Deloitte.

Future of Cyber 2021

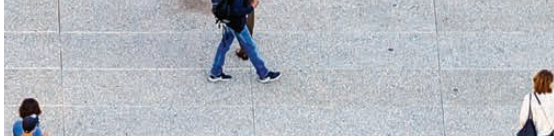
La complexité est la nouvelle norme.
Découvrez comment les entreprises
obtiennent plus de visibilité.

MAKING AN IMPACT THAT MATTERS since 1845

Future of Cyber 2021

Méthodologie

L'enquête Future of Cyber 2021, menée par Deloitte et Wakefield Research, a interrogé au sujet de la cybersécurité près de 600 hauts dirigeants d'entreprises présentant un revenu annuel d'au moins 500 millions de dollars, y compris près de 200 responsables de la sécurité de l'information, 100 directeurs des systèmes d'information, 100 dirigeants, 100 directeurs administratif et financier, et 100 directeurs marketing, entre le 6 juin et le 24 août 2021, par la voie d'une enquête en ligne.



Voir plus clair dans la complexité

Aujourd'hui, nous vivons la concrétisation d'un cybermonde où les initiatives de transformation numérique continuent de s'accélérer au milieu de l'émergence du télétravail, qui tend à se généraliser. Souvent, l'innovation technologique et la culture qu'elle produit semblent surgir avant que nous ayons la capacité de comprendre, de mesurer et de gérer les risques qui y sont associés, et qui croissent de manière exponentielle.

Malgré un niveau élevé de risque, la transformation numérique et la migration vers le cloud demeurent des priorités pour nos clients. Au-delà d'une simple amélioration de l'efficacité, les données qui circulent dans les organisations favorisent de nouveaux modes de création de valeur en reliant les lignes de services et en utilisant les données des consommateurs pour rehausser leurs expériences. Les résultats de notre enquête confirment cette migration : 94 % des directeurs administratif et financier ont indiqué qu'ils envisagent de déplacer leurs systèmes des finances ou leur ERP dans le cloud.

600
hauts dirigeants d'entreprises

Revenus d'au moins
500 M$

Siège social
40% en Amérique
28% dans les pays de l'EMEA
32% en Asie-Pacifique

L'état des lieux

Afin de demeurer concurrentielles, les entreprises d'aujourd'hui utilisent un éventail de technologies combinant une infrastructure on-premises, des systèmes d'information hybride et un assortiment de fournisseurs Cloud externes. Ces environnements intégrés sophistiqués nécessitent de nouvelles formes de gestion distinctes des architectures d' IT internes classiques. Une partie importante des directeurs des systèmes d'information et des responsables de la sécurité de l'information que nous avons interrogés (41 %) reconnaissent que la transformation et la visibilité des écosystèmes hybrides de plus en plus complexes sont les plus grands défis qu'ils doivent relever.

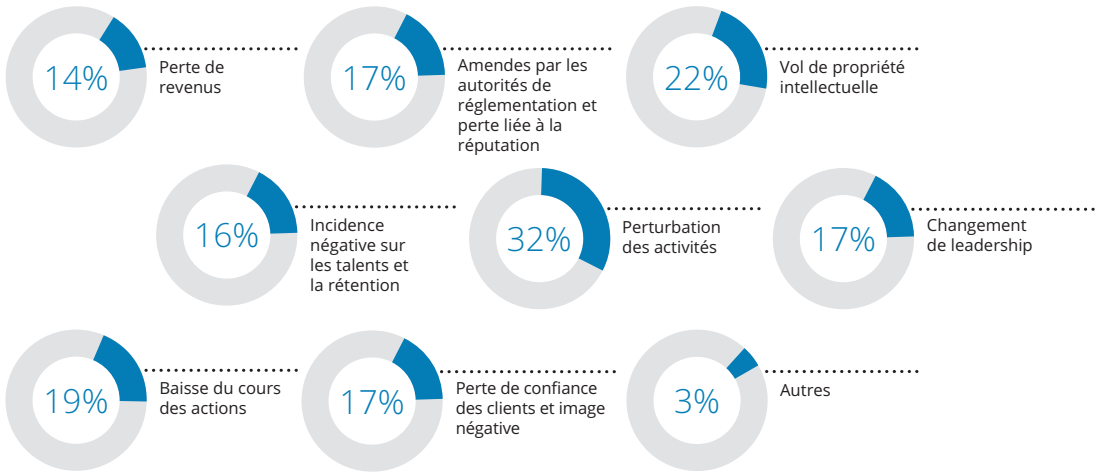
En plus des pressions du marché, la pandémie a entraîné l'arrivée du télétravail qui est destinée à devenir une caractéristique permanente du monde de l'emploi. Les organisations de toutes tailles ont rapidement transformé leurs environnements et ce faisant, elles ont multiplié leurs surfaces d'attaque sans avoir eu le temps nécessaire pour réfléchir aux conséquences sur la sécurité. Il n'est donc pas étonnant que l'on note une hausse des attaques ; en effet, 69 % des répondants ont indiqué une augmentation ou une augmentation importante des menaces à leur entreprise entre le début de 2020 et mai 2021, et cela de manière uniforme dans l'ensemble des secteurs et des régions. Ce sont 32 % des hauts dirigeants à l'échelle mondiale qui ont indiqué que les répercussions les plus importantes concernaient les perturbations opérationnelles, suivies par le vol de la propriété intellectuelle (22 %) et la baisse du prix des actions (19 %).

Ne jamais faire confiance. Toujours vérifier.

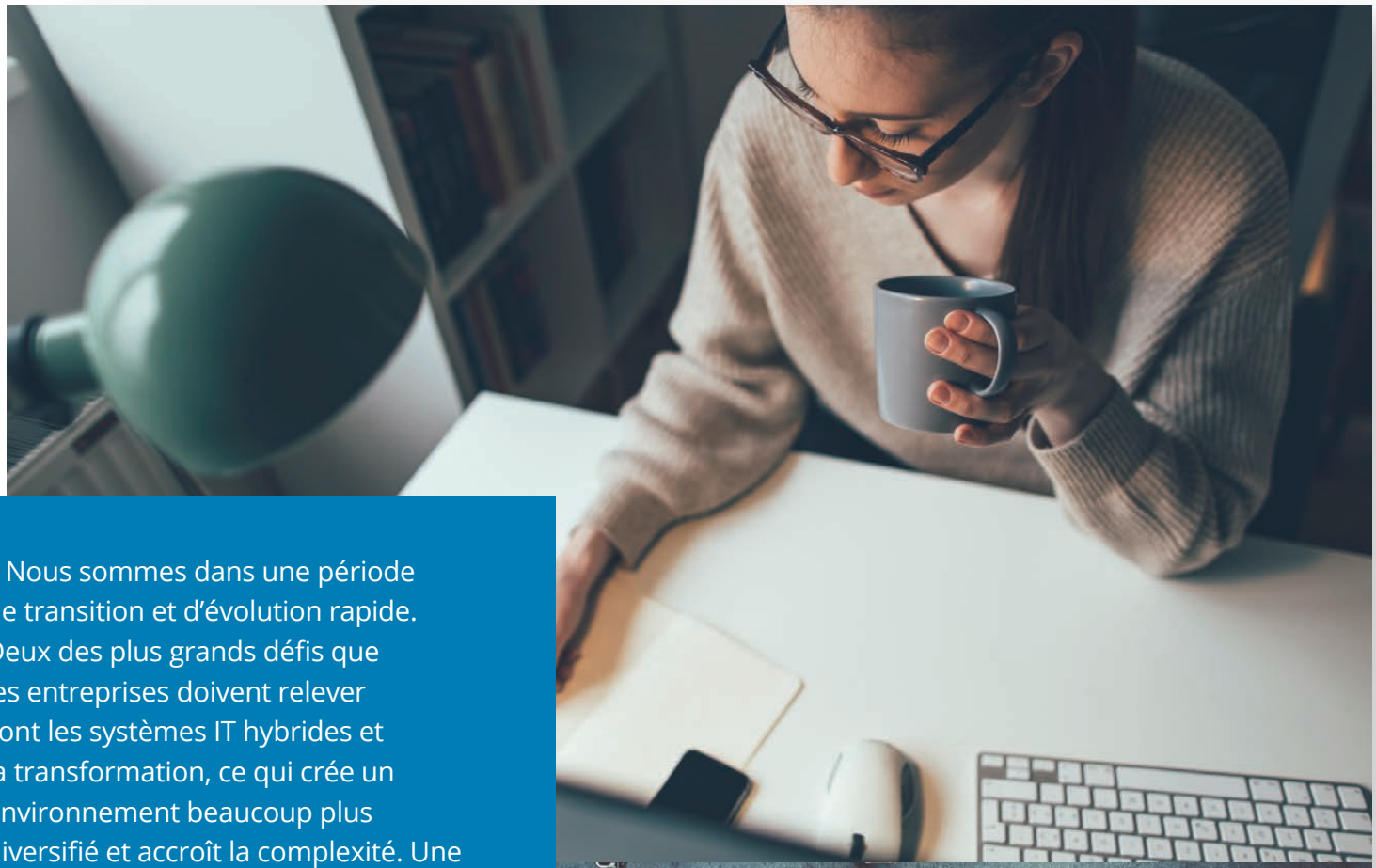
Lorsqu'on leur demande quels sont les plus grands obstacles à la gestion de la cybersécurité dans leur organisation, les répondants indiquent la gestion des données dans des périmètres complexes comme l'obstacle le plus important (44 %), suivie par la nécessité d'accorder une plus grande priorité aux cyberrisques à l'échelle de l'entreprise (31 %). Heureusement, il est maintenant possible de déployer le modèle zero trust, qui remplace la simple vérification des entités par des décisions d'accès en temps réel fondées sur le risque continu. La mise en oeuvre d'une telle architecture permet de réagir efficacement à la dissolution des périmètres dans les écosystèmes actuels, car elle reconnaît que chaque élément d'une architecture est vulnérable, et que chaque couche a besoin de protection.

Rendues possibles par les progrès récents de la puissance de calcul, l'émergence du modèle zero trust et son adoption entraînent des changements culturels dans les organisations qui révèlent à quel point le rôle de la cybersécurité se transforme et gagne en importance. Plus qu'une solution technologique, l'ensemble de solutions entrelacées qui constitue le modèle zero trust permet d'obtenir une vision des activités antagonistes et des risques opérationnels associés, et de l'information sur les changements qui sont requis pour réduire les risques. Cette information nécessite une coordination entre les systèmes d'informations et les lignes de services, de même que de l'éducation et de la formation à l'échelle de l'entreprise.

Incidences les plus importantes des cyberincidents*



*Les répondants pouvaient sélectionner jusqu'à deux réponses, c'est pourquoi les pourcentages ne totalisent pas 100%



« Nous sommes dans une période de transition et d'évolution rapide. Deux des plus grands défis que les entreprises doivent relever sont les systèmes IT hybrides et la transformation, ce qui crée un environnement beaucoup plus diversifié et accroît la complexité. Une plus grande visibilité, particulièrement dans le déploiement de solutions cloud, est la chose la plus importante que les organisations recherchent. »

— EMILY MOSSBURG, DELOITTE
LEADER MONDIALE DE LA CYBERSÉCURITÉ
CHEZ DELOITTE

Réorganiser vos défenses

À mesure que les pirates déploient des moyens plus sophistiqués et acquièrent une meilleure compréhension de la valeur marchande des actifs – qu'il s'agisse de brevets en pharmaceutique, en génie ou de produit, de données confidentielles de clients ou d'autres données essentielles – les organisations continuent d'accroître leur budget pour la cybersécurité. Près de 75 % de répondants qui présentaient des revenus supérieurs à 30 milliards de dollars ont indiqué qu'ils dépenseraient plus de 100 millions pour la cybersécurité cette année.

L'un des défis est de s'assurer que ces dépenses entraînent une meilleure visibilité des risques accrus que posent les écosystèmes de plus en plus complexes d'aujourd'hui. En plus de la technologie et de l'expertise, ils nécessitent un changement organisationnel pour faciliter la gouvernance programmatique, qui dépasse les limites de l'entreprise, car elle inclut les partenaires et les fournisseurs externes.

À mesure que la technologie change, le rôle du responsable de la sécurité de l'information évolue. Lorsque les cybertechnologies sont diffusées dans une entreprise, il est essentiel de repositionner la place du responsable de la sécurité de l'informationdans l'organigramme. Une place plus près du chef de la direction, en plus de simplifier la communication de l'information, permet au responsable de la sécurité de l'informationde comprendre les priorités de l'entreprise et de constater les innovations à mesure qu'elles sont mises en œuvre. Ce nouveau rôle opérationnel du responsable de la sécurité de l'information nécessitant un plus grand engagement à l'échelle de l'organisation permet à l'équipe de la cybersécurité de s'assurer que les exigences, les solutions techniques et les contrôles nécessaires peuvent être intégrés dans les initiatives d'innovation à partir du début. Cela réduit non seulement les risques au départ, mais aussi tous les risques associés à l'élaboration des produits et des services en général.

En raison des répercussions profondes que les cybertechnologies ont sur la culture, cette année, nous avons étendu notre enquête au-delà des dirigeants qui supervisent directement la cybersécurité pour inclure les personnes qui devraient être les plus grands champions de la cybersécurité : dirigeants, directeurs administratif et financier, directeurs marketing, directeurs des systèmes d'information et responsables de la sécurité de l'information. Ceux-ci ont exprimé des sentiments similaires, même si des variations sont observées selon les régions et les secteurs.

Vues sur l'avenir

Il n'existe pas de solution simple, tant sur le plan organisationnel que technologique, pour bien comprendre la complexité croissante des écosystèmes intégrés sur lesquels sont fondées les entreprises modernes. Cependant, l'utilisation combinée d'un certain nombre de mesures organisationnelles, culturelles et opérationnelles peut permettre aux organisations d'intégrer la cybersécurité au cœur des initiatives, de la culture et des écosystèmes technologiques en continuelle évolution de leur entreprise.

Dans ce rapport, nous explorons certaines de ces mesures et soulignons l'importance des capacités des organisations à voir plus clair dans les risques issus de la complexité, et d'avoir des vues sur l'avenir alors que la nouvelle vague d'évolution technologique continue d'accroître notre interconnectivité.

Le numérique et le défi de la transformation

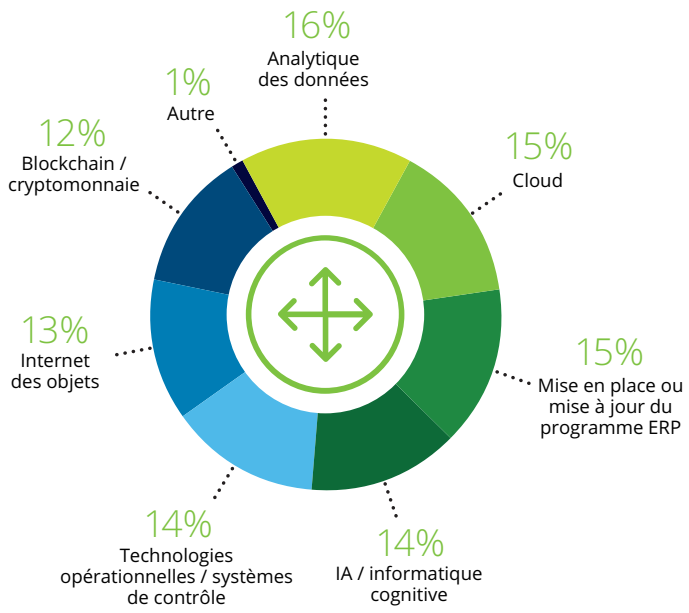
Dans chaque secteur, pour rester concurrentiel, il faut que de nouveaux produits et services soient développés et lancés sur le marché rapidement.

Dépassant la simple numérisation des processus actuels, les business modèles novateurs englobent les chaînes d'approvisionnement et ouvrent de nouvelles voies pour l'expérience client. Cette transformation expose également les entreprises à de nouvelles formes de cyberrisques, et nécessite de nouvelles stratégies de cybersécurité pour protéger les business modèles en évolution. Pour gérer ces risques, les hauts dirigeants et les membres du conseil d'administration doivent accepter le changement, établir une gouvernance efficace dans les lignes de services, et modifier les processus de gestion des risques pour avoir une vision d'ensemble de tous les secteurs nouvellement connectés de l'entreprise, incluant ceux qui sont gérés par des tiers. La réussite de cette opération dépend de l'engagement de la direction générale, de sa capacité à comprendre les cyberrisques et d'investissements judicieux dans la sécurité.

Lorsque nous avons demandé aux répondants de classer par ordre de priorité les initiatives de transformation numérique qu'ils comptent mener au cours des 12 prochains mois, l'analytique est arrivée au premier rang (16 %), le cloud au deuxième (15 %) et la mise en place / mise à jour du programme ERP au troisième (15 %). Dans l'enquête de cette année, l'ajout d'un nouveau choix de réponse concernant les technologies opérationnelles et les systèmes de contrôle industriel, qui a été sélectionné comme une grande priorité par 14 % des répondants, est révélateur des efforts que déploient divers secteurs pour numériser et moderniser les usines et les technologies opérationnelles.

La rapidité et l'ampleur du changement sont vraiment révolutionnaires. Cela est devenu une évidence lorsque nous avons vu une grande partie du monde passer en ligne à l'arrivée de la COVID-19. Des secteurs commerciaux entiers se sont transformés presque instantanément lorsque de grands pans d'effectifs se sont soudainement mis à travailler à distance. Heureusement, la plupart des éléments de l'écosystème numérique requis – du cloud et des technologies parallèles aux systèmes de contrôle industriel – étaient déjà en place et prêts à être déployés rapidement. Mais ce qui est moins visible, c'est l'éventail des cyberrisques qui a émergé de cette transformation, et peu d'entreprises disposent actuellement des moyens nécessaires pour comprendre et atténuer ces risques de façon acceptable.

Priorités dans la transformation numérique



"Le principal objectif des hauts dirigeants et des membres du comité éxécutif doit être de bien comprendre les risques que présente la transformation numérique pour leur entreprise, et de se doter des moyens de gérer ces risques comme tous les autres types de risques."

— MATTHEW HOLT, LEADER MONDIAL, STRATÉGIE EN CYBERRISQUES ET TRANSFORMATION, CYBERSÉCURITÉ DELOITTE

Comprendre les cyberrisques

Aujourd'hui, les cybermenaces affectent des entreprises entières, peuvent être dévastatrices pour les opérations et ruiner des réputations durement acquises. C'est pourquoi il est fondamental que les conseils d'administration évaluent les cyberrisques d'une manière qu'ils peuvent comprendre. Ils doivent pouvoir comparer les cybermenaces aux risques qu'ils ont l'habitude de gérer. L'analyse des profils de cyberrisques doit devenir pour eux aussi simple que de saisir la santé financière de leur entreprise par l'examen du bilan.

Lorsqu'ils comprendront la nature et l'ampleur des cyberrisques qui les menacent, ils sauront où investir pour atténuer le danger au maximum.

Dans le cadre de notre enquête, 41 % des répondants ont indiqué avoir recours à des évaluations de la cybermaturité pour orienter leurs décisions liées aux investissements dans la cybersécurité, 35 % ont dit utiliser des outils de quantification des risques, et 23 % ont avoué se fier à l'expérience des responsables de la cybersécurité de l'entreprise. Lorsqu'on leur a demandé à quelle fréquence ils effectuaient l'analyse des risques ou la modélisation des menaces pour leurs applications existantes ou nouvelles, 37 % des directeurs des systèmes d'information et des responsables de la sécurité de l'information ont indiqué le faire chaque trimestre, et 29 % ont indiqué le faire chaque mois. Bien que ces évaluations incombent normalement aux directeurs des systèmes d'information et aux responsables de la sécurité de l'information, il est essentiel que l'ensemble des parties prenantes comprenne la pertinence et l'importance de ces exercices.

À toute vapeur ?

Très souvent, la pression d'être concurrentiel amène les dirigeants d'entreprise à se concentrer sur les résultats de la transformation numérique et à négliger la gestion des cyberrisques. L'obsession de devancer les concurrents dans le marché crée une vision étroite, et de grands angles morts.

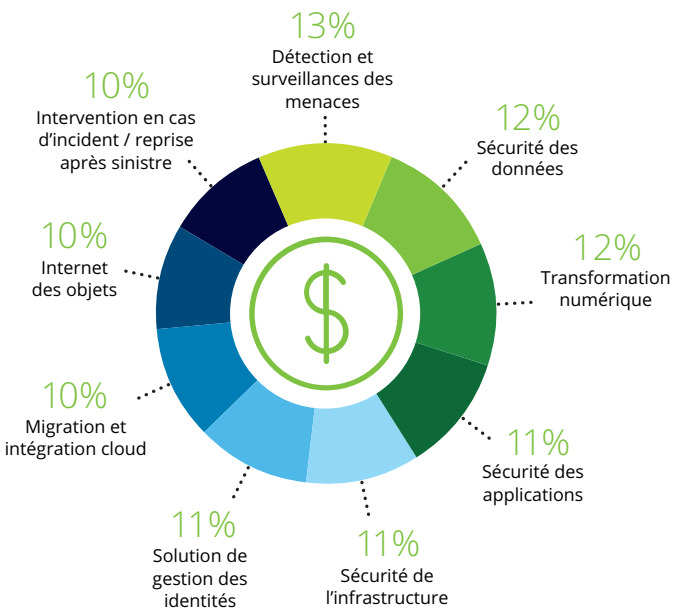
Maintenant que le numérique s'implante partout, des points de contacts avec la clientèle aux usines intelligentes en passant par les appareils à distance des employés, l'ère où le service IT gère des logiciels antivirus et des mots de passe est derrière nous. Maintenir le fonctionnement du réseau n'est plus suffisant. Il faut adopter une pensée plus large et plus profonde.

Les responsables de la sécurité de l'information d'aujourd'hui doivent avoir le pouvoir d'influencer toutes les lignes de services, de recueillir de l'information dans l'ensemble de l'entreprise et d'être en mesure de communiquer directement avec le conseil d'administration et la direction générale. Ils doivent de plus pouvoir orienter les investissements dans les ressources et les talents afin de protéger adéquatement les priorités et les actifs les plus stratégiques de l'entreprise.

Convaincre le directeur administratif et financier du bien-fondé de tels investissements n'est pas facile, car le résultat d'une somme bien investie dans la cybersécurité est souvent invisible : zéro cyberincident. Alors, comment les responsables de la sécurité de l'information planifient-ils leur budget de cybersécurité ? En 2019, les responsables de la sécurité de l'information et les directeurs des systèmes d'information nous ont indiqué que leur budget de cybersécurité était également réparti entre divers programmes. En 2021, cela n'a pas changé – les responsables de la sécurité de l'information et les directeurs des systèmes d'information indiquent une répartition similaire de leur budget. Les hauts dirigeants doivent comprendre qu'il n'existe pas de solution instantanée pour gérer les cyberrisques.

Par conséquent, les budgets de cybersécurité augmentent et sont consacrés notamment aux renseignements sur les menaces, à leur détection et à leur surveillance, à la transformation de la cybersécurité et à la sécurité des données. Partout dans le monde, les responsables de la sécurité de l'information et les directeurs des systèmes d'information investissent continuellement dans des solutions de cybersécurité de type cloud, la cyberrésilience ou la résilience technique, et l'évaluation et l'identification des menaces fondées sur l'IA afin d'établir le système de défense de leur organisation.

Le budget de cybersécurité des organisations est réparti à peu près également pour se protéger des risques de manière générale.



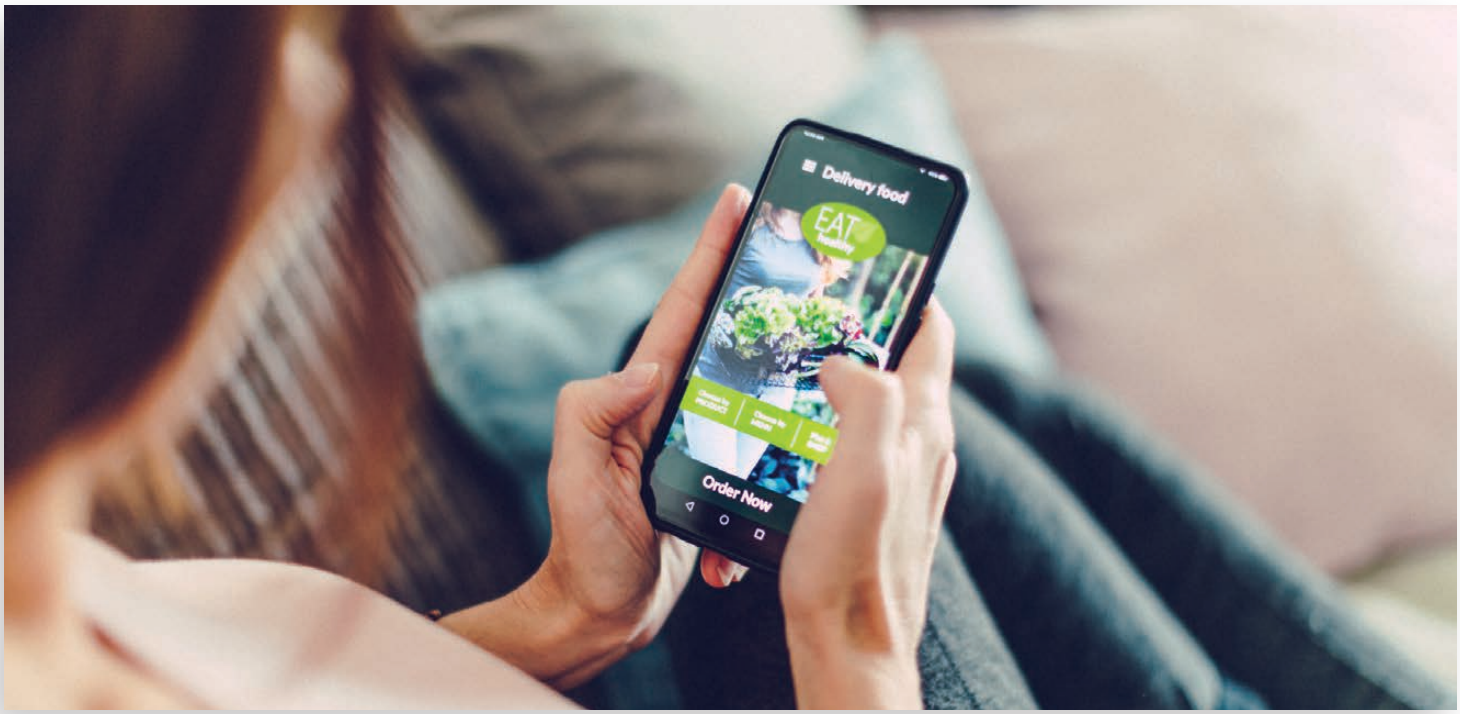
Constituer la bonne équipe de cybersécurité

Il n'est pas réaliste de s'attendre à ce que les membres du conseil d'administration ou de la direction générale deviennent des spécialistes en cybersécurité. Mais le conseil d'administration peut établir une équipe de cybersécurité transparente qui lui fournit l'information pertinente sous une forme compréhensible. Les décisions d'embauche clés doivent être prises au niveau du conseil d'administration ou de la direction générale.

Individualisées ou intrusives ? Utiliser les données personnelles avec éthique

Les gens recherchent des expériences personnalisées et ciblées. Nous aimons que tous nos services allant des livraisons de repas, aux voyages et aux soins de santé soient simples et fondés sur nos interactions antérieures. Mais nous ne voulons pas avoir l'impression d'être suivis à la trace par des spécialistes du marketing qui nous enverront une quantité infinie de coupons pour des choses qui ne nous intéressent pas.

La façon dont les entreprises gèrent les données des clients, relient les expériences en ligne et en personne et protègent les données confidentielles peut déterminer si elles feront des bénéfices ou des pertes, et même si elles survivront à long terme.



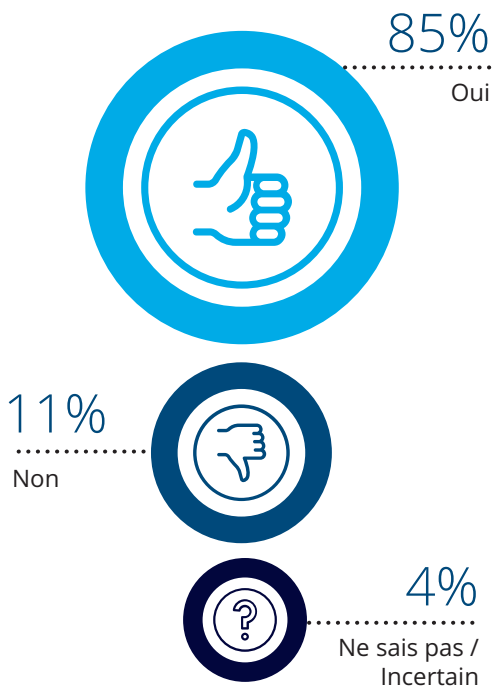
Protection des données dès la conception

Pour chaque projet incluant une interaction avec les clients, il est important de tenir compte de la protection des renseignements personnels et de la sécurité dès le départ. Demandez-vous dans quelle mesure votre business model repose-t-il sur ce niveau d'intimité avec vos clients. Prenez soin de réfléchir au type d'information dont vous avez besoin pour fournir un niveau adéquat de service. Assurez-vous ensuite de comprendre qui devra y accéder et comment l'information sera conservée et protégée. Lorsque nous avons demandé aux directeurs marketing s'ils étaient en mesure de mesurer et de démontrer le niveau de conformité avec les réglementations mondiales en matière de protection de renseignements personnels dans leur entreprise, la majorité (85 %) a répondu affirmativement.

Éviter l'excès de données

Recueillir de grandes quantités d'information en espérant qu'elles serviront plus tard sollicite inutilement des ressources et risque de nuire à votre réussite. Les clients sont réticents à fournir des renseignements s'ils n'y voient pas d'avantages. À l'opposé, une collecte et une utilisation efficaces de données pour créer des expériences authentiques, personnalisées et humaines peuvent agir comme catalyseur de la croissance. Mais plus vous recueillez des données, plus vous courez de risques. C'est une question d'équilibre. Lorsqu'on leur a demandé s'ils trouvaient plus important de recueillir des données pour personnaliser l'expérience client ou de limiter la collecte de données pour mieux se protéger contre les atteintes à la sécurité, les directeurs marketing se sont révélés divisés également entre les deux options.

Êtes-vous capable de mesurer et de démontrer que votre entreprise agit conformément aux réglementations mondiales en matière de protection des renseignements personnels ?



Valeur et confiance

Aujourd'hui, les gens sont conscients que leurs données personnelles ont une valeur intrinsèque. Les fournir est pour eux un investissement pour lequel ils veulent obtenir en retour un service qui leur facilite la vie. Comme tout ce qui a de la valeur, les données personnelles doivent être en sécurité. C'est pourquoi les consommateurs exigent que des organismes y voient, et veulent pouvoir décider comment et quand leurs données seront utilisées. Lorsque les entreprises sont fiables et respectent leurs promesses, elles approfondissent leurs relations avec leurs clients.

Le comportement de vos clients reflète la mesure de leur confiance. Il existe une étroite corrélation entre une confiance élevée et des achats répétés. Lorsqu'un client croit qu'une entreprise est fiable, il a 540 % plus de chances d'acheter de nouveau. Autre facteur important, il défendra également cette entreprise dans les médias sociaux. Par conséquent, les entreprises de confiance affichent un rendement beaucoup plus élevé que les autres. Par exemple, au cours de la dernière année, les entreprises de confiance ont présenté une résilience 2,5 fois plus élevée.

Notre enquête a révélé que 91 % des directeurs marketing considèrent que leur organisation assure « très bien » ou « plutôt bien » l'équilibre entre la collecte de données et l'établissement de la confiance. Un tel niveau de confiance nous amène à nous demander si les autres hauts dirigeants partagent ce point de vue. Il requiert certainement une approche collaborative pour s'assurer de ne pas négliger les angles morts.

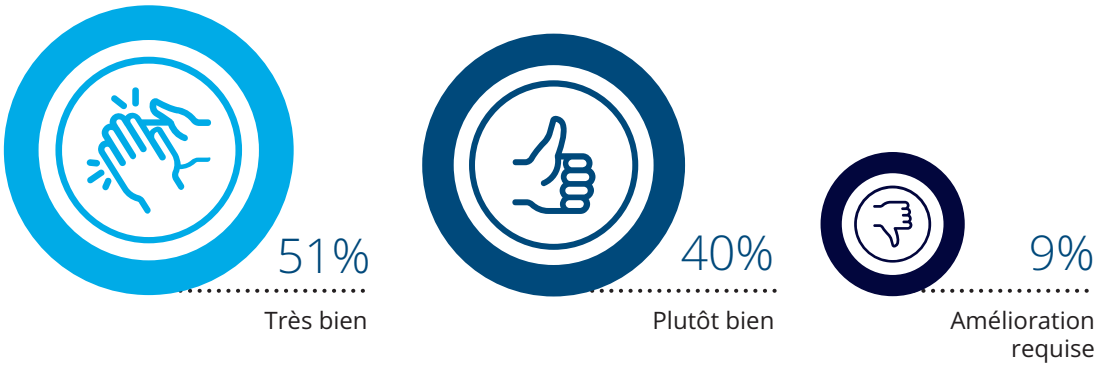
L'éthique avant la réglementation

De plus en plus, les consommateurs utilisent leur pouvoir d'achat pour soutenir les entreprises qui appliquent des politiques environnementales durables et interviennent activement à l'égard d'enjeux sociaux. Ils se préoccupent également de la manière dont les entreprises utilisent les données personnelles.

Traditionnellement, les entreprises se sont fondées sur les exigences des organismes de réglementation pour savoir ce qu'elles devaient faire ou non. Bien qu'il soit essentiel qu'elles se conforment aux diverses lois à l'échelle mondiale, elles ne doivent pas simplement présumer que les consommateurs sont prêts à partager leurs données personnelles sans qu'elles aient à en expliquer la raison. De plus, les explications doivent être formulées de manière simple et facile à comprendre.

Peu importe le lieu, les entreprises qui intègrent la confiance dans leur ADN et communiquent clairement leur volonté à respecter le droit à la protection des renseignements personnels des consommateurs bénéficient d'une plus grande loyauté. Même la plus simple entente d'utilisateur devrait assurer aux clients un moyen facile d'accéder à leurs données, de les supprimer ou de les déplacer. Lorsque les consommateurs constatent qu'une entreprise réfléchit à sa politique de gestion des données et établit sa propre feuille de route, ils sont plus enclins à lui confier leurs données.

Selon vous, dans quelle mesure croyez-vous que votre service de marketing assure un équilibre entre la collecte de données et l'établissement de la confiance auprès des consommateurs ?



*Recherche effectuée par Deloitte et HX TrustID (octobre 2020 à juin 2021)

Misez sur la confiance en tant qu'avantage concurrentiel

Décrivez l'expérience que vous essayez de créer et assurez-vous de comprendre les données dont vous avez besoin (ou non) pour y arriver. Tenez toutes les personnes de votre organisation responsables d'établir la confiance.

01 Commencez par la protection des données dès la conception

02 Utilisez les données que vous recueillez. Ne recueillez pas des données inutiles.

03 Éliminez les cloisons afin que l'information soit accessible et circule librement dans votre organisation.

04 Créez des expériences sans heurt qui inspirent la confiance.

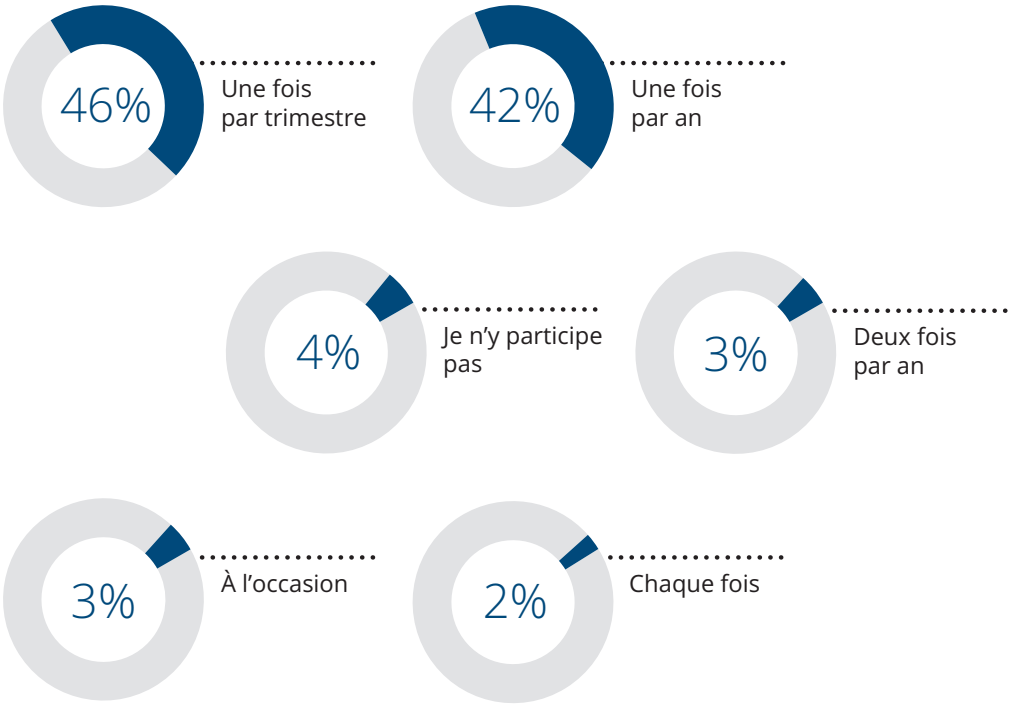
05 Si la sécurité est compromise, utilisez l'incident pour apprendre et générer encore plus de confiance à partir de vos erreurs.

06 Veillez à intégrer votre service des communications dans tout ce que vous faites.

Abolir les cloisons

Les directeurs marketing et les directeurs de l'expérience client ont tendance à prendre des décisions en se basant sur la marque et les besoins de la mise en marché, et c'est seulement à la fin qu'ils vérifient auprès du responsable de la sécurité de l'information si les données ont été recueillies correctement (et habituellement, la réponse est « Non ! »). Tout le monde est dans une équipe différente. Une équipe pense que son travail consiste à recueillir le plus de données possibles, et l'autre s'occupe de les protéger seulement lorsque c'est nécessaire. Une meilleure approche consiste à examiner ensemble comment établir le bon équilibre entre la collecte des données qui sont nécessaires pour fournir une expérience client sans heurt et la nécessité d'atténuer les risques à la fois pour l'entreprise et ses clients. Avant d'utiliser les données pour créer l'expérience client, les organisations ont besoin de gens qui cessent de travailler en vase clos et établissent des liens en dehors de leur équipe. Il s'agir d'une voie à double sens. Lorsque vous élaborez des politiques de protection des renseignements personnels et des plans de communication, demandez la participation du service de marketing, car cela est étroitement lié à la marque et au message.

À quelle fréquence participez-vous à la planification et aux essais des mesures d'intervention en cas d'incident de votre organisation ?



En cas d'incident

Malgré toutes les précautions possibles, des fuites de données peuvent se produire. Il est sage de considérer cet événement comme une éventualité et de s'y préparer, car être pris au dépourvu serait encore pire. La façon dont vous réagissez à un tel événement envoie un signal clair à propos de votre image. Non seulement vous devriez faire une répétition de votre plan d'intervention en cas d'incidents et demander à votre équipe de cybersécurité de mettre des scénarios de compromission de données à l'essai, mais vous devriez aussi travailler en collaboration pour élaborer un plan de reprise après sinistre et une stratégie de communication connexe.

Selon notre enquête, 46 % des directeurs marketing qui voient à harmoniser leur travail avec celui de leur service de cybersécurité indiquent participer à la planification et aux essais une fois par trimestre. Les réponses varient à l'échelle mondiale : les directeurs marketing de l'Argentine, de l'Allemagne et de l'Australie indiquent un meilleur niveau d'intégration de leur travail avec celui des équipes de cybersécurité que ceux des autres pays.

Lorsqu'une fuite de données se produit, vous devriez y voir une obligation d'informer pleinement le client de ce qui s'est produit. Décrivez clairement les services que vous fournissez pour réagir à la situation et réfléchissez aux canaux de communication qui conviennent le mieux à votre message : la situation exige-t-elle une lettre personnelle de votre dirigeant ? Un cadeau ? Une autre compensation ?

Malgré la gravité de la situation, si vous communiquez adroitement avec vos clients, vous aurez peut-être la possibilité d'approfondir votre relation avec eux. Le fait de bien gérer une situation difficile en mettant l'intérêt de vos clients en priorité peut vous aider à rétablir votre réputation rapidement et même à inspirer une confiance encore plus grande.

> "En matière de confidentialité, de sécurité et d'identité, les clients ne pensent pas à leurs données comme le font les entreprises. Ils se demandent : « L'entreprise agit-elle dans mon intérêt ? Utilise-t-elle mes données d'une manière avantageuse pour moi ou pour elle ? Fait-elle tout ce qu'elle peut pour protéger mes renseignements personnels ? "
>
> — ANNIKA SPONSELEE, LEADER MONDIALE, DONNÉES ET RENSEIGNEMENTS PERSONNELS, CYBERSÉCURITÉ DELOITTE

Créer un monde sans frontières

Dans les environnements traditionnels, les ressources IT étaient utilisées à l'intérieur de frontières clairement définies. Tout ce qui se trouvait à l'extérieur était considéré comme non fiable, et le trafic interne bénéficiait souvent d'une confiance inhérente. Mais qu'en est-il aujourd'hui ? Nous vivons dans un monde hyperconnecté, où tout est de plus en plus interrelié. Pour une bonne part des entreprises modernes, le périmètre s'est essentiellement dissous.

Parmi les répondants de notre enquête, 72 % ont indiqué que leur organisation a subi entre un et dix cyberincidents et fuites de données au cours de la dernière année uniquement. Aujourd'hui, le défi est d'oublier complètement le principe de confiance inhérente. Il s'agit d'un changement révolutionnaire dans la façon de concevoir les architectures de sécurité modernes. Heureusement, le modèle zero trust permet de le faire.

Facteurs favorisant le passage au principe de zero trust

01 Le rythme rapide de la numérisation accroît la complexité des systèmes d'informations et fait monter les coûts.

02 Une main-d'œuvre de plus en plus mobile s'attend maintenant à pouvoir travailler de n'importe où, avec n'importe quel appareil.

03 Le développement de produits et de services numériques s'oriente vers l'adoption du cloud.

04 La demande d'améliorer et de faciliter la collaboration.

05 Les concurrents adoptent un modèle plus sophistiqué qui surpasse les pratiques de cybersécurité actuelle.

Le modèle zero trust

Le modèle zero trust n'est pas une technologie ou une solution unique. Il s'agit d'un ensemble de lignes directrices architecturales basées sur le principe fondamental « ne jamais faire confiance, toujours vérifier ». Ce concept abandonne la vision traditionnelle de la gestion de la sécurité fondée sur le périmètre, ou une approche « château et douves », pour un modèle où la confiance est établie entre les ressources individuelles et les consommateurs de la façon et au moment où cela est nécessaire. Avec le modèle zero trust, les connexions de confiance sont établies sur la base de facteurs internes et externes qui sont constamment revérifiés.

Contrôle des accès en temps réel

Finalement, nous avons la capacité de calculer et la technologie pour éclairer les décisions de contrôle d'accès dynamiques est fondée sur les risques en temps réel.

Le contrôle des accès ne se limite plus à autoriser ou à refuser. Chaque demande de connexion peut être vérifiée par rapport à un ensemble de facteurs contextuels afin de prendre une décision d'accès fondée sur les risques :

- La demande de connexion provient-elle d'un utilisateur authentifié et autorisé ?
- Provient-elle d'un appareil connu et sécurisé ?
- Cette personne se connecte-t-elle habituellement à partir de ce lieu géographique ?
- L'heure de connexion correspond-elle à l'historique de l'utilisateur ?
- Y a-t-il d'autres signaux ou renseignements sur les menaces qui devraient être pris en considération avant d'accorder l'accès ?

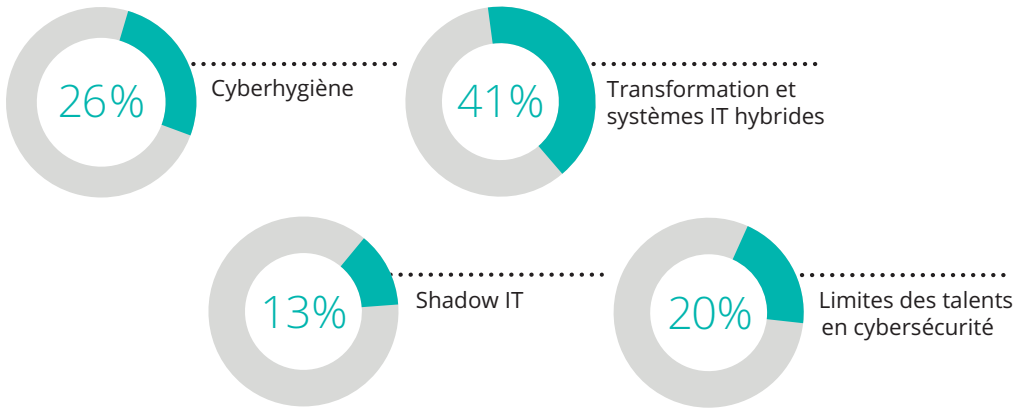
"On croit, à tort, que le fait d'adopter le principe de zero trust exige de tout jeter et de remplacer. Il est important de prendre du recul et de réfléchir de manière stratégique à l'approche itérative et par étapes à adopter pour atteindre la situation voulue."

— ANDREW RAFLA, LEADER ZERO TRUST, ÉTATS-UNIS, CYBERSÉCURITÉ DELOITTE

La situation actuelle

Notre enquête cerne les difficultés liées à la gestion des cyberrisques auxquelles les directeurs des systèmes d'information et les responsables de la sécurité de l'information font face dans leur entreprise. Leurs plus grands défis sont la transformation et les systèmes d'information hybrides, suivis de près par la cyberhygiène, les limites des talents et les technologies parallèles. Ces défis ne feront que se complexifier encore plus avec les transformations numériques qui s'accélèrent. Nous devons repartir du début et concevoir des architectures de sécurité pouvant soutenir le rythme croissant de la transformation numérique. C'est maintenant qu'il faut agir !

Parmi les éléments suivants, quel est le plus grand défi de gestion de la cybersécurité que présente l'infrastructure de votre organisation ?



Étape par étape

La plupart des entreprises, sciemment ou non, ont entamé un parcours zero trust. Leur approche peut être tactique, architecturale ou stratégique, à divers degrés. Bien que le modèle zero trust soit pertinent pour tous les secteurs d'activité, il n'existe pas de solution universelle. Une initiative zero trust doit se dérouler sur plusieurs années. Il s'agit d'un changement transformationnel où l'on doit éliminer les cloisons entre les fonctions liées aux affaires, aux IT et aux divers domaines du numérique. Tout parcours de zero trust rencontrera des obstacles qui nécessiteront un soutien solide de la direction, des investissements importants et l'adhésion de toute l'organisation pour réussir.

Plusieurs aspects doivent être pris en considération, comme les catalyseurs de l'entreprise, les capacités existantes et les cas d'utilisation pertinents pour votre organisation. Comme toujours, il est important de garder en tête les principes fondamentaux de la cybersécurité : Que tentez-vous de protéger ? Où se trouvent ces actifs ? Qui (identités) et quoi (appareils) devraient être en mesure d'accéder à ces actifs, et selon quelles modalités ? Pour répondre à ces questions fondamentales, les organisations doivent établir un ordre de priorité parmi les capacités de gestion des actifs IT et de gouvernance des données afin de comprendre la classification et l'importance de leurs actifs et de leurs données… et se baser sur ce contexte lors de l'élaboration des politiques de contrôle des accès. Par la suite, la manière la plus sûre d'atteindre les résultats que vous visez consistera à définir vos objectifs et à les intégrer dans votre stratégie de bout en bout. Toutefois, cela n'est pas facile. Lorsque nous avons demandé aux répondants quel était le plus grand défi de gestion de la cybersécurité dans leur organisation, l'élément le plus cité fut « l'augmentation de la gestion des données et le périmètre et la complexité ».

Plus qu'une solution technologique, le modèle de zero trust est un changement culturel qui touche l'ensemble de l'organisation et ne doit pas être sous-estimé. D'autres facteurs, comme la communication, la formation ciblée selon le rôle, la sensibilisation et la modification des processus opérationnels sont des éléments clés de la réussite. Dans l'ensemble, de tels programmes nécessitent une stratégie harmonisée à la vision de l'entreprise, soutenue par une direction solide, une architecture spécialisée, des flux de travail techniques et des projets pilotes stimulants qui mobilisent l'engagement de toutes les parties prenantes.

L'étoile Polaire

Des géants du secteur des technologies mènent l'aventure « zero trust » et en appliquent les principes pour élaborer et fournir des services de sécurité. D'autres organisations adoptent des stratégies zéro trust pour soutenir leurs priorités business, leur transformation numérique et leurs stratégies de gestion des risques d'entreprise. Au moment de moderniser votre propre architecture, le fait de comprendre comment des leaders ont innové et obtenu des résultats extraordinaires peut vous aider à réussir vous aussi votre transformation numérique. Il est indéniable que des changements se produisent. Plus vite vous prendrez en main votre transition vers le modèle zero trust, plus votre parcours sera sûr. Il vaut mieux prendre les commandes et choisir sa destination. C'est maintenant qu'il faut adopter la stratégie « zero trust ».

Avantages considérables

Intégré dans la stratégie de l'entreprise, le modèle de zero trust peut procurer de nombreux avantages stratégiques. En réduisant la complexité opérationnelle et en simplifiant l'intégration de l'écosystème, il peut :

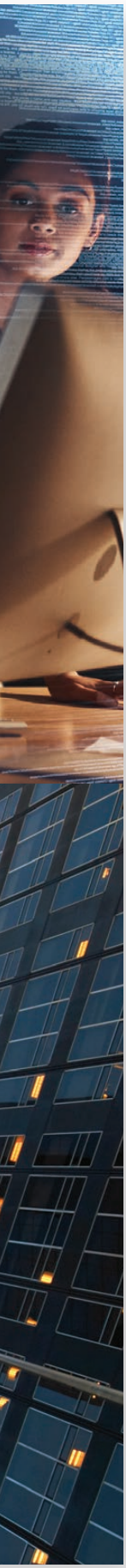
- **améliorer l'expérience client**
- **rehausser l'agilité de l'entreprise**
- **améliorer la résilience de l'entreprise**
- **réduire la superficie de la zone de menace**
- **réduire les coûts**
- **améliorer la collaboration avec les partenaires d'affaires**
- **accélérer l'adoption du cloud**

"Il est temps de tirer pleinement profit des principes de zero trust et d'établir des architectures de sécurité modernes qui peuvent suivre le rythme et permettre la transformation numérique."

— MARIUS VON SPRETI, LEADER MONDIAL, ZERO TRUST, CYBERSÉCURITÉ DELOITTE

"De nombreuses organisations sous-estiment les risques associés à la connexion des technologies déjà présentes dans leur environnement. La surface d'attaque augmente dans tout l'écosystème."

— DANA SPATARU, LEADER MONDIALE, TECHNOLOGIES ÉMERGENTES EN CYBERSÉCURITÉ, CYBERSÉCURITÉ DELOITTE



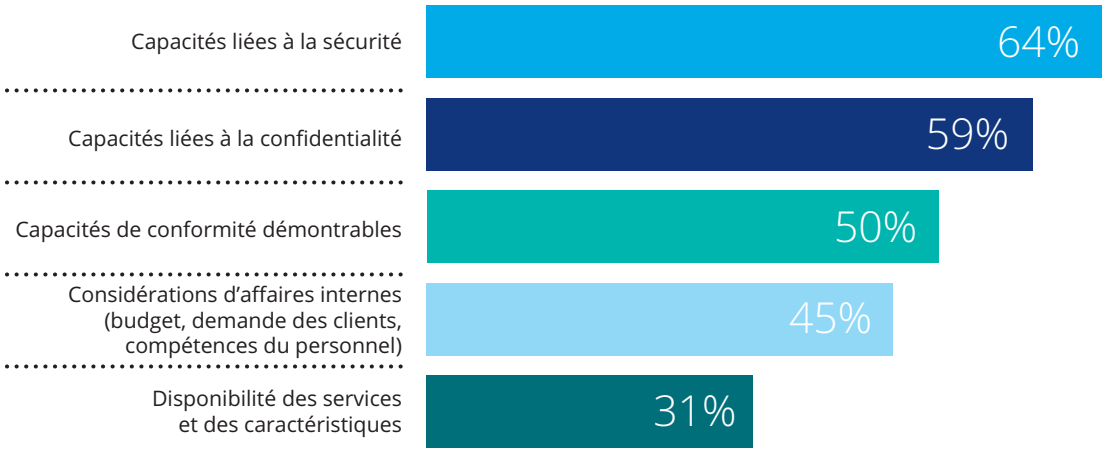
Connecter le spectre des technologies émergentes

Les grands titres de l'actualité se concentrent souvent sur les technologies de pointe comme l'informatique quantique, le réseau 5G et les jumeaux numériques, mais le spectre entier inclut également les technologies de développement de capacités existantes, comme la technologie opérationnelle, employée depuis des décennies dans le secteur de la fabrication.

Que l'on parle de technologies nouvelles ou utilisées depuis des années, l'aspect émergent de la technologie concerne la connexion à internet et la manière dont les mondes physique et numérique deviennent connectés de presque toutes les façons imaginables. Nous sommes témoins d'une métamorphose numérique dans tous les domaines : appareils médicaux, transports, agriculture, etc. Non seulement cela transforme la manière dont nous fabriquons et utilisons pratiquement tout, mais cela entraîne des risques à la sécurité auparavant inconcevables.

Lorsque nous avons demandé aux directeurs des systèmes d'information et aux responsables de la sécurité de l'information d'indiquer, dans l'ordre, quels seraient les facteurs qui favoriseraient le plus leur adoption de technologies émergentes dans les trois prochaines années, ils ont mentionné en premier lieu les capacités liées à la sécurité (64 %), puis les capacités d'amélioration de la confidentialité des données (59 %), et enfin les capacités de conformité (50 %).

Parmi les éléments suivants, lesquels vont favoriser l'adoption de technologies émergentes ? *



*Les participants pouvaient sélectionner toutes les réponses pertinentes, c'est pourquoi les pourcentages ne totalisent pas 100 %.

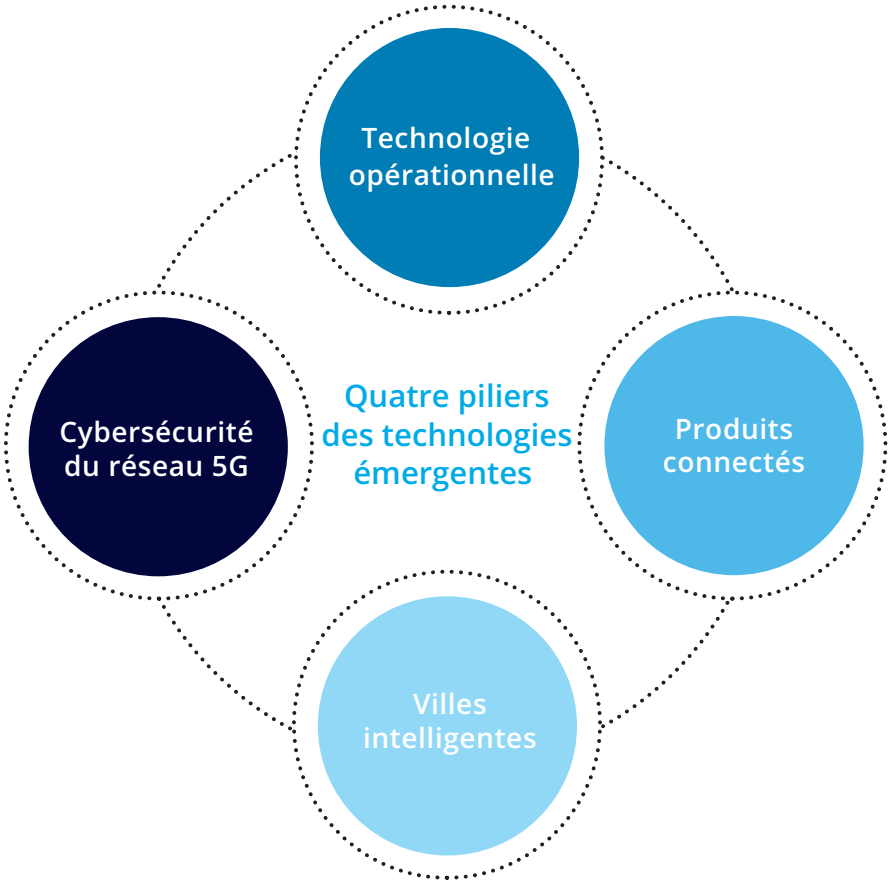
Connectivité croissante

Traditionnellement isolés de l'internet, les réseaux de technologies opérationnelles ont subi récemment des vagues d'attaques de logiciels de rançon. Les effets immédiats sur la production ont mis en lumière les vulnérabilités de la connectivité, une situation exacerbée par la COVID-19, car plus d'entreprises ont fait le choix de gérer des usines et du matériel à distance.

Il est important de comprendre que tous les écosystèmes connectés, qu'il s'agisse d'appareils médicaux, de véhicules ou de villes entières, présentent des caractéristiques de risques similaires. Des appareils médicaux conçus pour fonctionner avec les anciennes plateformes sur place dans les hôpitaux sont aujourd'hui utilisés à domicile par la voie de l'internet. Les voitures électriques, qui doivent remplacer rapidement les flottes de véhicules à combustibles fossiles partout dans le monde, exigent souvent d'être connectées pour être activées. Ces véhicules connectés nécessitent des pièces d'une foule de fournisseurs dispersés dans différentes régions, et qui n'ont pas nécessairement intégré la sécurité dans leur conception. Les villes connectent de plus en plus leurs services et leurs infrastructures critiques et établissent des partenariats avec de nombreux tiers, des fournisseurs de services cloud aux exploitants de plateformes. Dans toutes ces situations, la surface d'attaque augmente, les risques se multiplient, et les responsabilités deviennent floues.

Pour simplifier un domaine qui peut comprendre un éventail infini de technologies, le groupe Cybersécurité Deloitte se concentre sur certains aspects précis :

Ces piliers couvrent la vaste majorité des scénarios que nous rencontrons dans notre pratique.



Être au fait de la situation, même si elle n'est pas visible

Pour les organisations entièrement numérisées qui sont de petite taille, il est possible d'avoir une vue d'ensemble des cyberrisques. Mais ce ne sera bientôt plus le cas pour les grandes entités disposant d'écosystèmes interconnectés complexes. La solution est de laisser chaque partie assumer la responsabilité de la sécurité pour les processus qui relèvent d'elle. Si chacun sécurise efficacement une partie de l'écosystème, le risque global diminuera, même si on ne peut en obtenir une vue globale.

L'entité pourra mettre en place une telle solution plus ou moins rapidement selon le type et la complexité des technologies dont elle dispose, mais le but est d'assurer efficacement les besoins de sécurité de base et de partager l'information de manière sûre. Pour l'immédiat, il s'agit d'un changement simple à faire. À plus long terme, les organisations devront garder à l'esprit que si elles voient à uniformiser les processus à l'échelle des lignes de services, elles pourront faire des gains d'efficacité importants. Plus vite elles procéderont à cette uniformisation, plus vite elles permettront à leur système de sécurité d'atteindre une grande maturité. Des modèles centralisés et décentralisés peuvent présenter la même efficacité, mais il faudrait en fin de compte les combiner pour obtenir une vision globale intégrée des cyberrisques.

Le cœur de l'entreprise

Du point de vue de la gouvernance, les infrastructures de technologies émergentes peuvent être très complexes, mais quelqu'un doit assumer la responsabilité du programme de sécurité. La reconnaissance et le soutien du conseil d'administration aident non seulement à faciliter l'acquisition et la gestion des technologies, mais aussi à établir les bons partenariats stratégiques. Comme les technologies émergentes sont étroitement liées aux activités de base de l'entreprise, contrairement aux systèmes d'information IT traditionnels, cela facilite les choses.

Par exemple, si le réseau OT d'une entreprise manufacturière subit une cyberattaque, il est évident que le problème ne restera pas seulement celui du responsable de la sécurité de l'information. Si la production est paralysée, le chef de l'exploitation s'en préoccupera immédiatement, les pertes de revenus alerteront le directeur administratif et financier et le dirigeant, la publicité négative exigera l'intervention du directeur marketing, et ainsi de suite.

La sécurité vue comme un actif

Le scénario précédent illustre le fait que les technologies émergentes ont l'avantage de rendre les effets positifs de la cybersécurité plus évidents aux yeux des dirigeants d'entreprise. Si un directeur marketing veut vendre plus de produits, le fait d'y intégrer des éléments de sécurité en fera des produits plus attrayants dans notre monde de plus en plus connecté. Dans cette optique, la sécurité est perçue moins comme un coût, et plus comme une façon de créer de la valeur. On peut alors faire valoir que le besoin de réduire les temps d'arrêt commande l'amélioration des processus. La sécurité, bien sûr, est nécessaire et fondamentale, mais devient un argument secondaire.

> "Contrairement aux idées reçues, les récentes cyberattaques majeures ne sont pas attribuables à des stratagèmes très sophistiqués. La plupart s'expliquent par un manque de contrôles de sécurité de base et une cyberhygiène insuffisante, qui ne sont pas nécessairement compliqués à mettre en place."
>
> — DANA SPATARU, LEADER MONDIALE, TECHNOLOGIES ÉMERGENTES EN CYBERSÉCURITÉ, CYBERSÉCURITÉ DELOITTE

Il n’existe pas de solution unique

Dans tous les secteurs, les cyberrisques trônent parmi les trois principaux types de risques d’entreprise, tant du point de vue des membre du comité exécutif et du comité de direction que de ceux qui gèrent ces risques. On comprend de mieux en mieux comment la propriété intellectuelle est vulnérable, et la confiance des clients, fragile.

Cependant, selon le secteur, la transformation numérique s’opère dans le cadre de réglementations de maturité variable entourant la cybersécurité et un éventail de particularités géographiques et autres. Même si des réalités communes ont émergé pendant la pandémie, comme la sécurité de la chaîne d’approvisionnement et le télétravail accélérant la nécessité du modèle de zero trust, il n’existe pas de solution unique pour relever le défi de la cybersécurité.

Peu importe la direction que vous prenez, vous devez être au fait de domaines d’intérêt qui prennent de plus en plus d’importance. De nombreux gouvernements intensifient la mise en place d’exigences réglementaires pour lutter contre la hausse des cybermenaces, rendant la mise en œuvre d’initiatives de sécurité de pointe impérative. Là où le changement n’est pas imposé par la réglementation, c’est la connectivité croissante et la personnalisation de la technologie qui poussent à modifier l’architecture des écosystèmes sur la base de la sécurité. Finalement, le constat que tous les secteurs sont vulnérables entraîne un plus grand échange de connaissances. Il deviendra de plus en plus pertinent de s’adapter et d’apprendre ce qui fonctionne dans les autres secteurs.

Explosion des réglementations

Dans certains secteurs, les cyberattaques ont déclenché une réponse réglementaire démesurée. La récente attaque de rançongiciels qui a frappé Colonial Pipeline, le plus important fournisseur d’essence, de diesel et de kérosène sur la côte est des États-Unis, a entraîné un nouveau décret présidentiel et de nouvelles directives exigeant des sociétés d’énergie d’améliorer leur cybersécurité.

Dans le secteur Énergie, ressources et produits industriels, la pression d’améliorer les programmes de cybersécurité s’ajoute à d’autres directives à plus long terme, comme le passage à la décarbonation. Avec des échéances serrées – les États-Unis visant maintenant l’année 2035 –, la transformation du secteur de l’énergie nécessitera une formidable numérisation pour atteindre ses objectifs. Cela inclura le passage à la technologie 5G et le déploiement d’un éventail de technologies connectées, qui accroîtront le besoin de cybersécurité.

Leçons apprises de l'attaque de logiciels de rançon de Colonial Pipeline

Planifiez la crise de manière proactive. Préparez-vous à des scénarios de perturbation technologique incluant les cyberincidents :

- Déterminez les actifs qui sont essentiels pour vos opérations et pourraient être des cibles attrayantes
- Segmentez vos systèmes essentiels et votre réseau OT
- Accélérez l'adoption du modèle zero trust
- Augmentez la résilience de votre entreprise : accordez autant d'importance aux mesures d'intervention qu'à la prévention et à la détection

Passez à l'offensive. Les principes de sécurité modernes comme la recherche active de menaces, le machine learning et les systèmes capables d'autoréparation peuvent vous aider à appliquer une approche offensive.

"La direction doit réfléchir à la cybersécurité dès le départ, à l'étape de la conception du changement. Quelles données et quels actifs feront partie du changement ? De quelles technologies avez-vous besoin pour les protéger ?"

— SIMON OWEN, LEADER SECTORIEL, CYBERSÉCURITÉ DELOITTE

Personnalisation accrue. Risques accrus

Dans le secteur des sciences de la vie et des soins de santé, un nouveau modèle d'interaction directe avec les clients entraîne la nécessité d'accroître la cybersécurité. Alors que les fournisseurs de soins de santé cherchent à suivre les progrès des bénéficiaires et que les sociétés des sciences de la vie privilégient les services axés sur le patient pour améliorer les résultats de santé, l'utilisation d'appareils et d'applications à distance soulève des préoccupations concernant la protection des données et la confidentialité.

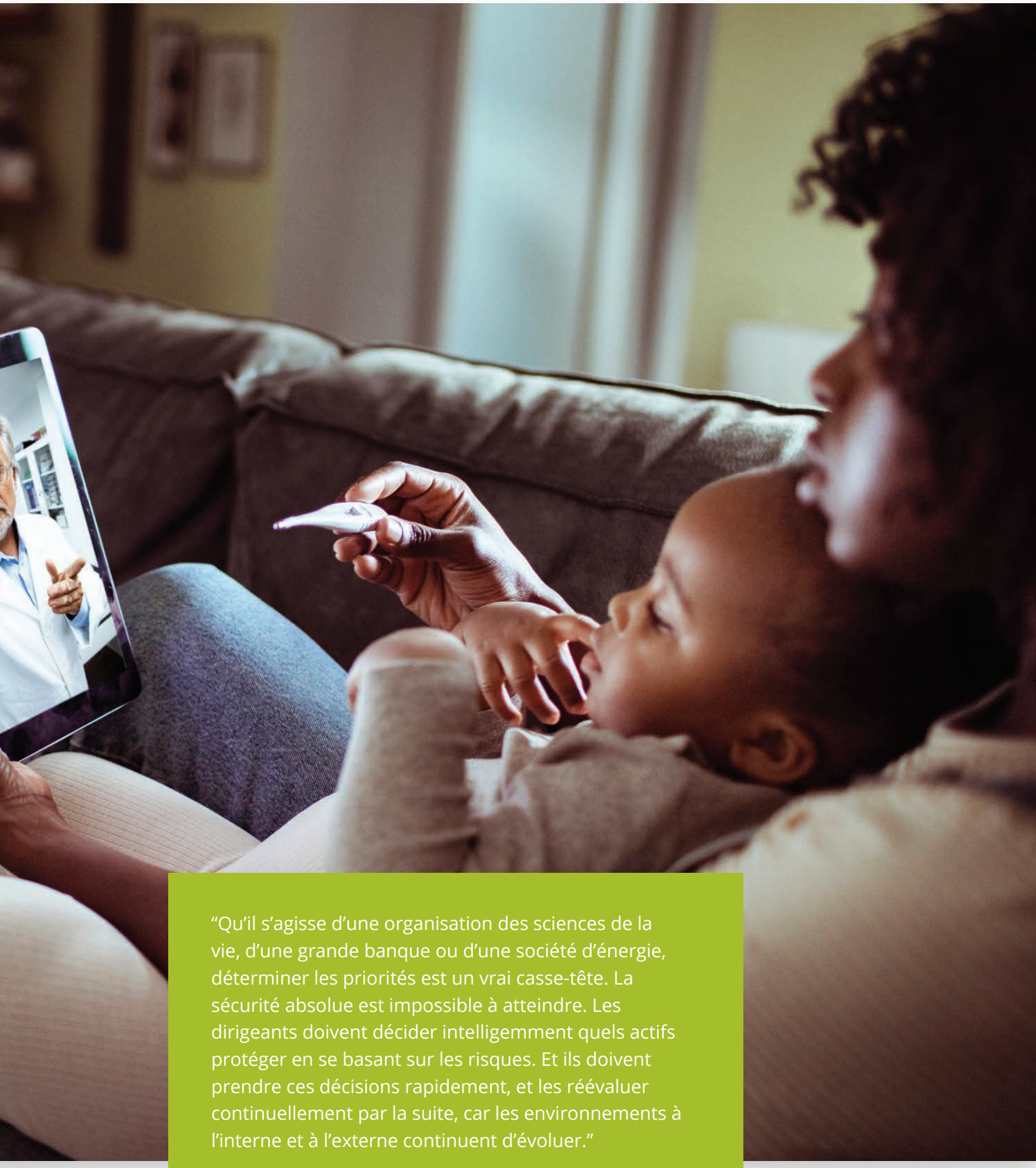
Cette surveillance et cette utilisation d'applications entraînent une accumulation rapide de données agrégées permettant aux entreprises de créer des datalakes cloud afin de recueillir de l'information pouvant mener à des améliorations sur le plan de la R&D, des traitements et du soutien, de l'adhésion des patients et du lancement de produits. Tous ces progrès technologiques ont des conséquences sur la cybersécurité. Les écosystèmes doivent être conçus et établis de manière à protéger, à chiffrer et à anonymiser les données, et à prévenir les fuites.

En général, les entreprises du secteur des sciences de la vie à l'échelle mondiale craignent plus d'être victimes d'une cyberattaque que d'être aux prises avec des problèmes liés aux réglementations, qui varient souvent d'un territoire à un autre. Ainsi, pour elles, maintenir la confiance lorsqu'elles se connectent avec leurs clients est essentiel, et protéger la propriété intellectuelle est primordial.

Partage de connaissance

L'omniprésence des cybermenaces et les vulnérabilités qui ont été exposées pendant la pandémie ont eu des répercussions sur la manière dont les connaissances sont partagées dans les secteurs. Bien que les atteintes à la réputation soient un effet secondaire des attaques, le partage de l'information à propos des incidents est vu comme valable et utile, et souvent perçu comme une mesure de rédemption qui aide à rétablir la réputation de la marque. Les entreprises ont pris conscience que ne pas faire preuve de transparence à l'égard de la cybersécurité ne leur confère pas un avantage concurrentiel, mais peut en fait compromettre leur secteur en entier.

Les gouvernements ont reconnu l'importance d'établir une défense collective, et aident à établir des partenariats public/privé pour le partage de l'information, comme les Information Sharing and Analytics Centers (ISAC) aux États-Unis. D'un point de vue moins formel, les responsables de la sécurité de l'information sont désireux d'apprendre les uns des autres. Même s'il est plus courant pour eux d'échanger avec des pairs de leur secteur, on commence à voir des échanges de pratiques entre des secteurs plus matures comme celui des services financiers et celui du pétrole et du gaz avec des secteurs moins avancés comme les sciences de la vie et le secteur manufacturier. De plus, les responsables de la sécurité de l'information migrent souvent d'un secteur à un autre et apportent leur expérience. Nous espérons voir plus de liens se tisser et plus de partages entre les secteurs et au niveau international dans un avenir proche.

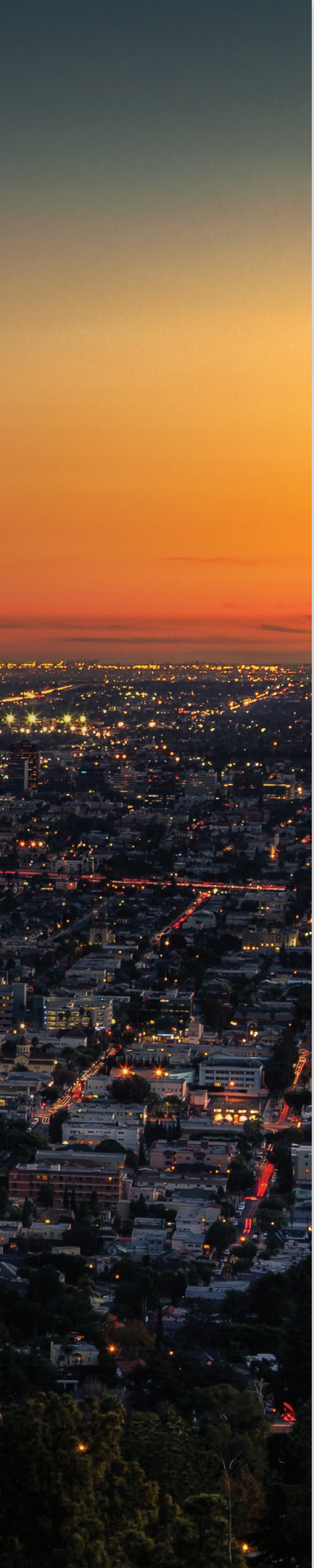


"Qu'il s'agisse d'une organisation des sciences de la vie, d'une grande banque ou d'une société d'énergie, déterminer les priorités est un vrai casse-tête. La sécurité absolue est impossible à atteindre. Les dirigeants doivent décider intelligemment quels actifs protéger en se basant sur les risques. Et ils doivent prendre ces décisions rapidement, et les réévaluer continuellement par la suite, car les environnements à l'interne et à l'externe continuent d'évoluer."

— SIMON OWEN, LEADER SECTORIEL, CYBERSÉCURITÉ DELOITTE

Un champ de vision clair

À mesure que la transformation numérique s'opère dans tous les aspects d'une entreprise, il devient évident que le numérique est à la fois un moteur incroyable qui offre aux personnes et aux processus de nouvelles possibilités, et un moyen d'amplifier et de répandre les risques. Notre enquête, menée pendant une période où les entreprises devaient réagir à un bouleversement mondial sans précédent, s'est avéré particulièrement instructif.



À mesure que la transformation numérique s'opère dans tous les aspects d'une entreprise, il devient évident que le numérique est à la fois un moteur incroyable qui offre aux personnes et aux processus de nouvelles possibilités, et un moyen d'amplifier et de répandre les risques. Notre enquête, menée pendant une période où les entreprises devaient réagir à un bouleversement mondial sans précédent, s'est avérée particulièrement instructive.

Il n'existe pas de solution simple pour bien comprendre la complexité croissante des écosystèmes intégrés sur lesquels sont fondées les entreprises modernes. Cependant, l'utilisation combinée d'un certain nombre de mesures organisationnelles, culturelles et opérationnelles peut permettre de gérer les cyberrisques à la manière des autres risques mieux connus.

Confier la responsabilité aux dirigeants

Le principal constat est sans doute que les organisations qui n'intègrent par la cybersécurité dans tous les aspects de leurs activités risquent de laisser passer une partie de la valeur de la transformation numérique en plus d'augmenter leur vulnérabilité aux attaques.

Notre plus importante recommandation à cet égard est d'accorder une plus grande autonomie au responsable de la sécurité de l'information, notamment en faisant en sorte qu'il reporte directement au PDG. De plus, un tel changement permet également au responsable de la sécurité de l'information d'être au fait de tout ce qui se passe dans l'ensemble des lignes de services. La relation doit être dans les deux sens. Le responsable de la sécurité de l'information doit fournir des évaluations des risques dans une forme compréhensible pour le conseil d'administration. Mais en plus de produire des rapports, le responsable de la sécurité de l'information doit participer aux nouvelles initiatives dès le début de leur élaboration afin de s'assurer d'une gouvernance appropriée de la cybersécurité en aval.

Éliminer les cloisons

À mesure que la technologie permet à l'information de circuler librement dans l'ensemble des organisations, il est également essentiel d'abolir les cloisons pour permettre aux membres des différentes lignes de services de collaborer pour assurer la cybersécurité. Les responsables de la stratégie, du développement de produit, de la conformité, IT et du marketing doivent pouvoir travailler ensemble pour comprendre les actifs qui sont nécessaires et les exigences de sécurité et de protection de la confidentialité qui y sont associées au début de toute nouvelle initiative. Concevoir en ayant la sécurité et la confidentialité en tête est la meilleure façon d'éviter les problèmes plus tard.

Le principe de zero trust

La complexité est une réalité. Recourir aux anciennes méthodes d'authentification des utilisateurs, c'est ouvrir la porte aux pirates et courir au désastre. Heureusement, il est maintenant possible d'intégrer dans les architectures complexes des moyens d'évaluer les risques de manière continue et de faire des vérifications en temps réel.

Le principe de zero trust est une innovation à la fois culturelle et technologique. Amener les gens à modifier leur comportement exige de la communication et de la formation. Le principe de zero trust permet de sécuriser l'exécution des stratégies d'innovation et d'affaires. Il est essentiel que chacun prenne conscience des avantages continus que procure son déploiement pour le soutien de la transformation numérique en constante évolution.

La sécurité vue comme un actif

Les données sont la pierre angulaire de la transformation numérique. Bien qu'il soit essentiel de reconnaître le rôle fonctionnel des données dans la manière dont elles favorisent les résultats de l'entreprise et l'expérience client, il est tout aussi important d'apprécier la valeur qu'elles procurent à long terme. Les entreprises qu'on associe à une gouvernance exemplaire des données, à une politique de protection des données confidentielles réfléchie et à une sécurité solide gagnent la confiance des clients et des partenaires d'affaires. Même si l'on est tenté de percevoir la cybersécurité seulement comme une dépense, tenir compte de son incidence sur l'image et sur le maintien de la valeur des actionnaires est fondamental dans le nouveau monde de l'hyperconnectivité.

Partage des connaissances

Même s'il n'existe pas de solution universelle simple pour gérer la cybersécurité, de plus en plus d'information circule concernant les menaces qui pèsent sur les organisations qui ont emprunté la voie de la transformation numérique. Comme les cyberattaques deviennent plus fréquentes et n'épargnent aucun secteur ni aucun pays, nous pouvons apprendre les uns des autres sur les manières de gérer efficacement un incident lorsqu'il se produit. Dans cette optique, partager nos expériences et nos connaissances avec les pairs est un élément essentiel pour améliorer nos environnements de sécurité.

Risques et récompenses

Peu importe le budget que vous consacrez à la cybersécurité, le fait d'adopter ces approches vous aidera à assurer une utilisation plus efficace de vos ressources.

Il est facile de se concentrer sur la complexité et les nombreux risques que la transformation provoquera, mais il est tout aussi important de le reconnaître. Lorsque vous aurez obtenu la visibilité que vous recherchez, que vous constaterez l'agilité que les systèmes d'information hybrides procurent à votre organisation, que vous aurez gagné la confiance de vos clients et que vous serez confiant par rapport à la manière dont vous gérez la complexité, vous verrez que votre récompense surpasse vos efforts.

Contacts

Imade Elbaraka
Associé responsable des activités cyber pour la France et l'Afrique Francophone

+33 1 55 61 74 64
ielbaraka@deloitte.fr

Kevin Prigent
Directeur, Responsable des activités Cyber en région

+33 1 55 61 79 35
kprigent@deloitte.fr

Auteurs

Emily Mossburg
Leader mondiale de la cybersécurité

+1 571 766 7048
emossburg@deloitte.com

Simon Owen
Leader mondial, Clients et secteurs

+44 20 7303 5133
sxowen@deloitte.co.uk

Annika Sponselee
Leader mondiale, Confidentialité des données et protection de la vie privée

+31882882463
asponselee@deloitte.nl

Dana Spataru
Leader mondiale, Technologies émergentes

+31882888882
dspataru@deloitte.nl

Matthew Holt
Leader mondial, Stratégie et transformation

+393351421906
maholt@deloitte.it

Marius von Spreti
Leader mondial, Zero trust

+49 89 290365999
mvonspreti@deloitte.de

Ashley Reichheld
Leader, Service à la clientèle et marketing, États-Unis

+1 617 449 5067
areichheld@deloitte.com

Andrew Rafla
Leader, Zero trust, États-Unis

+1 201 912 6535
arafla@deloitte.com

Amir Belkhelladi
Associé, Leader de la Cybersécurité, Canada

+1 514 393 7035
abelkhelladi@deloitte.com.ca

Deloitte.