29_P-112

Rapport d'audit

Sécurité de l'information

1er mandat

Présenté au CTI-CAPV

11 mars 2021

Société de l'assurance automobile Québec

Plan de la présentation

- Contexte
- Étendue et portée des travaux
- Objectifs d'audit
- Constats/Recommandations et Plan d'action
- Liste des acronymes

Contexte

Dans les dernières années, la Société a entrepris un projet de transformation numérique ayant comme objectif de bonifier ses services d'affaires avec ses clients et ses partenaires. Dans ce contexte, la Société doit maintenir la confiance de sa clientèle et de ses partenaires afin de s'assurer de leur adhésion à ses nouveaux services en ligne. La Société doit donc assurer la sécurité des informations qu'elle détient de sa clientèle et de ses partenaires afin de maintenir cette confiance.

Cette obligation est également encadrée notamment par la *Loi sur l'accès aux documents des organismes publics et sur la protection des renseignements personnels,* la *Politique gouvernementale de cybersécurité et la Directive sur la sécurité de l'information gouvernementale.* Cette dernière exige, entre autres, la réalisation d'un audit de sécurité minimalement au deux ans.

Étendue et portée des travaux

Les travaux d'audit se sont déroulés de juin 2018 à novembre 2020, mais peuvent également faire référence à des situations antérieures ou ultérieures à cette période, le cas échéant.

Les procédés d'audit visaient à recueillir les éléments probants suffisants et appropriés pour fonder raisonnablement les conclusions.

Les constats et recommandations portent principalement sur les obligations découlant de la *Directive sur la sécurité de l'information gouvernementale*.

Étant donné qu'il s'agit ici d'un mandat statutaire, les travaux se poursuivent et les résultats vous seront communiqués de façon périodique.

Objectifs d'audit

Le mandat d'audit vise à s'assurer que:

- la politique, le cadre de gestion et les principes de bonne gouvernance en sécurité de l'information sont appliqués et suivis;
- des mesures de protection appropriées sont définies, appliquées et suivies en fonction des risques et de la nature des informations à protéger.

Constat

1. La Société a réalisé des tests d'intrusion au cours des dernières années, toutefois, leur portée est limitée. Ces tests sont insuffisants pour s'assurer de l'efficacité des mesures de sécurité mises en place pour se protéger contre les cybermenaces.

Impact: En l'absence de test d'intrusion complet, des vulnérabilités dans l'environnement informatique de la Société pourraient être présentes et permettre notamment à des pirates informatiques de compromettre certains actifs informationnels critiques.

RECOMMANDATION

La Société doit réaliser des tests d'intrusion couvrant notamment l'ensemble des composantes vulnérables aux cyberattaques. Ces tests doivent être effectués minimalement une fois par année par des personnes indépendantes.

Plan d'action - Recommandation 1

Recommandation	Actions prévues	Responsables	Échéances
La Société doit réaliser des tests d'intrusion couvrant notamment l'ensemble des composantes vulnérables aux cyberattaques. Ces tests doivent être effectués minimalement une fois par année par des personnes indépendantes.	➢ Réaliser les tests planifiés à la suite de la mise en œuvre des 3 initiatives suivantes du plan de sécurité de l'information numérique 2020-2022 (PSIN). o No 5: Mettre en place un coffre à outils complet de gestion des vulnérabilités et de test d'intrusion; o No 11: Effectuer la planification triennale des tests internes et externes; o No 12: Mettre en place des outils centralisés permettant d'avoir un inventaire complet des actifs TI.	SSGO (DGSI)	Décembre 2022
	➢ Réaliser les balayages des adresses IP et des URL de la SAAQ (inscription au service du SCT-CGCD).	SSGO (DGSI)	Décembre 2021
	➢ Réaliser les tests selon la planification prévue dans l'entente avec la firme [redacted] (14 tests). Possibilité de revoir la planification en fonction du contexte ex. nouvelle menace, nouveau risque, etc.	SSGO (DGSI)	Décembre 2021

Constat

2. Il n'existe pas de lignes directrices permettant d'identifier, lors de la rédaction d'une entente de services ou d'un contrat, les clauses garantissant le respect des exigences de sécurité de l'information par les fournisseurs. À titre d'exemple, les clauses ayant traits aux habilitations de sécurité pour les ressources externes, qui accèdent à des données sensibles, sont absentes dans certains contrats, bien que requises. Il en va de même pour les exigences de la Société pour l'infonuagique, pour l'utilisation des appareils mobiles, etc.

Impact: Étant donné l'absence de certaines exigences de sécurité dans les contrats, des actifs informationnels de la Société pourraient être utilisés de façon inappropriée voire même être détruits.

RECOMMANDATION

Élaborer des lignes directrices permettant d'identifier clairement les clauses à être intégrées dans les contrats afin de garantir le respect des exigences de sécurité de l'information par les fournisseurs.

Plan d'action - Recommandation 2

Recommandation	Actions prévues	Responsables	Échéances
Élaborer des lignes directrices permettant d'identifier clairement les clauses à être intégrées dans les contrats afin de garantir le respect des exigences de sécurité de l'information par les fournisseurs.	➢ En collaboration avec la Direction de la gestion et de la conformité contractuelle (DGCC) de la VPFCO, revoir le processus d'inclusion des clauses relatives à la sécurité de l'information dans les contrats, notamment pour couvrir de nouvelles préoccupations (appareils mobiles, continuité, etc.). ➢ Pour des dossiers complexes, un architecte en sécurité est attitré pour analyser les clauses à inclure au contrat.	DGSI DGCC	Décembre 2021

Constat

3. La société ne possède pas de programme formel et continu de formation en matière de sécurité de l'information pour l'ensemble du personnel.

Impact: Sans une formation adéquate, des utilisateurs peuvent mettre en péril la sécurité des actifs informationnels de la Société.

RECOMMANDATIONS

3A Mettre en œuvre un programme formel de formation à la sécurité de l'information pour l'ensemble des employés de la Société;

3B Procéder à une évaluation périodique de ce programme afin de s'assurer de son efficacité.

Plan d'action - Recommandations 3

Recommandations	Actions prévues	Responsables	Échéances
3A: Mettre en œuvre un programme formel de formation à la sécurité de l'information pour l'ensemble des employés de la Société.	➢ Assurer, pour tout le personnel de la Société, le déploiement des autoformations mises en place par le Secrétariat du Conseil du trésor (4 capsules). ➢ Mettre en place avec la direction des ressources humaines un processus pour assurer l'inscription des nouveaux employés à ce programme de formation. ➢ Ajouter des activités de formation ou de sensibilisation dans le courant de l'année 2021. ➢ Analyser le besoin de mettre en place une plate-forme automatisée pour gérer les inscriptions aux formations et effectuer le suivi des formations.	DGSI DGRH	31 mai 2021 (1er bloc – 4 capsules) 31 mai 2021 31 décembre 2021 31 décembre 2021
3B: Procéder à une évaluation périodique de ce programme afin de s'assurer de son efficacité.	➢ Effectuer annuellement un questionnaire d'évaluation sur les connaissances en sécurité de l'information.	DGSI	31 décembre 2021

Constat

4. La catégorisation des actifs informationnels de la Société n'est pas complétée. À titre d'exemple, la livraison 1 de CASA n'est pas catégorisée bien que des données sensibles y soient présentes. De plus, la mise à jour du registre d'autorité n'est pas toujours effectuée en temps opportun lors de nouvelles assignations.

Impact: Sans une catégorisation appropriée et la désignation formelle d'un détenteur, certains actifs informationnels de la Société pourraient ne pas bénéficier d'une protection adéquate.

RECOMMANDATIONS

4A Mettre à jour le registre d'autorité dès qu'il y a un changement dans l'assignation d'une responsabilité;

4B S'assurer que l'ensemble des actifs informationnels de la Société, autant numérique que non numérique, soit catégorisé.

Plan d'action - Recommandations 4

Recommandations	Actions prévues	Responsables	Échéances
4A: Mettre à jour le registre d'autorité dès qu'il y a un changement dans l'assignation d'une responsabilité.	➢ Effectuer une mise à jour régulière et en temps opportun du registre jusqu'à l'implantation d'un outil de mise à jour automatique.	DGSI	Mars 2021 Juin 2021 Septembre 2021 Décembre 2021
4B: S'assurer que l'ensemble des actifs informationnels de la Société autant numérique que non numérique, soit catégorisé.	➢ Actifs numériques : o Réaliser la catégorisation des actifs des nouveaux systèmes; o Mettre en place des outils centralisés permettant d'avoir un inventaire complet des actifs TI (initiative 12 du PSIN 2020-2022); o Catégoriser l'ensemble des actifs TI (initiative 13 du PSIN 2020-2022). ➢ Actifs non numériques: o Effectuer l'inventaire des actifs non numériques afin d'effectuer un plan d'action en lien avec les nouveautés.	DGSI	Juin 2021 (CASA) Mars 2022 Juin 2023 Décembre 2021

Constat

5. En décembre 2019, dans le cadre du mandat d'audit *Gestion des incidents,* la DVIEP avait mentionné que la portée du plan de reprise n'avait pas fait l'objet d'une révision récente. De plus, les derniers essais de la reprise informatique ne couvraient pas l'ensemble des éléments inclus dans ce plan. Quant aux deux exercices de reprises planifiés en 2020, ils ont dû faire l'objet de report à cause de la pandémie.

Impact: En l'absence d'exercices de reprise informatique complets et concluants, la Société n'a pas l'assurance qu'elle pourra rétablir l'ensemble de ses activités essentielles à la suite d'un sinistre important. Qui plus est, certaines données essentielles à la reprise de ces activités pourraient être perdues définitivement.

RECOMMANDATIONS

5A Mettre à jour le plan de continuité des activités (PCA) afin d'identifier les activités essentielles de la Société ainsi que leur délai maximal d'interruption;

5B Réviser le plan de reprise informatique afin de s'assurer que l'ensemble des systèmes informatiques supportant le PCA soient pris en charge;

5C Réaliser périodiquement des exercices de reprise complets.

Plan d'action - Recommandations 5

Recommandations	Actions prévues	Responsables	Échéances
5A: Mettre à jour le plan de continuité des activités (PCA) afin d'identifier les activités essentielles de la Société ainsi que leur délai maximal d'interruption.	➢ La responsabilité du PCA relève de la VPFCO. La VPRHMSN s'occupera de la partie BIA du PCA. ➢ Patrimoine : Maintien selon la cible de l'analyse des impacts d'affaires (BIA) de 2015 tel qu'approuvé par le Comité de direction du 17 février 2015. Il sera revu en 2021-2022 dans le cadre des activités de CASA. ➢ CASA: o Analyse et révision de la stratégie du plan de reprise; o Réalisation de la stratégie et mise à jour du BIA.	DGSI	Décembre 2021 Décembre 2022
5B: Réviser le plan de reprise informatique afin de s'assurer que l'ensemble des systèmes informatiques supportant le PCA soit pris en charge.	➢ Patrimoine: assurer l'entretien régulier des plans ➢ CASA: o L1 : Intégrer les activités au plan de reprise; o L2 : Révision de la stratégie du plan de reprise; o L2 : Réalisation de la stratégie.	DGSI	Mars 2021 Décembre 2021 Décembre 2022
5C: Réaliser périodiquement des exercices de reprise complets.	➢ Patrimoine : Réviser le contenu de chaque essai lors de la préparation de l'exercice pour envisager l'ajout d'activités supplémentaires des systèmes patrimoniaux. ➢ L2: Révision de la stratégie du plan de reprise.	DGSI	Novembre 2021 Décembre 2021

Liste des acronymes

Selon l'ordre de la présentation:	
PSIN	Plan de sécurité de l'information numérique
SSGO	Service de la surveillance et de la gestion opérationnelle
DGSI	Direction générale de la sécurité de l'information
SCT-CGCD	Centre gouvernemental de cyberdéfense situé au Secrétariat du Conseil du trésor
DGCC	Direction de la gestion et de la conformité contractuelle
VPFCO	Vice-présidence aux finances et au contrôle organisationnel
DGRH	Direction générale des ressources humaines
PCA	Plan de continuité des activités
VPRHMSN	Vice-présidence aux ressources humaines, matérielles et aux services numériques
BIA	Bilan d'impact sur les activités « Business Impact Analysis »