Démystifier la conformité réglementaire

à l'intention des responsables de la sécurité et des décideurs IT

Introduction

L'élaboration de cadres réglementaires et de normes est née de la nécessité de relever les défis et les exigences liés à la gestion des technologies de l'information et à la protection des données. Ces cadres et normes ont non seulement évolué au fil du temps, mais ils ont aussi été façonnés par les progrès technologiques et les nouvelles menaces de cybersécurité. L'élaboration de cadres et de normes a été principalement motivée par les facteurs suivants :

- **Les organismes de réglementation** insistent sur le fait que les entreprises doivent être responsables de leurs pratiques en matière de cybersécurité et se conformer à des normes et réglementations spécifiques.
- **Les cybermenaces sophistiquées** sont de plus en plus fréquentes et leurs conséquences de plus en plus néfastes. Elles utilisent souvent la sophistication qui était autrefois confinée aux menaces parrainées par les États, mais qui sont maintenant entre les mains d'opportunistes et d'« hacktivistes ».
- **Les infrastructures critiques et les services essentiels** (p. ex., soins de santé, énergie, finances) qui sont indispensables au fonctionnement de la société et de l'économie. Cela inclut les lois fédérales, telles que la Loi sur la déclaration des incidents cybernétiques pour les infrastructures essentielles (CIRCA) de mars 2022.
- **Le manque d'uniformité** des pratiques de cybersécurité dans les différents secteurs et régions. Des approches incohérentes peuvent mener à des lacunes en matière de sécurité et de défis de conformité.
- **Le décret** sur l'amélioration de la cybersécurité du pays qui a été adopté par le président des États-Unis en mai 2021.

Il est évident que les entreprises doivent faire preuve de résilience face aux cybermenaces, afin de pouvoir continuer leurs activités et de les restaurer rapidement après une interruption. Le volume croissant de données personnelles collectées et traitées nécessite d'autant plus de les protéger contre les cybermenaces et les violations de données. Non seulement les cyberincidents ont un impact économique considérable, entraînant des pertes financières et une perte de confiance dans les services numériques pour l'ensemble de l'économie. Mais ils peuvent aussi parfois coûter des vies, en particulier lorsque le secteur de la santé est pris pour cible.

La conformité réglementaire est essentielle pour renforcer la résilience de l'entreprise. Les entreprises qui saisissent l'étendue de leurs risques reconnaissent que la conformité n'est pas une simple tâche à cocher, mais un élément fondamental d'une stratégie de sécurité globale. En respectant les réglementations et en mettant en œuvre les meilleures pratiques en matière de sécurité, les entreprises peuvent mieux se préparer à résister à la plupart des cyberincidents et à s'en remettre rapidement. Cette approche garantit qu'en cas de crise, les bases d'une reprise rapide sont déjà en place.

1.

Cyberattaques

Si l'infrastructure numérique d'une entreprise est attaquée, les conséquences peuvent aller bien au-delà de la simple perte de données. Les conséquences des temps d'arrêt, la perte de fonctions essentielles, les perturbations potentielles des ventes et la façon dont l'entreprise est perçue sont toutes des conséquences potentielles d'un cyberincident.

Dans le sillage de ces possibilités, l'impact sur la vie humaine est le facteur le plus important à garder à l'esprit. Dans les secteurs des services financiers et de la santé, les cybermenaces peuvent engendrer des bouleversements sur le plan humain, notamment en ce qui concerne les factures, les paiements et l'accès aux soins médicaux, entre autres. De telles préoccupations et de tels risques sont une bonne raison pour inciter les entreprises à améliorer leur dispositif de sécurité en se conformant aux réglementations en vigueur dans leur secteur.

Pourquoi la conformité est-elle importante ?

La conformité implique le respect des lois et réglementations qui s'appliquent au secteur d'activité et à la localisation géographique de l'entreprise. Être en conformité peut contribuer à réduire l'impact sur votre entreprise, qu'il s'agisse de pertes de chiffre d'affaires liées au paiement de rançons, de perturbations opérationnelles, d'expositions à des violations de données, d'amendes réglementaires ou d'atteinte à la réputation. Les normes de conformité évoluent rapidement et continueront de le faire. Les règlements élaborés aujourd'hui pour atteindre les objectifs actuels pourraient ne pas fonctionner à l'avenir. Rester à jour avec les nouveaux cadres et réglementations et leurs nouvelles attentes constitue un moyen infaillible de protéger votre entreprise.

Réglementations et cadres

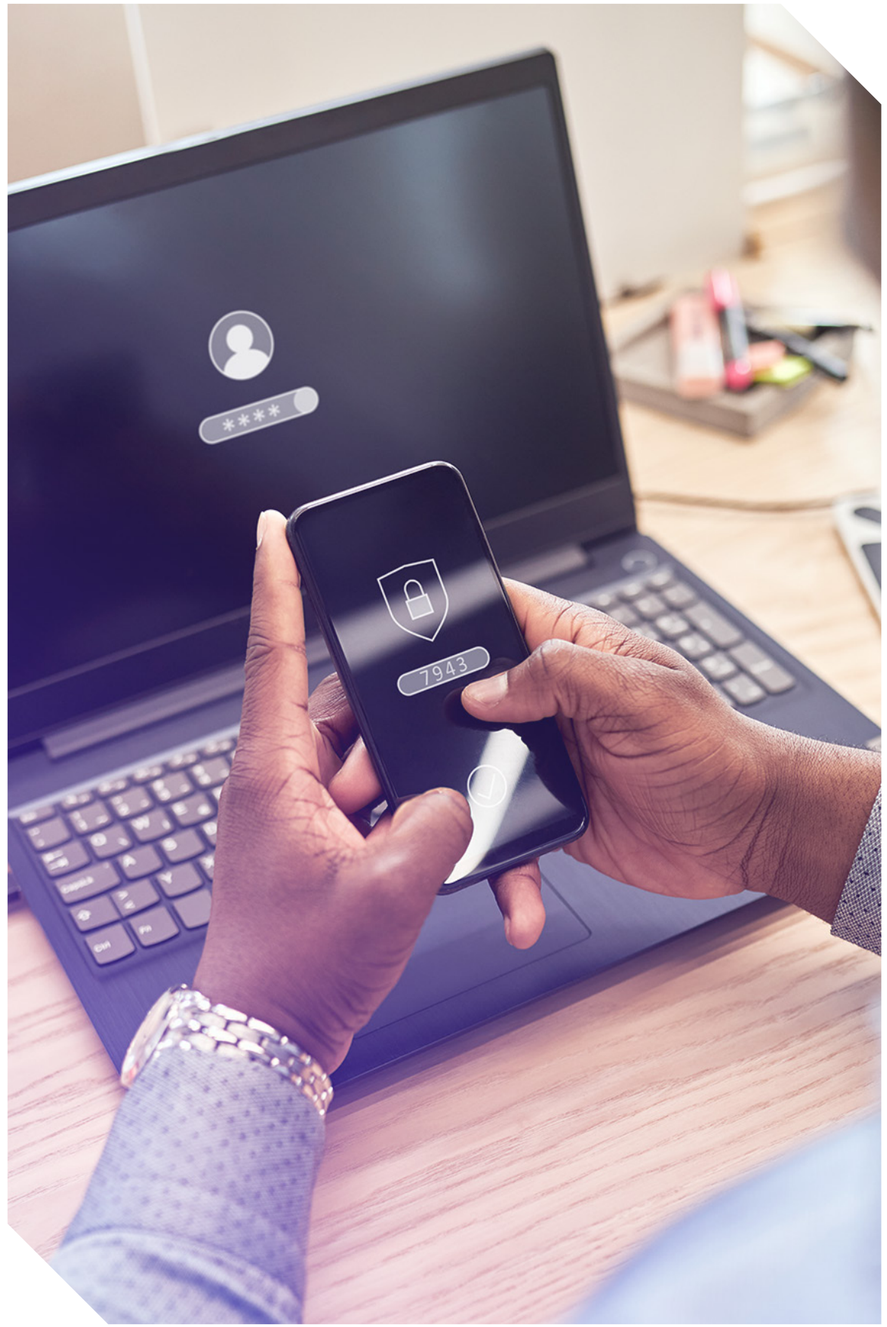
La principale différence entre les réglementations et les cadres réside dans l'objectif que vous visez. Les cadres fournissent un ensemble structuré de lignes directrices, de meilleures pratiques et de normes que les organisations peuvent utiliser pour gérer et améliorer leur posture de cybersécurité. Les réglementations, quant à elles, sont des exigences légales imposées par les gouvernements ou les organismes de réglementation pour appliquer un standard minimal de pratiques de cybersécurité dans toutes les organisations. Voici quelques-unes des réglementations les plus répandues :

- **RGPD** (Règlement général sur la protection des données) — Règlement de l'Union européenne sur la protection des données et de la vie privée.
- **HIPAA** (Loi sur la portabilité et la responsabilité en matière d'assurance maladie) — Réglementation américaine sur la protection des informations relatives à la santé.
- **SOX** (Sarbanes-Oxley Act) — Réglementation américaine des pratiques financières et de la gouvernance d'entreprise.
- **PCI DSS** (Norme de sécurité des données de l'industrie des cartes de paiement) — Normes pour la sécurisation des transactions par carte de crédit.
- **FISMA** (Federal Information Security Management Act) — Loi américaine sur la protection des informations gouvernementales.

De telles réglementations fonctionnent de concert avec les cadres. Par exemple, les cadres constituent la base de la conformité aux réglementations, et les réglementations favorisent l'adoption des cadres. Ces cadres aident également les entreprises à dépasser les exigences réglementaires minimales et facilitent la mise en conformité et l'audit, tandis que les réglementations garantissent une sécurité de base cohérente dans tous les secteurs. Voici quelques-uns des cadres les plus utilisés :

- **NIST Cybersecurity Framework (CSF)** — Propose une approche complète de la gestion des risques liés à la cybersécurité.
- **Contrôles CIS** — ensemble de meilleures pratiques de défense contre les cybermenaces.
- **COBIT** — Fournit un cadre pour la gestion et la gouvernance informatiques, en mettant l'accent sur les objectifs de contrôle de l'informatique, y compris la cybersécurité.

Les cadres fournissent les meilleures pratiques en matière de gestion de la cybersécurité, tandis que les réglementations appliquent des normes minimales pour garantir une sécurité de base dans tous les secteurs.



Gestion des risques et conformité

Une approche fondée sur les risques commence par une évaluation approfondie des risques. Ce processus doit impliquer les contributions de diverses parties prenantes, notamment les équipes de sécurité, les membres du personnel informatique, les experts juridiques et les chefs d'entreprise.

Par exemple, un fournisseur de soins de santé peut considérer la protection des dossiers de santé électroniques (DSE) comme une priorité absolue en raison de la nature sensible des données et des conséquences potentielles d'une violation, telles que la perte des données des patients et les amendes réglementaires en vertu de la loi HIPAA. En accordant la priorité à la sécurité des DSE, le fournisseur peut concentrer ses efforts de conformité sur la mise en œuvre de contrôles qui atténuent les risques les plus importants.

Alors que les exigences réglementaires continuent de gagner en complexité, les organisations se tournent de plus en plus vers des outils de gouvernance, de gestion des risques et de conformité (GRC) pour rationaliser leurs processus de conformité, améliorer leur visibilité et assurer une surveillance et une amélioration continues.

Une approche de la conformité fondée sur les risques permet d'adapter les efforts de sécurité aux risques spécifiques de chaque entreprise, de sorte à garantir que les menaces critiques sont classées par ordre de priorité.

Vue d'ensemble des outils GRC et de leurs avantages :

Les outils GRC sont conçus pour aider les organisations à automatiser et à gérer divers aspects de la conformité, notamment l'élaboration de politiques, l'évaluation des risques, le suivi des audits et la réponse aux incidents. Ces outils offrent plusieurs avantages clés :

- **Gestion centralisée de la conformité :** Les outils GRC permettent aux organisations de fusionner les activités de conformité dans une seule plateforme.
- **Automatisation des tâches de conformité :** En automatisant les tâches de conformité de routine, telles que la surveillance des journaux d'accès ou la génération de rapports d'audit, les outils GRC permettent de gagner un temps précieux.
- **Visibilité et reporting améliorés :** Les outils GRC offrent une visibilité en temps réel de l'état de la conformité, ce qui permet aux responsables de la sécurité de suivre plus facilement les progrès réalisés, d'identifier les lacunes et de démontrer la conformité aux régulateurs et aux auditeurs.
- **Supervision et amélioration continues :** Les outils GRC prennent en charge la supervision continue des activités de conformité, ce qui permet aux organisations d'identifier et de résoudre les problèmes de manière proactive plutôt que réactive.

2.

Pourquoi il est important d'adopter des réglementations de conformité

L'objectif de la compréhension des risques encourus par votre entreprise et des moyens d'en tenir compte n'est pas de trouver des coupables. Il est plutôt important de trouver des faits afin d'aider votre organisation à se protéger et à aller de l'avant. Si les dirigeants pensent que leur entreprise est prête et résiliente en matière de cybersécurité, la réalité peut être très différente et mettre les organisations en danger.

S'assurer de la participation et de l'engagement du conseil d'administration est le principal moyen d'atteindre la conformité. Les entreprises doivent promouvoir une culture de la conformité dans l'ensemble de l'organisation afin de réduire les risques. La direction est responsable de la mise en œuvre des processus et de la technologie conformément à la réglementation. Il est important de prendre du recul et de s'assurer que les lois et réglementations sont respectées dans le contexte du secteur et de l'implantation géographique de la société.

Au fur et à mesure que le secteur se développe et évolue, les normes de conformité et de réglementation évolueront également. Cependant, vous ne souhaitez pas que votre entreprise prenne du retard en matière de conformité, car vous risqueriez alors de devenir négligent, et c'est à ce moment-là qu'un dirigeant ou un membre du conseil d'administration devient passible de mesures punitives. Une panne ou une attaque par ransomware peut entraîner des pénalités financières et une atteinte à la réputation. Mais plus votre entreprise gagne en maturité pour répondre aux différentes exigences de conformité réglementaire, meilleures sont vos chances de reprendre vos activités rapidement.

Conformité dans le monde entier

À l'échelle mondiale, si vous regardez la législation en matière de cybersécurité, au total, plus de 150 pays ont mis en place une sorte de règlement en lien avec la cybersécurité. Certains d'entre eux incluent DORA dans l'UE, ainsi que NIS/NIS2 au Royaume-Uni. Le Japon a élaboré la FSA et le Moyen-Orient la NESA et la DIFC qui sont des lois sur la protection des données. À l'échelle mondiale, les pays peuvent se tourner vers le NIST. Aux États-Unis, quand il est question de ransomwares et d'amendes réglementaires, on pense à la Securities and Exchange Commission (SEC). Malgré le large éventail d'options réglementaires, moins de 100 pays disposent d'une réglementation concernant les infrastructures critiques. Cela montre que de nombreux pays ne se préoccupent pas de la sécurité à un niveau élevé, même s'il existe un besoin bien réel de se concentrer sur ces environnements d'infrastructures critiques. S'agissant du secteur de la santé en particulier, y compris la recherche et la biotechnologie, les règles sont souvent différentes d'un pays à l'autre.

Les réglementations en matière de conformité garantissent que votre organisation est prête à faire face aux cyberincidents, l'engagement du conseil d'administration étant crucial pour faire régner une culture de la sécurité.

En quoi les secteurs des services financiers et de la santé diffèrent-ils ?

Aux États-Unis, le Cyber Incident Reporting for Critical Infrastructure Act (CIRCA) répertorie 16 secteurs critiques qui doivent être en conformité avec différentes réglementations. Lorsque les gens pensent aux secteurs critiques, ils pensent normalement aux barrages, aux réseaux électriques et, bien sûr, aux soins de santé. Les services de santé et les services financiers jouent un rôle essentiel dans la vie quotidienne des gens partout dans le monde. Lorsque l'on examine les effets négatifs qu'un défaut de conformité en matière de sécurité peut entraîner sur les organismes de soins de santé, c'est la vie des gens qui est impactée.

La loi américaine HIPAA est l'une des principales réglementations qui vient à l'esprit lorsque les gens pensent à la conformité des soins de santé. La HIPAA Privacy Rule établit des normes nationales pour la protection de certaines informations de santé, tandis que la HIPAA Security Rule définit un ensemble de normes de sécurité pour la protection de certaines informations de santé détenues ou transférées sous forme électronique. Si un fournisseur de soins de santé n'est pas correctement protégé ou conforme, il peut s'exposer au risque que les données de ses patients soient compromises en cas d'attaque avec demande de rançon.

Dans le secteur financier, l'une des principales réglementations est la GLBA, ou Gramm-Leach-Bliley Act. Cette loi oblige les sociétés financières qui offrent aux consommateurs des produits ou des services financiers tels que des prêts, des conseils financiers ou d'investissement, ou des assurances, à expliquer leurs pratiques de partage d'informations à leurs clients et à protéger les données sensibles. Lorsqu'une société financière n'est pas conforme aux cadres ou aux réglementations, elle court le risque de faire face à des coûts, tels que des pertes financières importantes, des amendes, la perte de stabilité économique et une atteinte à sa réputation.

Les entreprises doivent s'adapter en permanence aux nouvelles réglementations pour maintenir leur conformité et garder une longueur d'avance sur les menaces de cybersécurité en constante évolution.

3.

Meilleures pratiques recommandées et implémentation

La conformité est loin d'être une considération ponctuelle. Les exigences réglementaires ne sont pas figées ; elles évoluent au fil du temps, à mesure que de nouvelles menaces apparaissent et que la réglementation est mise à jour. Dans ce contexte, il existe des meilleures pratiques à mettre en œuvre pour s'assurer que votre entreprise reste conforme à tous les cadres et réglementations essentiels.

Surveillance continue

La surveillance continue est un élément essentiel d'une gestion efficace de la conformité. Les outils GRC facilitent la supervision continue en s'intégrant dans l'infrastructure de sécurité existante, telle que les systèmes SIEM (Security Information and Event Management, gestion des informations et des événements liés à la sécurité), pour assurer le suivi de la conformité en temps réel.

Par exemple, une société de services financiers assujettie à la loi SOX peut utiliser un outil GRC pour surveiller en permanence l'accès aux systèmes financiers, en veillant à ce que seul le personnel autorisé ait accès aux données financières sensibles. En intégrant les outils GRC dans leurs stratégies de cybersécurité, les organisations peuvent rationaliser leurs efforts de conformité, réduire le risque de non-conformité et s'assurer que leurs pratiques de sécurité évoluent conjointement avec les exigences réglementaires.

Audits et évaluations réguliers

Pendant une attaque, il ne sera pas question de savoir si vous disposez d'un plan de réponse aux incidents, mais plutôt de savoir si ce plan est en place. Vous devez *savoir que* votre plan fonctionnera. Les tests constituent un des meilleurs moyens de s'en assurer. C'est en testant le plan de votre entreprise et en démontrant que le test a réussi que vous garantissez le niveau de conformité.

Les étapes clés de la conformité

Lors de l'examen des réglementations à mettre en œuvre pour être en conformité, il est important d'adopter une approche holistique. Chaque secteur de votre organisation peut être lié à un autre aspect de votre environnement. La planification et la prévoyance joueront un rôle énorme pour assurer la conformité de votre organisation. Voici quelques étapes à prendre en compte :

- **Élaborez un processus de gestion des risques :** Il s'agit d'identifier tous les risques informatiques potentiels qui pourraient affecter votre entreprise ainsi que d'évaluer vos vulnérabilités.
- **Analysez et hiérarchisez vos risques :** Cela est possible en élaborant une stratégie d'atténuation des risques et en formant votre personnel.
- **Élaborez un plan de réponse aux incidents :** Dans ce plan, vous pouvez prendre en compte des éléments tels que le transfert des risques tout en maintenant la visibilité et la connaissance de votre environnement.
- **Instaurez une culture de la sécurité :** Il peut s'agir d'impliquer toutes les parties prenantes concernées, de choisir les bonnes technologies et de ne jamais oublier de documenter, toujours documenter.

Développez un processus de gestion des risques, hiérarchisez les risques et créez une culture de la sécurité pour maintenir la conformité et renforcer la résilience.

Conclusion

L'avenir de la conformité réglementaire mettra l'accent sur la résilience, les entreprises devant anticiper les nouvelles réglementations et concevoir des programmes de conformité adaptables et proactifs.

Le paysage réglementaire est dynamique et il est peu probable que le rythme des changements réglementaires ralentisse, d'autant plus que les gouvernements et les organismes de réglementation se mettent au pas des progrès rapides de la technologie. Dans cette optique, il s'agit pour les organisations d'adapter les cadres de sécurité et de continuer à assurer la conformité réglementaire. Un objectif secondaire serait la normalisation des meilleures pratiques en matière de sécurité afin d'aboutir à un point où les organisations atteignent une posture de sécurité acceptable.

En conclusion, la conformité réglementaire est un parcours continu qui nécessite d'incessants efforts d'adaptation et de collaboration.

Il ne suffit pas d'assurer la conformité ; les entreprises doivent s'efforcer de maintenir et d'améliorer leurs programmes de conformité pour faire face à l'évolution des menaces et des réglementations. Les responsables de la sécurité et les décideurs informatiques jouent un rôle crucial dans ce processus, en guidant leurs organisations vers une stratégie de conformité qui ne vise pas seulement à éviter les sanctions, mais aussi à bâtir une organisation plus forte et plus résiliente aux cybermenaces. En intégrant la conformité dans le tissu de leurs opérations et de leur culture, et en restant informées et agiles face au changement, les organisations peuvent naviguer dans les complexités du paysage réglementaire avec confiance et succès.