqu'ils sont persuadés de l'importance de la cybersécurité, les ESTP peuvent rapidement repérer ce qui ne va pas et prendre immédiatement des mesures

Conseils en matière de cybersécurité :

- La sécurité informatique est importante, et les règles s'appliquent également à vous
- Obtenez des exemples précis de ce que vous pouvez faire différemment, et agissez en conséquence

ISFJ

- Les ISFJ sont susceptibles de repérer les incohérences et les erreurs dans les emails d'hameçonnage
- Il sont peu susceptibles de se faire piéger deux fois par la même cyberattaque

Conseils en matière de cybersécurité :

- Ne faites pas confiance à un réseau public pour les données sensibles, même s'il est accessible via un mot de passe
- Faites attention à qui vous faites confiance. En ligne, les gens ne sont pas forcément ceux que vous croyez

Malwares

Les malwares se présentent sous une grande variété de formes, notamment des virus, des logiciels espions et des ransomwares, qui peuvent compromettre votre ordinateur et vos données. **DePriMon est un exemple récent de téléchargeur malveillant** avec plusieurs étapes d'infection, qui utilise de nombreuses techniques non traditionnelles. Pour parvenir à ses fins, le malware enregistre un nouveau moniteur de port local, ce qui est une astuce qui relève de la technique « Moniteurs de port » de la base de connaissances MITRE ATT&CK. Il utilise le nom « Windows Default Print Monitor » pour dissimuler sa nature malveillante.

Les types de personnalité tels que les ESTJ et ENTJ peuvent être plus vulnérables aux téléchargements malveillants déguisés en logiciels ou modules légitimes. Bien qu'ils maîtrisent généralement les protocoles de sécurité, cette tendance peut les amener à prendre une décision rapide par souci d'efficacité. Ces types de personnalité devraient s'attacher à recueillir toutes les informations pertinentes avant de prendre des décisions. Ils devraient également s'efforcer de renforcer leur savoir sur la cybersécurité avant toute action.

ESTJ

- Les ESTJ sont susceptibles de suivre les règles et les processus de sécurité informatique, et de chercher à les améliorer
- En général, ils prennent la cybersécurité au sérieux

Conseils en matière de cybersécurité :

- Ne faites pas toujours les choses de la même façon et n'utilisez pas toujours les mêmes mots de passe
- Ne soyez pas tenté de faire des économies pour être plus efficace

ESFJ

- Les ESFJ sont conscients des politiques de sécurité informatique et les suivent consciencieusement
- Ils forment des habitudes de sécurité et les utilisent pour suivre efficacement les règles

Conseils en matière de cybersécurité :

- Faites attention à qui vous faites confiance. Les personnes en ligne ne sont pas forcément ce qu'elles semblent être
- Ne faites pas toujours les choses de la même manière et n'utilisez pas toujours les mêmes mots de passe

INFJ

- Les INFJ peuvent compliquer les choses à l'excès et chercher des significations cachées. Cela peut être un atout pour la sécurité informatique

Conseils en matière de cybersécurité :

- Quand quelque chose semble suspect, vérifiez, vérifiez et vérifiez encore
- N'oubliez pas de vérifier les détails – ils sont importants !

ENTJ

- Les ENTJ sont parmi les premiers à se rendre compte de la mise en place d'un nouveau processus de sécurité
- Ils se tiennent au courant et posent des questions pour comprendre les problèmes de sécurité

Conseils en matière de cybersécurité :

- Ne vous précipitez pas pour changer les processus de sécurité ; commencez par en savoir plus sur eux
- Évitez d'écarter les autres, qui pourraient avoir une connaissance plus approfondie de la sécurité informatique

ENFJ

- Ils respecteront les règles lorsque celles-ci sont claires
- Ils prendront la sécurité au sérieux s'ils sont conscients des effets des attaques sur les personnes

Conseils en matière de cybersécurité :

- Soyez proactif en matière de sécurité informatique, même à la maison
- Ne réutilisez pas les mots de passe et n'utilisez pas le même pour différentes applications

INTJ

- Les INTJ valorisent la connaissance, et s'efforcent d'être capables et compétents
- Ils suivent en général les règles et les politiques de sécurité informatique

Conseils en matière de cybersécurité :

- Vous ne savez pas nécessairement ce qui est le mieux, même si les règles semblent inutiles
- Si vous voulez être compétent, pensez à vérifier les détails des emails

Objets connectés

Nos vies sont de plus en plus envahies d'appareils, souvent tous connectés les uns aux autres, et fonctionnant sur les mêmes réseaux et systèmes connectés. Que ce soit à la maison ou au travail, nos appareils connectés créent des vulnérabilités pour des systèmes entiers lorsque chaque appareil n'est pas correctement sécurisé, comme un téléphone personnel ou une smartwatch se connectant à un réseau d'entreprise. Des chercheurs ont récemment découvert qu'avec un modèle de smartwatch particulier, ils étaient en mesure d'accéder à la localisation, au numéro de téléphone, aux **photos** et aux **conversations de plus de 5 000 enfants**, le fabricant n'ayant pas sécurisé ses serveurs correctement.

Les types de personnalité tels que les ISTP et les INTP peuvent être vulnérables lorsqu'ils gèrent eux-mêmes leurs appareils connectés, même s'ils suivent généralement les règles. La meilleure pratique pour ces types de personnalité est de ne pas toujours supposer que vous savez tout, et de vous assurer que vous n'ignorez pas les règles ou les protocoles parce que vous pensez qu'ils ne s'appliquent pas à vous.

ISTP

- Les ISTP ont une saine méfiance des systèmes et des autres personnes en ligne
- Ils sont ravis de suivre les règles de sécurité informatique lorsqu'elles ont un sens logique

Conseils en matière de cybersécurité :

- Faites l'effort de trouver les raisons d'une règle avant de l'enfreindre
- Faire les choses à sa façon, rapidement sur le moment, peut être risqué

INTP

- De nombreux INTP sont bien informés sur les questions de cybersécurité
- Ils ont bien conscience que n'importe qui peut se faire piéger par des cyberattaques

Conseils en matière de cybersécurité :

- Trouvez les règles de sécurité informatique de votre entreprise et suivez-les
- Vous ne savez pas toujours ce qui est le mieux ! Les règles existent pour être appliquées

INFP

- Les INFP sont peu enclins à faire des choix soudains et risqués
- S'ils sont conscients des effets d'une mauvaise sécurité sur les autres, ils peuvent voir la nécessité de règles

Conseils en matière de cybersécurité :

- Votre entreprise aura des règles de sécurité informatique. Suivez-les
- Pour éviter de nuire à autrui, faites de la sécurité informatique une responsabilité personnelle

ISFP

- Les ISFP prennent la sécurité informatique au sérieux et font preuve de prudence dans leur comportement en ligne
- Ils suivent en général les règles et les politiques de sécurité informatique

Conseils en matière de cybersécurité :

- Prenez du recul avant de cliquer
- N'oubliez pas que les personnes en ligne, même les amis, peuvent ne pas être qui ou ce qu'elles semblent être

Leadership

Un leadership fort est au cœur d'une entreprise résiliente. Tout comme la dispersion physique de la main-d'œuvre a eu un impact sur la nature de la cybersécurité, elle a également influencé notre façon d'estimer ce qu'est un leadership efficace. En temps de crise, nous nous tournons vers les dirigeants pour être motivés et rassurés. La capacité d'un dirigeant à susciter une préoccupation et une sensibilisation authentiques à l'égard de la cybersécurité est un élément essentiel de la sécurité des entreprises. La cybersécurité est un problème qui concerne l'ensemble de l'entreprise. Ce n'est pas uniquement à la direction de l'aborder ou de la dicter.

À l'instar du maillon le plus faible d'une chaîne, un salarié peut mettre une entreprise en danger, quel que soit son niveau d'ancienneté. Par conséquent, une approche traditionnelle du sommet vers la base n'est pas nécessairement le moyen de mobiliser un soutien pour la cybersécurité. La direction d'une entreprise est par ailleurs souvent l'objet d'attaques à un rythme plus élevé, comme le « spear phishing », une attaque ciblée de malwares utilisant souvent des informations personnalisées afin de paraître légitime. Être victime d'une cyberattaque n'a rien à voir avec l'ancienneté, mais bien plus avec l'éducation et la sensibilisation. Pour qu'une stratégie de cybersécurité soit efficace, il est impératif que des habitudes et des processus positifs de cybersécurité soient intégrés à la culture des entreprises, et ne soient pas considérés comme étant une corvée ou un fardeau.

Plus haut dans ce rapport, nous recommandions des « conseils types » pour différentes personnalités quant au stress et à la cybersécurité. Si ces conseils constituent certainement un bon point de départ pour identifier les forces et les faiblesses individuelles, il est important que les entreprises tiennent compte de la manifestation des différentes préférences des personnalités dans une dynamique d'équipe. La manière dont une équipe interagit a un effet direct sur sa réaction face à une cyberattaque et sur les éléments de cyberhygiène qui pourraient être négligés dans les moments de stress ou de panique. Les dirigeants doivent également reconnaître leurs propres forces et faiblesses afin d'encourager la sensibilisation au sein des équipes et de l'entreprise.

En cultivant leur propre sensibilisation, les dirigeants peuvent non seulement mieux se comprendre, mais également commencer à apprécier les nuances de comportement au sein de leurs équipes, de leur département et de leur entreprise. Les types MBTI sont un moyen efficace et direct de le faire, mais les dirigeants qui souhaitent approfondir leur compréhension peuvent se tourner vers le Niveau II de l'évaluation MBTI. Pour chacune des quatre préférences MBTI, le Niveau II examine cinq facettes du comportement, donnant ainsi une image personnalisée de l'individu. Par exemple, la plupart des personnes ayant une préférence pour l'extraversion se sentiront à l'aise pour engager une conversation avec des inconnus dans des situations sociales (initier), mais certaines préféreront rester en retrait et attendre que les autres viennent à elles (recevoir). Inversement, la plupart des personnes ayant une préférence pour l'introversion joueront le rôle de receveur, mais d'autres auront un comportement d'initiateur. Le feedback résultant du Niveau II peut être particulièrement utile pour les dirigeants qui ont le sentiment d'être incompris par leur personnel.

La conscience de soi d'une équipe est tout aussi importante que la conscience de soi individuelle en matière de cybersécurité. Comprendre le profil de Niveau II d'une équipe peut aider à identifier les comportements grâce auxquels une cyberattaque pourrait réussir, et peut aider les équipes RH et informatiques à dispenser une formation personnalisée à la cybersécurité en fonction des besoins de l'équipe.

Conclusion

Indépendamment de ce que l'avenir nous réserve, deux choses sont certaines : notre façon de travailler a été irrévocablement transformée et les cyberattaques ne vont pas disparaître. La pandémie de COVID-19 n'a fait qu'accélérer la mise en œuvre de la technologie dans tous les domaines de la vie, et comme nos vies professionnelles et personnelles sont de plus en plus numérisées, la cybersécurité restera le pilier de la sécurité des entreprises. Les cyberattaques sont une menace constante pour les entreprises, qui doivent mettre en place des équipes et des systèmes informatiques résistants pour éviter les conséquences des attaques sur leurs finances et leur réputation. La sensibilisation de la main-d'œuvre joue un rôle essentiel dans la stratégie de cybersécurité de toute entreprise, pour améliorer l'efficacité des formations et inciter les collaborateurs à s'investir davantage dans leurs propres compétences. Comprendre que l'élément humain de la cybersécurité est tout aussi important que l'élément technique est la première étape de l'implémentation de protocoles holistiques qui tiennent compte des forces et des points faibles des individus.

En temps de crise, le leadership a un impact profond sur la culture et le moral de l'entreprise. Lorsque les dirigeants ont conscience d'eux-mêmes et de leurs équipes, ils peuvent instiller des processus et des pratiques plus efficacement, et guider les autres salariés dans leur propre cheminement vers la conscience de soi. De bonnes pratiques de cybersécurité doivent être ancrées à tous les niveaux d'une entreprise, et l'investissement dans la formation des salariés, tant en matière de cybersécurité que de conscience de soi, permettra aux équipes informatiques et RH d'élaborer des stratégies de cybersécurité intégrées, efficaces et proactives.