OSLER

Une cybersécurité digne de confiance grâce à une approche concrète : normes et programmes de validation pour les PME

12 FÉVRIER 2025 10 MIN DE LECTURE

Expertises Connexes

- Cybersécurité et intervention en cas d'incident lié à la sécurité
- Respect de la vie privée et gestion de l'information
- Sociétés émergentes et à forte croissance
- Technologie

Auteurs(trice): Sam Ip, Justin P'ng, CIPP/C/US, Joseph Ierullo

Le 6 février 2025, le Conseil de gouvernance numérique, un organisme à but non lucratif qui joue un rôle essentiel dans l'établissement des normes canadiennes, a lancé son nouveau programme de validation CyberReady. Ce programme vise à aider les petites et moyennes entreprises (PME)[1] à renforcer leurs mesures de cybersécurité grâce à un service d'examen de leurs pratiques de cybersécurité et de vérification de leur conformité aux exigences de base.

Un tel lancement arrive à point nommé et coïncide avec l'introduction par le gouvernement du Canada de sa nouvelle Stratégie nationale de cybersécurité, qui vise à répondre à la myriade de cybermenaces auxquelles le pays est confronté. Compte tenu de la complexité et de la fréquence croissantes des incidents de cybersécurité, ainsi que de la vulnérabilité des petites entreprises en raison de leurs ressources limitées, le programme de validation CyberReady pourrait combler une lacune dans la promotion et la normalisation de la préparation des PME en matière de cybersécurité.

Les menaces de cybersécurité devenant de plus en plus fréquentes, il est essentiel que les PME mettent en œuvre des contrôles de cybersécurité fondés sur des normes accessibles, pragmatiques et réalistes. En ce qui concerne le secteur de l'IA, nous avons déjà étudié les risques émergents en matière de sécurité de l'IA et les cadres généraux de l'IA tels que le cadre de gestion des risques liés à l'IA du NIST pour les entreprises de développement et de déploiement de l'IA. De manière générale, de nombreuses entreprises reconnaissent la norme ISO/IEC 27001 comme l'une des normes de sécurité de l'information les plus connues, mais nombre de PME la trouvent impossible à mettre en œuvre à cause de sa rigueur et de ses exigences détaillées.

Face à ce défi, la norme CAN/DGSI 104 : 2021 / Rév. 1 : 2024 propose des contrôles de cybersécurité de base qui aideront les PME à naviguer dans cet environnement à risque. Associée au programme de validation CyberReady, cette norme peut constituer une approche économique permettant de faire face aux risques de cybersécurité et de renforcer la confiance des parties prenantes.

Vue d'ensemble

CAN/DGSI 104 : 2021 / Rév. 1 : 2024 – Contrôles de cybersécurité de base des PME

La norme CAN/DGSI 104 : 2021 / Rév. 1 : 2024 (la norme de cybersécurité des PME), qui a été révisée en décembre 2024, établit les contrôles de cybersécurité de base des PME. Elle englobe un éventail de contrôles, allant d'aspects organisationnels tels que la direction et la responsabilité à des mesures techniques telles que l'application automatique des correctifs, l'authentification des utilisateurs et le contrôle de l'accès.

Reconnaissant la diversité des besoins des entreprises, en particulier des petites, la norme de cybersécurité des PME présente les exigences suivant deux niveaux : les exigences du niveau 1 s'adressent aux petites entreprises pour qui la cybersécurité est un domaine nouveau, et les exigences de niveau 2 s'adressent aux entreprises qui ont gagné en maturité et qui cherchent à améliorer leurs mesures de cybersécurité. La norme de cybersécurité des PME comprend également des annexes pratiques, telles qu'un modèle de plan d'intervention en cas d'incident, un questionnaire d'évaluation des risques de cybersécurité et un questionnaire d'analyse des risques associés aux fournisseurs.

Programme de validation CyberReady

Selon le Conseil de gouvernance numérique, le programme de validation CyberReady vise à aider les entreprises à évaluer et à valider leur état de préparation en matière de cybersécurité, en s'assurant que leurs pratiques et leurs contrôles répondent à la norme de cybersécurité des PME. À ce jour, deux services sont proposés, à savoir un examen de validation basé sur les renseignements déclarés et un audit de validation plus approfondi.

Assorti de coûts relativement modestes, le programme constitue une option relativement abordable pour les PME qui cherchent à renforcer et à démontrer leur posture. Cela dit, bien qu'il soutienne la certification, il est important de noter qu'il ne s'agit pas d'une certification en soi, même si les entreprises retenues recevront une déclaration de validation ou de vérification et la marque de confiance associée. Les entreprises intéressées par ce service peuvent examiner ces options afin de déterminer si elles sont adaptées à leur activité.

De vastes conséquences

Des outils tels que la norme de cybersécurité des PME et des programmes tels que le programme de validation CyberReady du Conseil de gouvernance numérique ont de vastes conséquences, en particulier pour les sociétés émergentes et à forte croissance pour lesquelles la cybersécurité représente souvent un défi. En particulier :

- **Point de départ de la cybersécurité.** De nombreuses PME n'ont pas les ressources nécessaires pour mettre en œuvre un programme de cybersécurité de qualité supérieure comparable à celui des grandes entreprises de leur secteur. Les cadres d'entreprise tels que la norme ISO/IEC 27001 nécessitent un investissement financier important et font souvent appel à des fonctions organisationnelles entièrement dédiées, ce qui les rend impraticables pour les petites entreprises. Certaines PME sont également intimidées par leur complexité, tandis que d'autres n'y voient pas une priorité immédiate. À première vue, la norme de cybersécurité des PME constitue une base relativement accessible. Associée à des initiatives telles que le programme de validation CyberReady, elle semble offrir une approche pratique et structurée pour la mise en place d'un programme de sécurité de l'information et de la gestion des risques courants en matière de cybersécurité, tels que les rançongiciels, l'hameçonnage et d'autres types d'atteintes à la protection des données ou des systèmes.
- **Normalisation des attentes des PME en matière de cybersécurité.** Compte tenu de la

variabilité des contrôles de sécurité de l'information, de nombreuses PME qui ne souscrivent pas encore à une norme industrielle telle que la norme ISO/IEC 27001 suivent une série d'approches différentes pour sécuriser leur environnement. La norme de cybersécurité des PME représente une référence intégrée – et un sous-ensemble pratique de la norme ISO/IEC 27001 – par rapport à laquelle les PME peuvent s'évaluer, ainsi qu'une opportunité d'harmoniser les attentes et les approches pour ces types d'entreprises, y compris dans des domaines critiques tels que la planification des interventions en cas d'incident.

- **Imputabilité revenant à un tiers.** Comme c'est le cas pour d'autres programmes d'examen indépendants, le programme de validation CyberReady rehausse les attentes des PME en servant de mécanisme officiel d'imputabilité revenant à un tiers relativement à la norme de cybersécurité des PME. Les PME qui veulent s'assurer qu'elles obtiennent une vérification ou une validation réussie seront incitées à améliorer sensiblement leur posture de cybersécurité. D'autres PME qui souhaitent commercialiser leur adhésion à la norme de cybersécurité des PME seront incitées à démontrer leur conformité en recourant au programme de validation CyberReady ou à disposer d'une base crédible pour ne pas accepter de se soumettre à un examen dirigé par un tiers.
- **Confiance accrue sur le marché.** Pour de nombreuses sociétés émergentes et à forte croissance novatrices, il est essentiel de démontrer leur état de préparation en matière de cybersécurité. De nombreuses jeunes entreprises – en particulier celles qui proposent des solutions basées sur des logiciels-services – traitent d'importants volumes de données et de renseignements de nature sensible. L'adoption d'une norme de cybersécurité reconnue, telle que la norme de cybersécurité des PME, peut donner des assurances aux clients, aux partenaires commerciaux et même aux investisseurs actuels et potentiels, et ainsi réduire les inquiétudes et renforcer la confiance et la crédibilité.
- **Processus de passation de marchés simplifié.** Les sociétés émergentes et à forte croissance ont souvent du mal à conclure des ventes rapides avec de grandes entreprises complexes et des entités gouvernementales en raison de préoccupations liées à la cybersécurité. Les listes de contrôle jointes à titre d'annexes de la norme de cybersécurité des PME constituent un point de départ utile pour répondre à ces préoccupations. En particulier :
  - L'annexe B (Questionnaire d'évaluation des risques de cybersécurité) aide les PME à évaluer et à déceler les lacunes de leur posture de sécurité.L'annexe C (Questionnaire d'analyse des risques associés aux fournisseurs) prépare les PME aux types de questions auxquelles elles peuvent s'attendre de la part d'entreprises clientes complexes.
- **Contrats commerciaux.** Les jeunes entreprises sont souvent confrontées à la complexité des différents engagements en matière de sécurité dans leurs contrats, car chaque client peut imposer des exigences de sécurité légèrement différentes (par exemple, la norme de chiffrement AES par rapport à d'autres normes). En adhérant à des normes reconnues telles que la norme de cybersécurité des PME, les PME peuvent se doter de contrôles de base, ce qui rend plus crédible le fait que leurs pratiques de sécurité sont conformes aux

attentes du secteur et devraient être considérées comme acceptables. De même, pour ceux qui achètent des solutions aux PME, le fait d'exiger qu'elles se conforment à une norme reconnue telle que la norme de cybersécurité des PME constitue un moyen rapide d'éviter des négociations fastidieuses et prolongées sur les dispositions touchant la sécurité, tout en obtenant dans le contrat des engagements de base en la matière.

- **Outil dans le cadre des opérations de fusion et d'acquisition.** Les risques liés à la cybersécurité sont souvent une question clé à considérer dans le cadre d'une opération de fusion et d'acquisition, car les acheteurs et les investisseurs cherchent à atténuer les risques liés aux cybervulnérabilités. Des programmes tels que le programme de validation CyberReady ne remplaceront pas la vérification de sécurité détaillée traditionnelle, mais ils peuvent simplifier les évaluations de cybersécurité, aider les vendeurs à démontrer leur état de préparation au-delà de ce qui a été dit au cours de la vérification diligente et accroître chez les acheteurs leur degré de confiance envers la sécurité des cibles d'acquisition.

Conclusion

L'efficacité de la norme de cybersécurité des PME, tout comme celle du programme de validation CyberReady, reste à démontrer, et son succès dépendra de sa capacité à rester alignée sur des normes sectorielles bien connues qui évoluent rapidement pour faire face aux nouvelles menaces en matière de cybersécurité. En outre, il est essentiel de trouver un équilibre entre la rentabilité et une validation complète. Sans une validation rigoureuse, le risque subsiste de créer un faux sentiment de sécurité si l'efficacité des contrôles ne fait pas l'objet d'une évaluation approfondie.

Cela dit, la norme de cybersécurité des PME et le programme de validation CyberReady peuvent offrir une solution pratique et structurée aux PME qui n'ont pas les ressources nécessaires pour mettre en œuvre un programme de sécurité exhaustif et démontrer qu'elles s'y conforment. En s'appuyant sur des normes établies telles que la norme CAN/DGSI 104 : 2021/ Rév. 1 : 2024, les entreprises peuvent franchir des étapes importantes vers le renforcement de leur posture de cybersécurité, l'accroissement de la confiance des parties prenantes et leur conformité aux attentes en matière de sécurité, qui ne cessent d'évoluer.

Quoi qu'il en soit, la norme de cybersécurité des PME et le programme de validation CyberReady ne sont que deux des nombreux outils auxquels les PME peuvent recourir pour renforcer leur résilience en matière de cybersécurité. Bien que les programmes de ce type offrent des directives structurées, les PME devraient évaluer soigneusement les normes de cybersécurité existantes et adopter celle qui correspond le mieux à leurs besoins, à leurs ressources et à leur profil de risque.

---

[1] Selon la norme CAN/DGSI 104 : 2021 / Rév. 1 : 2024, une PME comptera généralement moins de 500 employés.