Raconteur

Maîtriser la confiance numérique : un enjeu essentiel pour les dirigeants

digicert®

Contenu

Transformation de la conformité : cinq leviers d'action pour inscrire l'excellence de la sécurité dans la durée

Les nouvelles exigences en matière de cybersécurité redéfinissent les risques commerciaux. Pour les entreprises, ces obligations draconiennes peuvent devenir un véritable facteur de différenciation. Découvrez en cinq étapes comment relever le défi de la conformité à l'ère du tout numérique.

Le monde de l'entreprise vit actuellement une transformation majeure, sur fond de durcissement des règles de cybersécurité et d'apparition de nouveaux régimes réglementaires. Résultat : les organisations sont soumises à une pression sans précédent pour passer d'une posture de sécurité réactive et à une démarche proactive de renforcement de leur compétitivité.

Face à des menaces de plus en plus sophistiquées, la conformité réglementaire est

passée d'une simple contrainte administrative à un véritable facteur de différenciation. Un changement de paradigme que les dirigeants ont parfois du mal à assimiler. Pourtant, c'est maintenant qu'ils doivent agir – et vite.

En gérant de façon proactive leur sécurité numérique, les entreprises ne se protègent pas uniquement des compromissions et des interruptions de services. Elles garantissent également la résilience de leurs opérations pour se conformer aux exigences des nouveaux textes applicables, notamment de la réglementation DORA. Avec la prolifération des menaces numériques, des pratiques de conformité rigoureuses deviennent indissociables d'une bonne gouvernance d'entreprise.

Or, les obligations en la matière vont connaître un profond bouleversement. Entré en vigueur le 17 janvier 2025, le règlement européen DORA (Digital Operational Resilience Act) est appelé à transformer le secteur des services financiers et les systèmes TIC utilisés par ces entreprises.

Outre-Manche, le Cyber Security and Resilience Bill (abrégé en CS&R) continue son cheminement législatif et devrait être présenté au Parlement britannique courant 2025. Il reprend les grandes lignes de la directive européenne NIS2, promulguée en 2022. Sous ces deux textes, les responsabilités liées à la gestion des risques de cybersécurité incombent directement aux dirigeants.

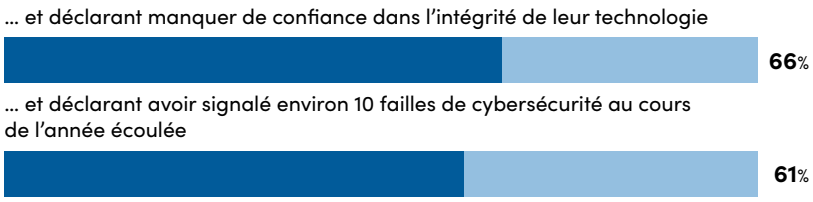
Comme l'explique Patrick Beckman Lapré, Directeur et spécialiste de la confiance numérique chez DigiCert : « L'objectif est de rendre l'entreprise aussi résiliente que possible. C'est une étape importante pour atteindre l'excellence en matière de sécurité. Nous ne pouvons pas tout contrôler, mais nous pouvons apprendre à réduire l'impact d'une cyberattaque sur vos clients et sur votre entreprise. »

Face à l'évolution du champ des menaces, les responsables de la sécurité et de la gestion des risques ont besoin d'une approche structurée. La question se pose alors : comment transposer des exigences complexes et parfois redondantes en stratégies actionnables ? La réponse tient en deux points : tracer une feuille de route claire et repenser l'écosystème numérique.

Les cinq étapes listées ci-dessous aideront les managers et autres dirigeants à faire de la contrainte réglementaire un véritable levier de compétitivité, tout en préparant leur entreprise aux futurs audits de conformité.

Les cybermenaces évoluent parallèlement aux changements réglementaires et les entreprises ont besoin de stratégies solides pour se défendre efficacement

Pourcentage de dirigeants exprimant des inquiétudes en matière de cybersécurité



Deloitte 2024

01 Dresser un inventaire complet des actifs numériques

Pour garantir l'efficacité de ses stratégies de cybersécurité, l'entreprise doit cerner l'intégralité de son parc numérique. Cet inventaire complet offre aux responsables une meilleure visibilité sur les actifs. Découverte automatique des ressources, surveillance continue, vue à 360° sur les connexions externes au réseau… tous ces éléments font partie de l'équation.

« Les actifs peuvent prendre plusieurs formes : PC, serveurs, applications, certificats numériques, règles de pare-feu, équipes internes, prestataires, etc. Sans un inventaire complet de cet écosystème, impossible de savoir si vos contrôles de cybersécurité protègent tout ce qu'ils doivent protéger », met en garde Simon Lawrence, Directeur et Co-fondateur du cabinet de conseil en risque et en sécurité i-confidential.

« Par exemple, si un serveur manque à l'appel dans votre CMDB (Configuration Management Database), votre scanner de vulnérabilités ne pourra pas l'analyser, et vous pouvez vous retrouver avec des vulnérabilités critiques non détectées », poursuit-il.

Cette cartographie de l'écosystème TIC doit regrouper les actifs en fonction des systèmes IT qui les utilisent. Une méthode qui permet d'établir des priorités selon leur niveau de criticité, mais aussi selon l'impact (organisationnel ou réputationnel) d'une éventuelle compromission du système en question.

« Faute de visibilité sur le niveau de criticité de leurs systèmes, les entreprises ont tendance à sous-investir dans les contrôles de leurs systèmes les plus critiques, et à surinvestir dans des systèmes moins à risque.

Résultat, les systèmes critiques sont exposés à des risques cyber significatifs », ajoute Simon Lawrence.

« Ce décalage peut également nuire à l'efficacité de la sécurité opérationnelle. Par exemple, en cas d'attaque, l'équipe de réponse à incident n'aura pas toutes les informations nécessaires pour concentrer ses efforts sur les systèmes critiques. »

02 Optimiser l'architecture de contrôle des accès et des autorisations

L'architecture de contrôle des accès requiert des autorisations granulaires qui déterminent précisément à quels actifs les utilisateurs peuvent accéder, et quelles actions ils peuvent réaliser sur ces ressources. La gestion des accès basée sur les rôles (RBAM) permet, comme son nom l'indique, d'octroyer ces autorisations en fonction des rôles plutôt que des utilisateurs. Cette pratique simplifie l'administration tout en réduisant les risques.

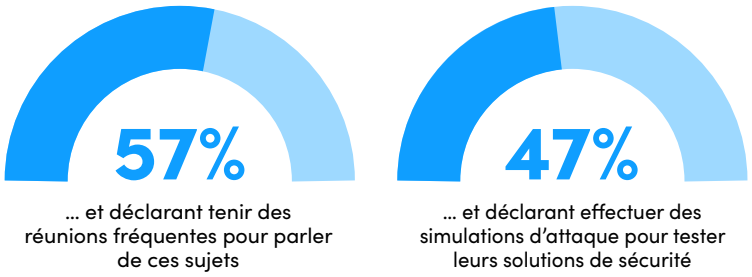
L'efficacité du contrôle des accès passe quant à elle par une vérification rigoureuse des identités, notamment à l'aide de certificats numériques. Véritables gages de confiance, ces certificats authentifient l'identité des utilisateurs, des appareils et des charges de travail dans toute l'infrastructure.

La vérification des identités basée sur les certificats ne peut se faire sans un suivi automatisé de toutes les étapes de leur cycle de vie : émission, renouvellement et révocation. L'automatisation garantit que les certificats n'expireront pas de façon soudaine et permet également de révoquer ceux qui ne sont plus utilisés.

Le système enregistre le détail de toutes les interactions pour savoir à tout moment qui accède à quelle ressource, et quand. Cette piste d'audit assure une surveillance et une conformité constantes.

Les dirigeants doivent mettre en place des systèmes de sécurité résilients et capables de résister à un examen approfondi pour passer haut la main les audits de conformité

Pourcentage de dirigeants faisant état d'un engagement proactif du Comex dans les mesures de cybersécurité…



Deloitte 2024

> Si vous ne tenez pas un inventaire complet de vos actifs, vous n'aurez aucun moyen de vous assurer que vos contrôles de cybersécurité protègent la totalité de votre environnement

L'architecture doit être suffisamment flexible pour tolérer des mises à jour dynamiques et s'adapter à l'évolution des besoins métiers, sans compromis sur l'intégrité de la sécurité. Les workflows automatisés pour les demandes, les autorisations ou les suppressions d'accès facilitent ces mises à jour tout en empêchant les accès non autorisés.

L'efficacité de cette stratégie repose sur deux piliers : des mises à jour continues et une définition claire des responsabilités de chaque équipe. Sans processus capables d'automatiser les tâches tout en tenant compte du facteur humain, les contrôles d'accès censés protéger l'entreprise peuvent devenir eux-mêmes un vecteur de risque.

La gestion des contrôles d'accès n'est pas une tâche ponctuelle intervenant à un instant t. C'est un processus au long cours nécessitant une surveillance et un contrôle continus, pour notamment prendre en compte l'intégration de nouvelles recrues ou le départ de collaborateurs qui pourraient emporter avec eux des données de l'entreprise.

03 Élaborer des protocoles de réponse à incident

Les équipes dirigeantes et SecOps ont un rôle primordial à jouer dans la réponse à incident.

« L'efficacité et l'efficience de la réponse initiale détermineront le niveau d'impact opérationnel et réputationnel d'une attaque, mais aussi le montant des pertes financières subies », assure Katherine Kearns, responsable

EMEA des services proactifs pour le cabinet de conseil S-RM.

Pour surmonter ces obstacles, les entreprises doivent favoriser une collaboration étroite entre les décideurs stratégiques et les équipes techniques chargées de la réponse à incident, et ce, le plus en amont possible.

Elle conseille notamment d'organiser régulièrement des exercices d'entraînement pour que chacun connaisse ses responsabilités et adopte les bons réflexes dans un environnement sans risque. Les leçons tirées de ces mises en situation permettent d'améliorer la réponse à incident le moment venu.

« Des exercices de réponse efficaces mettent à l'épreuve les capacités clés de l'entreprise : continuité des activités, gestion des ressources, restauration des systèmes, gestion des menaces, communication et conformité réglementaire. »

04 Automatiser les contrôles de conformité

En abandonnant la surveillance manuelle au profit d'un processus d'assurance automatisé, les responsables peuvent se préparer en amont aux éventuels audits de conformité. Ils montrent également à leurs partenaires que l'entreprise gère efficacement les risques à tout moment, même en dehors du calendrier d'audit.

Plus important encore, l'automatisation permet de mesurer l'efficacité de la cybersécurité. Les lacunes ou vulnérabilités identifiées sont corrigées en temps réel, assurant ainsi la protection et la conformité de l'entreprise.

De nombreuses entreprises déploient déjà des outils technologiques pour sécuriser leur environnement. Le problème, c'est qu'elles négligent de vérifier leur efficacité au fil du temps, laissant ainsi apparaître des failles que les attaquants n'hésitent pas à exploiter.

« Les contrôles sont souvent évalués à l'aide de tests. On sélectionne un échantillon d'actifs et on détermine si les contrôles nécessaires sont bien appliqués. Ces tests sont généralement réalisés une à deux fois par an. Cette approche offre une certaine visibilité sur l'efficacité et la conformité des contrôles, mais elle a ses limites », tempère Simon Lawrence.

« Par exemple, l'échantillon n'est pas représentatif de tout le parc numérique, donc toute lacune dans les actifs non analysés passera sous les radars. De la même manière, des contrôles trop espacés exposent l'entreprise à des failles de sécurité jusqu'au prochain test, qui peut parfois n'arriver qu'un an plus tard. Les tests de contrôles sont aussi très chers et nécessitent une intervention manuelle. Pour les grandes et moyennes entreprises, ils requièrent une équipe dédiée pour garantir une couverture optimale. »

Les outils CCM (Continuous Control Monitoring) comblent les lacunes des tests de contrôle. Ils automatisent l'évaluation de tout le parc d'actifs et mesurent l'efficacité des contrôles à une fréquence hebdomadaire et même journalière.

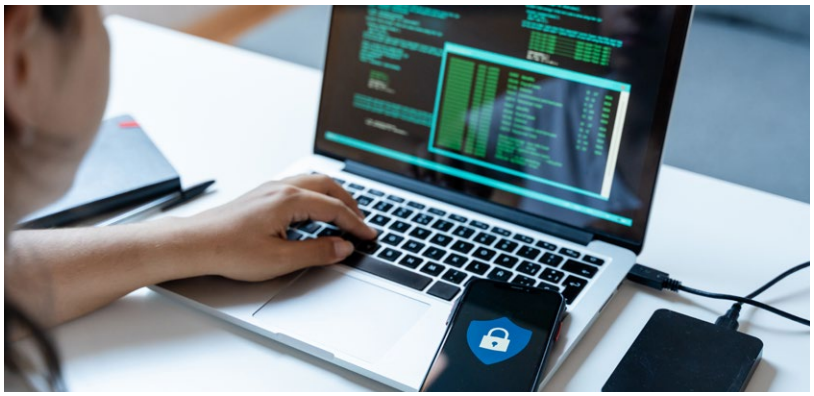
05 Aligner la stratégie de cybersécurité sur les réglementations à l'échelle mondiale

Les entreprises présentes à l'international doivent composer avec les exigences changeantes de multiples juridictions. Ce numéro d'équilibriste exige une parfaite maîtrise des obligations réglementaires et de reporting en vigueur, et ce dans chaque pays où l'entreprise est établie.

Appliquer des frameworks scalables, comme ISO 27001 ou NIST CSF, peut simplifier considérablement les opérations de conformité d'une région à l'autre.

Il est essentiel de désigner des équipes chargées de tenir une veille permanente des changements réglementaires et des menaces émergentes.

Enfin, les équipes régionales sont souvent confrontées aux mêmes défis. Elles doivent donc coordonner leurs actions pour éviter toute fragmentation ou toute redondance dans leurs efforts de mise en conformité.



DORA : une nouvelle opportunité pour libérer tout le potentiel des solutions de sécurité

Face aux dangers que font peser les processus manuels de conformité, les solutions de sécurité automatisées doivent figurer en tête des priorités des dirigeants

Publication commerciale
en association avec
digicert®

En dépit des risques numériques croissants, nombreuses sont les entreprises qui rechignent à délaisser leurs processus manuels au profit d'un système de sécurité automatisé. Erreurs coûteuses, surutilisation des ressources, continuité de l'activité menacée… cette réticence s'avère pourtant préjudiciable.

Car la veille manuelle des changements de réglementation peut accroître le risque de non-conformité, avec pour conséquences de fortes amendes, une chute de la cote de confiance numérique de l'entreprise et une érosion durable de sa réputation.

Entre l'entrée en application du règlement DORA (Digital Operational Resilience Act) de l'Union européenne et une hausse des budgets de cybersécurité attendue par 57 % des responsables au cours des 12-24 prochains mois, selon Deloitte, la conformité s'impose comme un enjeu majeur et prioritaire pour les Comex.

Cap sur la rentabilité

Selon Patrick Beckman Lapré, Directeur et spécialiste de la confiance numérique chez DigiCert, fournisseur mondial de solutions PKI et de gestion du cycle de vie des certificats pour les entreprises, la transformation digitale aide à réduire les tâches manuelles et les coûts associés, permettant ainsi aux responsables de se recentrer sur les stratégies porteuses de compétitivité.

« Le coût des erreurs, de l'inefficacité opérationnelle et des pénalités financières peut vite dépasser les économies que semblent initialement apporter les approches manuelles. Ces dernières vous acculent dans une posture purement réactive, où il vous est impossible d'avoir une bonne compréhension de la situation ou d'anticiper les effets négatifs. »

Pour le directeur de la confiance numérique chez DigiCert, c'est là que l'agilité cryptographique entre en jeu. Cette capacité à passer rapidement d'un mécanisme de chiffrement des données et d'une méthode de sécurité à l'autre s'impose comme une nécessité pour garder l'avantage.

« La cryptographie protège les informations en les convertissant dans des formats chiffrés et sécurisés. D'où l'importance pour les organisations de s'inscrire dans une démarche proactive, en dressant un inventaire complet de leurs outils cryptographiques et en nourrissant leurs capacités à remplacer des solutions vulnérables avant qu'elles ne soient exploitées », constate-t-il.

Et de poursuivre : « Les responsables doivent être en mesure de modéliser les scénarios en amont. En cas de problème, il leur faut pouvoir compter sur des processus et contrôles à même de minimiser les perturbations. »

En effet, la sécurité et la conformité ne relèvent pas d'actions ponctuelles, mais d'un engagement de tous les instants. Dans ce contexte, les plateformes d'automatisation s'avèrent très utiles pour

assurer un suivi en temps réel, signaler les risques et accélérer le lancement de réponses proactives.

Les systèmes de gestion des certificats numériques permettent de réagir rapidement aux évolutions du cadre réglementaire, à l'image de DORA. Le but : ne rien laisser passer pour éviter des amendes et autres sanctions pour non-conformité.

Pour ce faire, ils établissent un suivi et une gestion automatiques des certificats numériques pour aider les responsables à repérer et corriger les problèmes de sécurité avant même qu'ils ne puissent perturber l'activité. Notons que cette capacité constitue un impératif essentiel des nouvelles règles de sécurité de DORA.

Transformation numérique top-down

Entre les gains d'efficacité et une prise de décision plus rapide et éclairée, les arguments en faveur des technologies de conformité numérique sont imparables. Cependant, la réussite de ces solutions exige un leadership et un soutien sans faille de la direction.

Comme l'explique M. Lapré : « De nombreuses entreprises perçoivent la transformation numérique comme une question purement technique. Très souvent, elles se contentent de nommer un RSSI sans prendre toute la mesure des enjeux de cybersécurité. Pourtant, il est indispensable que les cadres et dirigeants s'impliquent pleinement sur ce terrain et cernent parfaitement la situation. »

« Ce sont les membres du Comex qui décident des dépenses. Or si on leur demande d'investir dans une solution sans qu'ils sachent quand exactement elle portera ses fruits, ils seront probablement tentés de miser sur des projets avec un retour garanti sous trois mois. Les dirigeants doivent comprendre que sans investissement dans la conformité de la cybersécurité, la confiance numérique de leur entreprise risque de s'éroder, avec les conséquences désastreuses que cela implique », prévient-il.

Redéfinition de la confiance numérique

Détection précoce des compromissions de données, protection des actifs IP critiques, renforcement de la confiance des clients… une conformité numérique robuste offre de précieux avantages aux entreprises.

En plus de sécuriser les données personnelles et la propriété intellectuelle, ces mesures convertissent les investissements de sécurité en fidélité client et en levier d'action pour créer de la valeur sur le long terme.

> **Une stratégie de conformité numérique renforce la protection des entreprises et améliore ainsi leur cote de confiance numérique**

« Concrètement, les réglementations obligent les entreprises à prendre soin de leur clientèle », pointe l'expert en confiance numérique. « Quelle que soit la nature de votre activité, dans le secteur financier ou la prestation de services, il est capital de réduire les risques et de renforcer la sécurité et la fiabilité des interactions commerciales en ligne. »

« Ces derniers temps, avec la montée en puissance de l'IA, il est de plus en plus difficile de distinguer le vrai du faux. Entre de mauvaises mains, cette arme pourrait causer des dégâts irrémédiables dans les entreprises », avertit M. Lapré.

D'où l'importance de bien choisir son partenaire de solutions numériques, tant pour garantir la robustesse des processus et contrôles que pour renforcer l'arsenal de sécurité, et ce sans accroître les effectifs.

Des défis en constante mutation

« Chaque audit offre l'opportunité de s'améliorer. DigiCert mène 26 audits par an sur l'intégralité de ses activités, y compris à l'international. C'est un gage incontestable de confiance, qui montre que votre partenaire a mis tous les processus en place pour réduire les risques au maximum », remarque M. Lapré.

Même s'il est impossible de maîtriser les risques cyber à 100 %, l'adoption d'une stratégie robuste de cybersécurité vous met à l'abri de lourds préjudices financiers et réputationnels.

« Face à des cybermenaces toujours plus sophistiquées, et des réglementations de plus en plus complexes et contraignantes, une stratégie de conformité numérique offre aux entreprises une protection renforcée et, in fine, une plus grande confiance numérique. »

Et M. Lapré de conclure : « Manquer le tournant décisif de la stratégie numérique est un risque qu'aucune entreprise ne peut se permettre de prendre. » ●

La force de votre stratégie de conformité se mesure à celle de votre équipe de cybersécurité

La pérennité des entreprises repose certes sur de solides stratégies de sécurité. Mais encore faut-il qu'elles soient implémentées par des équipes formées aux pratiques de conformité et conscientes de leur rôle moteur dans la confiance numérique.

Malgré des investissements conséquents dans les outils de conformité numérique, l'erreur humaine reste une cause majeure des compromissions de sécurité dans le monde. Pour preuve, Verizon estime à 68 % la part de l'humain dans ces incidents en 2024.

Ce fossé entre capacités technologiques et performances humaines révèle au grand jour une vérité capitale : une cybersécurité passe non seulement par des outils adaptés, mais aussi par des équipes qui les maîtrisent parfaitement.

En clair, les dirigeants doivent investir autant dans les technologies de défense que dans les connaissances humaines en matière de conformité. Ce juste équilibre permet aux équipes

d'appliquer efficacement les mesures de sécurité et de les maintenir dans la durée, gage d'une défense robuste contre des menaces en constante évolution.

Mais pour garder un coup d'avance sur les défis complexes du numérique, votre stratégie de cybersécurité ne vaut que par la capacité de vos équipes à l'implémenter.

Renforcer la responsabilité collective

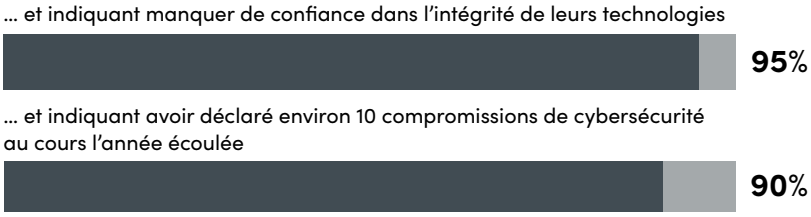
En matière de cybersécurité, la conformité relève de la responsabilité collective. En ce sens, elle dépasse le mandat du seul département IT pour incomber à tous au sein de l'entreprise. Car face à la complexification des obligations réglementaires, les organisations doivent former des équipes de conformité pluridisciplinaires, maîtrisant une large palette de compétences.

Aujourd'hui, une cybersécurité conforme exige une implication de tous les départements. L'époque où le numérique était la chasse gardée de la fonction IT est révolue. Le maintien d'une conformité efficace repose sur les savoir-faire et les perspectives de chaque individu.

Selon Tommaso De Zan, Responsable senior de la gouvernance des données pour le cabinet de conseil technologique Access Partnership : « On tend à sous-estimer le rôle pourtant crucial des différents collaborateurs face à la complexité réglementaire croissante. Les dirigeants devraient former des équipes entières pour l'adoption de processus de sécurité robustes. La proactivité est la meilleure défense », recommande-t-il.

Pour inscrire leur succès dans la durée, les dirigeants doivent considérer la conformité non plus comme une simple liste de cases à cocher, mais comme le pilier d'une culture de l'adaptation et de l'apprentissage

Pourcentage de dirigeants s'exprimant sur leur approche de l'apprentissage des pratiques de conformité dans toute l'entreprise,



Deloitte 2024

> **Les dirigeants devraient former des équipes entières pour l'adoption de processus de sécurité robustes. La proactivité est la meilleure défense.**

À l'heure où les changements incessants de réglementations mettent à rude épreuve les équipes de conformité même les mieux organisées, la montée en compétences devrait figurer en tête des priorités pour rester en phase avec l'évolution des risques.

Dans tous les secteurs et les régions du globe, de nouvelles obligations ne cessent d'apparaître, plongeant les équipes dans un dédale complexe de règles à suivre, à interpréter et à implémenter. Dès lors, la réussite ne dépend pas de la seule vigilance des équipes de conformité, mais aussi d'une implication véritable de tous les départements pour maintenir les standards et adopter rapidement les nouvelles exigences.

Favoriser une culture d'entreprise « compliance-first »

Fini l'époque où la conformité consistait à cocher des cases une fois pour toutes. Désormais, elle s'inscrit dans une culture que les équipes doivent intégrer et entretenir en permanence. La conformité est une responsabilité collégiale. En ce sens, la sécurité doit être l'affaire de tous. Loin d'être une formalité de plus, elle fait partie intégrante des missions des équipes.

Cette approche permet aux entreprises de respecter le volet sécurité d'une transformation numérique porteuse de croissance, tout en sensibilisant durablement aux enjeux d'une protection renforcée.

Pour Casey Ellis, qui conseille les agences nationales de sécurité aux États-Unis, au Royaume-Uni et en Australie, une conformité forte ne doit être que la résultante naturelle d'opérations métiers robustes et bien pensées.

« Une conformité efficace est une conformité que l'on ne remarque pas. Le but ultime est de faire en sorte que la conformité ne fonctionne plus en vase clos et qu'elle devienne une force fédératrice capable de sensibiliser tous les départements aux questions de sécurité, de célébrer les victoires et de faire de la sécurité un domaine d'excellence qui différencie l'entreprise sur ses marchés. Tous ces outils s'avèrent très utiles pour inscrire la conformité de la sécurité au cœur de la culture d'entreprise », constate-t-il.

Favoriser la formation et la reconversion

Force est de constater que l'évolution des menaces et des atteintes à la vie privée complique un peu plus l'équation. Les équipes doivent absolument cerner l'impact de ces nouveaux risques sur leurs obligations réglementaires, et cela passe par un développement continu des compétences et connaissances.

Seulement voilà, nombre d'entreprises n'ont ni les budgets ni les ressources pour organiser des formations et séances d'information sur la conformité.

« Décrocher les fonds nécessaires pour mener des programmes de conformité de premier plan peut engendrer des conflits budgétaires avec d'autres priorités métiers. Et la création de cadres de conformité applicables à différentes juridictions ne fait qu'ajouter au casse-tête », explique M. De Zan.

« Cependant, le défi majeur reste probablement l'application généralisée de ces réglementations dans l'ensemble de l'entreprise. Il s'agit en effet de changer les comportements et d'instaurer une culture de la conformité à laquelle tous les collaborateurs seront réceptifs », ajoute-t-il.

Toutefois, une formation ponctuelle ne suffit pas. Elle doit s'inscrire dans un programme continu d'évaluation et de renforcement des compétences pour s'assurer que les équipes retiennent et appliquent véritablement leurs acquis.

Concrètement, la conformité exige une approche holistique qui pose les collaborateurs en gardiens de la conformité. L'intégration de la conformité dans les workflows au quotidien s'impose comme la méthode la plus efficace, car elle crée le sentiment d'une mission commune qui fait défaut aux formations traditionnelles.

« Les entreprises ne sont pas les seules à s'inscrire dans une telle démarche, les cabinets d'audit et les autorités de surveillance font de même. Ainsi, aux Pays-Bas, la taille de l'équipe responsable de la supervision de ces réglementations a doublé, voire triplé, au cours des deux ou trois dernières années. Et sa croissance se poursuivra avec l'entrée en vigueur d'autres règles et standards », constate Patrick Beckman Lapré, Directeur et spécialiste de la confiance numérique chez DigiCert.

« De nouvelles exigences qu'il faudra vérifier, implémenter et contrôler. Cela demande des compétences, et on peut donc s'attendre à une explosion des recrutements dans ces domaines », ajoute-t-il.

Repenser les bonnes pratiques

Tout l'enjeu consiste à donner aux équipes les moyens de s'adapter rapidement aux changements de réglementation sans pour autant sacrifier l'efficacité opérationnelle ni la créativité. Une mission d'autant plus difficile que si elles se sentent entravées par le devoir de conformité, les équipes pourront être tentées de résister, voire de retarder l'application des nouvelles obligations.

Comme l'explique Casey Ellis : « Au bout du compte, les entreprises devraient appliquer une sécurité adaptée aux menaces et modèles de risques qui les concernent. Or comme ces deux points fluctuent et sont souvent mal compris au sein de l'entreprise, la conformité joue un rôle vital pour réduire les erreurs humaines, guider les bonnes pratiques et, plus généralement, combler les lacunes. »

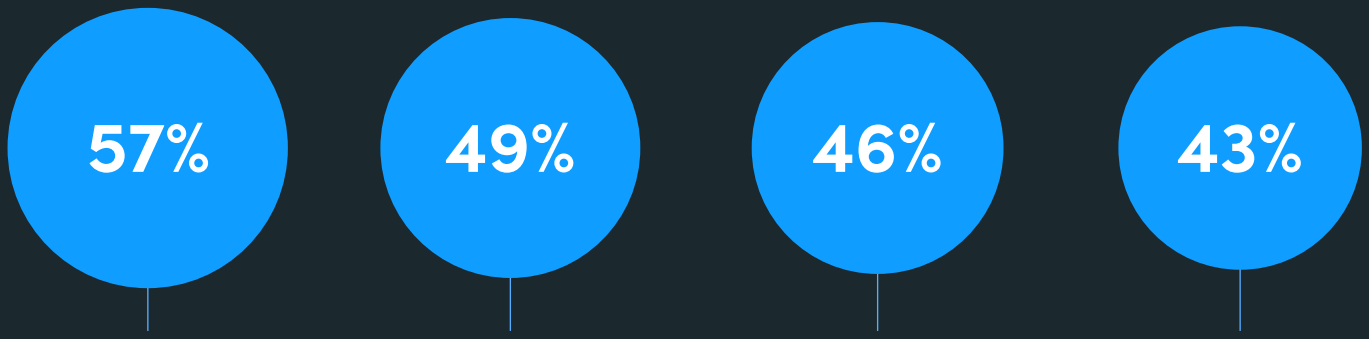
Et de conclure : « Certes, choisir le bon partenaire, établir les priorités en fonction des points forts de l'entreprise, et s'aligner sur les besoins des business units qui produisent et génèrent des revenus représente un défi de taille, mais aussi un formidable levier d'excellence et de différenciation lorsque tout est fait dans les règles de l'art. » ●

Avenir de la conformité cyber : la grande refonte réglementaire

Entre obligations de conformité et impératifs de cybersécurité, comment les dirigeants peuvent-ils négocier le durcissement réglementaire, redessiner les cadres de la gestion du risque et établir une gouvernance robuste ?

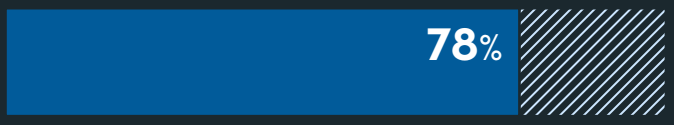
Une réponse efficace à l'évolution des régimes réglementaires et des lois sur le cyber peut aider les dirigeants à maintenir la compétitivité de leur entreprise

Pourcentage de dirigeants considérant l'efficacité des pratiques de conformité comme un levier de compétitivité...

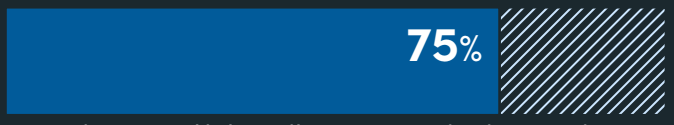


À mesure que les exigences de conformité se resserrent, la cybersécurité est passée d'un problème IT à un sujet incontournable dans les réunions des Comex

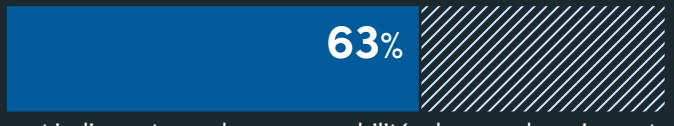
Pourcentage de grandes entreprises déclarant que la cybersécurité est une priorité des Comex...



... et indiquant informer leurs hauts dirigeants des avancées dans ce domaine tous les trimestres



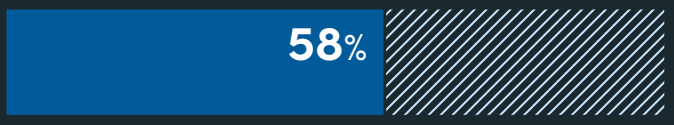
... et indiquant qu'il s'agit d'une priorité absolue pour leurs hauts dirigeants



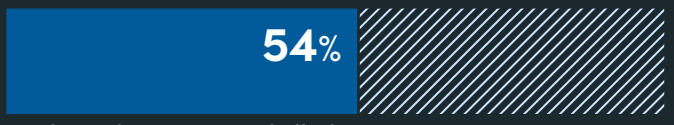
... et indiquant que des responsabilités dans ce domaine ont été explicitement confiées à certains de leurs membres et autres hauts dirigeants

Pour pérenniser leurs opérations, les dirigeants doivent trouver le juste équilibre entre adoption des outils de sécurité et sensibilisation des collaborateurs aux questions de conformité

Pourcentage de dirigeants considérant ces leviers d'action comme étant prioritaires pour les deux prochaines années :



Améliorer la sensibilisation des collaborateurs à la cybersécurité



Renforcer la protection de l'information

Consolider et simplifier les solutions et outils de sécurité

digicert®

Leader mondial de la **confiance numérique**, DigiCert apporte aux entreprises et aux particuliers les outils qui leur permettront d'échanger et de communiquer de façon sereine et sécurisée **dans l'univers du digital**. Sa plateforme **DigiCert® ONE** assure aux organisations une visibilité centralisée et un contrôle inégalé sur leurs besoins en certificats publics et privés pour sécuriser tout leur environnement : site web, accès et communications d'entreprise, logiciels, identités, contenus et appareils. Les solutions primées de DigiCert sont l'aboutissement d'un leadership incontesté en matière de standards, de support et de service, ce qui fait de nous le partenaire privilégié des organisations du monde entier.

Pour en savoir plus, rendez-vous sur **www.digicert.com/fr** ou suivez **@digicert**.

Raconteur

Editor: Larnie Hur
Design: James Lampard, Samuele Motta
Contributors: Alison Coleman

Although this publication is funded through advertising and sponsorship,all editorial is without bias and sponsored features are clearly labelled.
For an upcoming schedule, partnership inquiries or feedback, please call +44 (0)20 3428 5230 or e-mail info@raconteur.net