Aperçu du cadre de protection et de sécurité des renseignements personnels

Le partenariat canadien contre le cancer (le partenariat) remplit un vaste mandat visant à mettre en œuvre une stratégie de lutte contre le cancer afin d'unir les efforts des partenaires de partout au pays et collaborer avec les cancérologues, les organismes caritatifs et les organismes nationaux en matière de santé, les gouvernements, les organismes en matière de cancer, les survivants, etc. Lorsqu'il exécute son mandat, le partenariat collecte, emmagasine et partage une grande quantité de renseignements possédant différentes sensibilités, c'est pourquoi il a aménagé un programme de sécurité des renseignements tout aussi robuste.

Cadre de protection et de sécurité des renseignements personnels du partenariat

Le cadre de protection et de sécurité des renseignements personnels (Figure 1) forme la base du programme de sécurité des renseignements qui inclut une vaste gamme de normes et de politiques relatives aux technologies de l'information. L'ensemble des normes et des politiques relatives aux technologies de l'information et à la gestion des renseignements sont élaborées en fonction des normes de l'industrie et sont conçues pour étayer et pour guider la vaste gamme d'activités des TI en lien avec la sécurité dans le cadre des différents travaux du partenariat. Le programme de sécurité des renseignements a des retombées positives sur l'ensemble de l'organisation grâce aux activités de sécurité du système et aux renseignements opérationnels qui appuient les opérations commerciales stratégiques et quotidiennes ainsi que la surveillance des consultations, des éléments techniques et des politiques de différentes activités de projet qui influent sur les systèmes d'information d'entreprise du partenariat.

Le programme de sécurité des renseignements est géré et exécuté sous l'autorité et l'administration de l'agent de la protection de la vie privée et des services généraux du partenariat. Les rapports de surveillance et de conformité du cadre de protection et de sécurité des renseignements personnels sont présentés chaque année au comité du conseil des finances et de la vérification du partenariat.

Dix éléments essentiels du cadre de protection et de sécurité des renseignements

1. *Groupe de politiques de sécurité d'un système complet et en expansion* qui fournit des conseils sur une vaste gamme de questions relatives à la sécurité.
2. *Examen annuel de l'ensemble des politiques de sécurité du partenariat* afin de veiller à sa pertinence et à son efficacité.
3. *Programme de formation personnalisé portant sur les systèmes de sécurité* exécuté via une formation en ligne, qui comprend des séances de formation annuelles pour tous le personnel ainsi que des séances d'orientation pour tout le nouveau personnel.
4. *Évaluation de la menace et des risques (EMR)* de tous les systèmes d'information et de tous ceux ayant été modifiés de manière significative ainsi que la gestion des mesures correctives découlant de ces évaluations à l'aide de plans de mise en œuvre et de sauvegarde.
5. *Programme de gestion des risques* retraçant et surveillant la mise en œuvre des contrôles de sécurité et des risques à la sécurité au sein des systèmes d'information d'entreprise de l'organisation.
6. *Examens périodiques approfondis de l'accès utilisateur* aux archives de données d'entreprise les plus sensibles.

7. *Conseil consultatif relatif aux modifications apportées aux TI* formé de membres clés du service des TI du partenariat, d'un fournisseur externe expert en TI, d'un membre externe de la sécurité des TI et de gestionnaires de programme, au besoin, pour veiller à ce que les modifications à apporter aux systèmes soient vérifiées et évaluées minutieusement d'une perspective technique et commerciale afin de minimiser les risques.

8. *Examens de la sécurité* des processus d'examen des systèmes du partenariat pour veiller à la détection précoce des problèmes potentiels liés à la sécurité, à la détermination du niveau de risque associé à ces problèmes et à l'atténuation ou à l'acceptation des risques.

9. *La maintenance et l'amélioration continues des systèmes d'information d'entreprise du partenariat* y compris la sécurité de réseau, la gestion de la segmentation et de l'accès afin de minimiser et d'atténuer les risques potentiels pour la sécurité.

10. *Introduction de nouvelles technologies centralisées de gestion de l'identité et de l'accès* afin d'offrir un haut degré d'accès utilisateur à l'ensemble des services de l'organisation et à ceux axés sur le public.

Le service de soutien des technologies de l'information au partenariat

Le directeur des technologies de l'information a la responsabilité de la gestion de la sécurité des renseignements au partenariat et de la direction de la stratégie en matière de sécurité des renseignements. Sous la responsabilité de l'agent de la protection de la vie privée, le directeur des technologies de l'information recommande des politiques en matière de sécurité de l'information en lien avec les initiatives stratégiques, avec l'architecture technologique et avec les questions liées à la sécurité des systèmes.

Le service des technologies de l'information, sous la supervision du directeur des technologies de l'information, est doté de deux gestionnaires en TI à temps plein et d'une équipe d'architectes, d'analystes et de développeurs Web qui sont dévoués à assurer une gestion efficace et rentable des systèmes d'information d'entreprise du Partenariat.

Le partenariat compte également sur une équipe dévouée d'experts externes en sécurité de l'industrie, disponibles sur demande, pour effectuer une évaluation discrète et plus détaillée de la sécurité et pour fournir des conseils portant sur la politique, sur l'architecture des systèmes, sur les pratiques opérationnelles et sur la sécurité des renseignements dans son ensemble. Le partenariat se penche sur les très importantes questions de sécurité en lien avec l'infrastructure de l'entreprise, la vérification, l'évaluation des risques ou les nouveaux projets et les projets existants à l'aide du savoir-faire des fournisseurs et des ressources internes et externes.