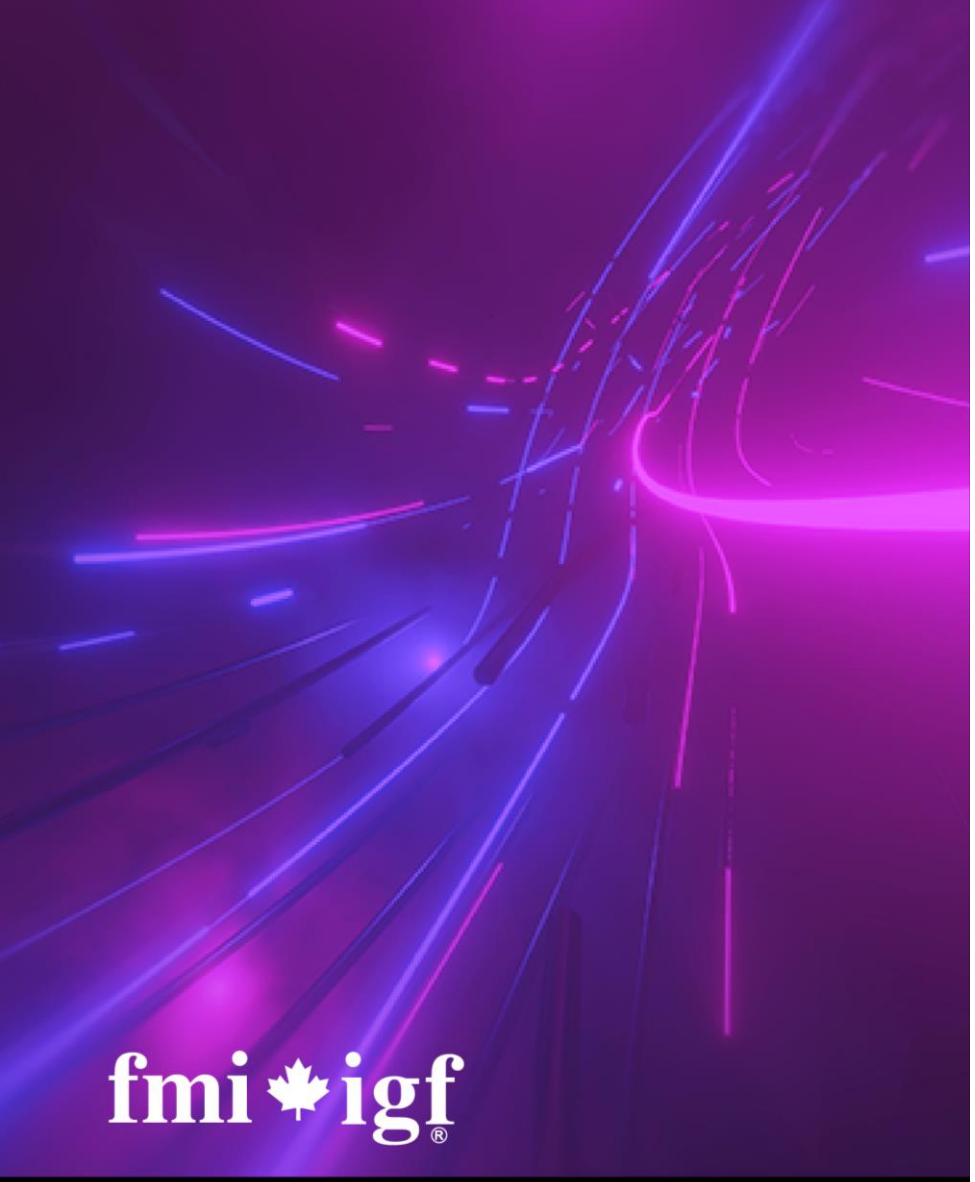


Une approche d’entreprise en matière de cybersécurité

SONY PERRON,

Président, Services partagés Canada

Dans cette présentation

Une compréhension commune des risques liés à la cybersécurité.

L'effet d'une approche d'entreprise sur la posture de cybersécurité.

L’importance de la responsabilité personnelle.

Comment intégrer la cybersécurité dans vos plans.

Cyberrisques

La cybersécurité est toujours une priorité pour SPC.

Les menaces sont en constante augmentation.

La défense à plusieurs couches et l'approche d'entreprise sont essentielles.

Nous devons investir dans les personnes talentueuses pour anticiper les menaces.

Le Comité de sécurité de la technologie de l'information tripartite (CSTIT)

Rôles et responsabilités

Approche pangouvernementale

La sécurité du gouvernement et la continuité des programmes et des services du gouvernement du Canada (GC) dépendent de la capacité des ministères et des organismes ainsi que du gouvernement pour gérer les événements liés à la cybersécurité.

IDENTIFIER • PROTÉGER • DÉTECTER • RÉPONDRE • RÉCUPÉRER

Orientation stratégique et surveillance
Secrétariat du Conseil du Trésor

Établir une vision et une orientation stratégiques pour les services d'entreprise, de l'information, des données, des technologies de l'information (TI) et de la cybersécurité;

Prise de décision sur la gestion des risques de cybersécurité au nom du GC;

Attribuer à un haut fonctionnaire la mise en œuvre d'une réponse spécifique aux événements de cybersécurité.

Services de réseaux et de sécurité
Services partagés Canada

Offrir certains services liés au courriel, aux centres de données, aux réseaux et aux utilisateurs d'appareils technologiques, y compris les services de sécurité de TI;

Surveiller les appareils et les réseaux électroniques ministériels;

Réaliser les identifications et les enquête concernant des problèmes et mise en œuvre de mesures correctives en cas d'utilisation inacceptable.

Cyberdéfense
Centre canadien pour la cybersécurité

Leadership, conseils et orientation concernant les questions techniques liées à la SÉCURITÉ DE LA TI;

Protection et surveillance de l'information et de l'infrastructure électronique;

Identification, protection et atténuation des menaces contre les cyberévénements;

Diriger le développement de source d'approvisionnement de confiance;

Autorité nationale pour la sécurité des communications (SECOM).

Gestion de la cybersécurité
Ministères et organismes

Fonction de gestion de la cybersécurité ministérielle;

Élaborer et offrir des services axés sur les clients dès la conception, y compris la sécurité;

Protège les informations sensibles sous le contrôle du ministère;

Signaler les événements et les incidents de cybersécurité;

S'assurer que des mesures correctives appropriées et opportunes sont prises.

Défense du périmètre/Intégrité de la chaîne d’approvisionnement

Contrôles et surveillance active de l'environnement réseau du GdC.

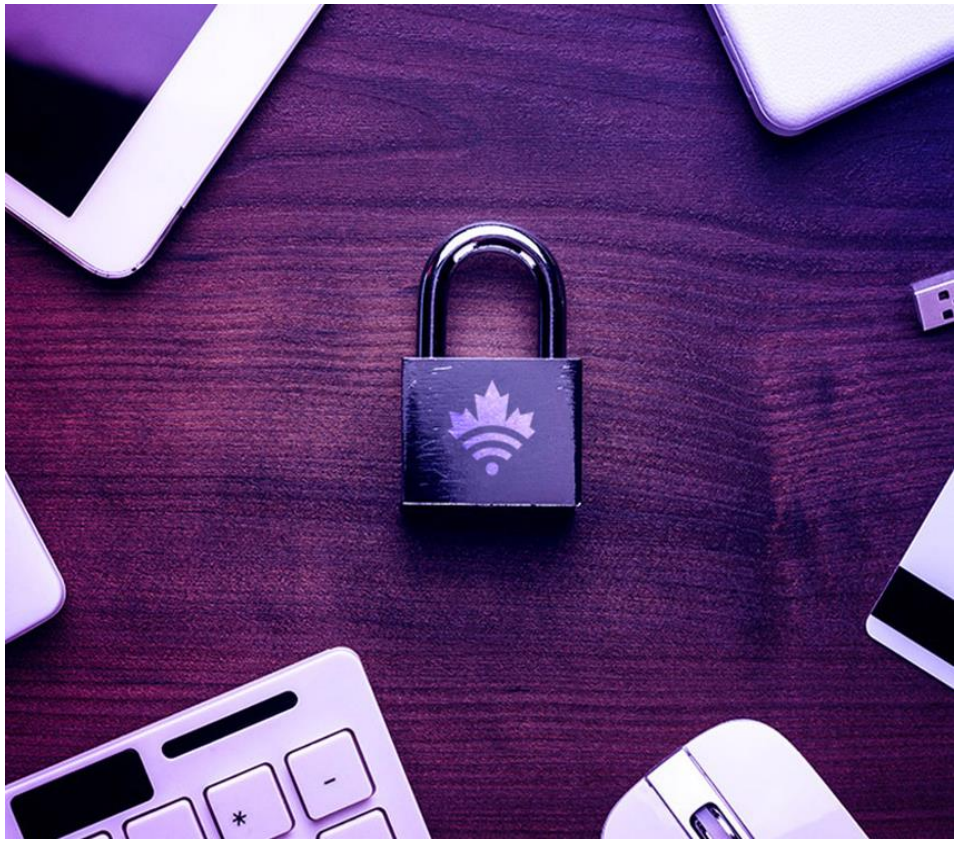
Achats de services et d'équipements soumis aux normes d'intégrité les plus strictes.

Modernisation de l'infrastructure du centre de données du GdC.

Mise en œuvre sécurisée de l'utilisation de l'infonuagiqueue publique.

Les applications et les technologies obsolètes constituent un facteur ou un risque permanent.

Modernisation



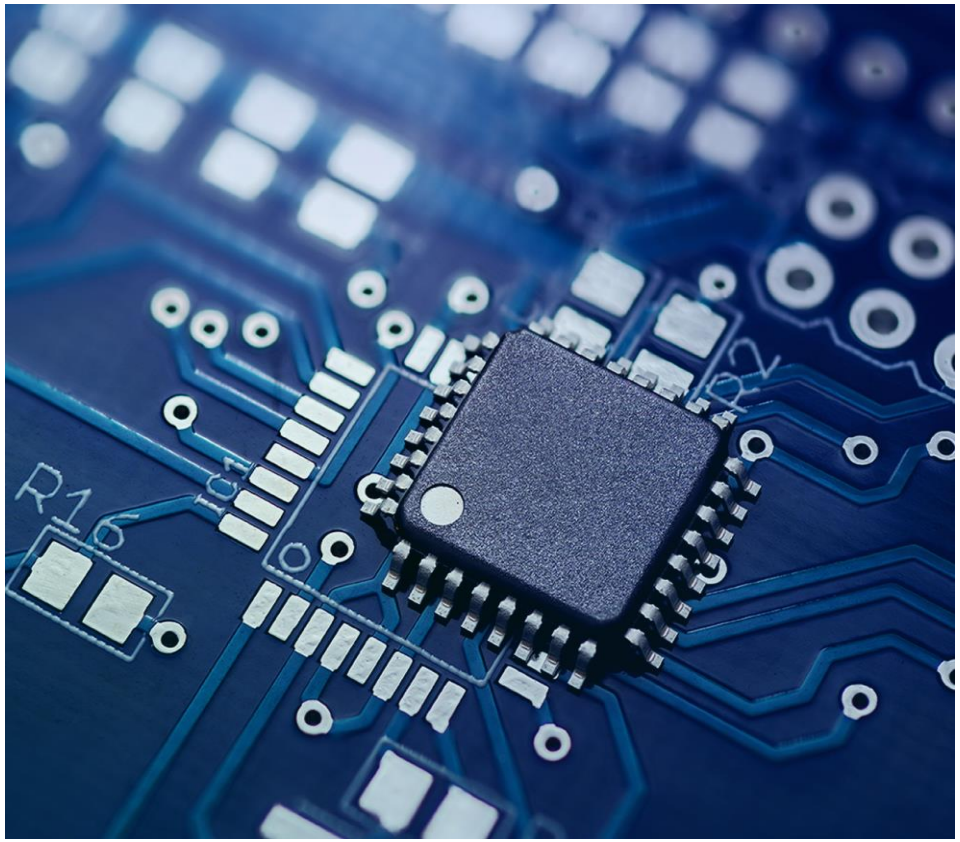
Normalisation, simplification, visibilité.

La conception d’un réseau sécuritaire de A à Z minimise les défauts qui pourraient compromettre la sécurité.

Un réseau d’entreprise partagé améliore la fiabilité et la stabilité, ce qui réduit le temps et les efforts que nous prenons à régler des problèmes.

Renforcer la capacité à réagir à un cyberévénement.

Le Centre canadien pour la cybersécurité



Créé en 2018 dans le cadre du Centre de la sécurité des télécommunications.

La plupart des systèmes de sécurité sont conçus et gérés par SPC.

Le cybercentre utilise des solutions complémentaires pour compléter ces systèmes (par exemple, un capteur basé sur l'hôte pour la surveillance et la protection des points d'extrémité du GdC).

Approche d’entreprise

L’objectif est de réduire la quantité de nombreuses solutions de TI semblables du gouvernement du Canada qui répondent aux besoins de TI les plus communs.

C’est essentiel à la réussite d’un gouvernement numérique.

Notre réponse à la pandémie a démontré les avantages d'une approche d'entreprise à l'échelle du gouvernement pour les services d'infrastructure informatique.

Automatisation à titre de protection

Le gouvernement du Canada dispose de systèmes qui préviennent automatiquement et rapidement les attaques au moyen d'algorithmes d'apprentissage par machine avancés.

La conscientisation partagée est essentielle.

L'information doit être disponible pour toutes les personnes concernées au même moment.

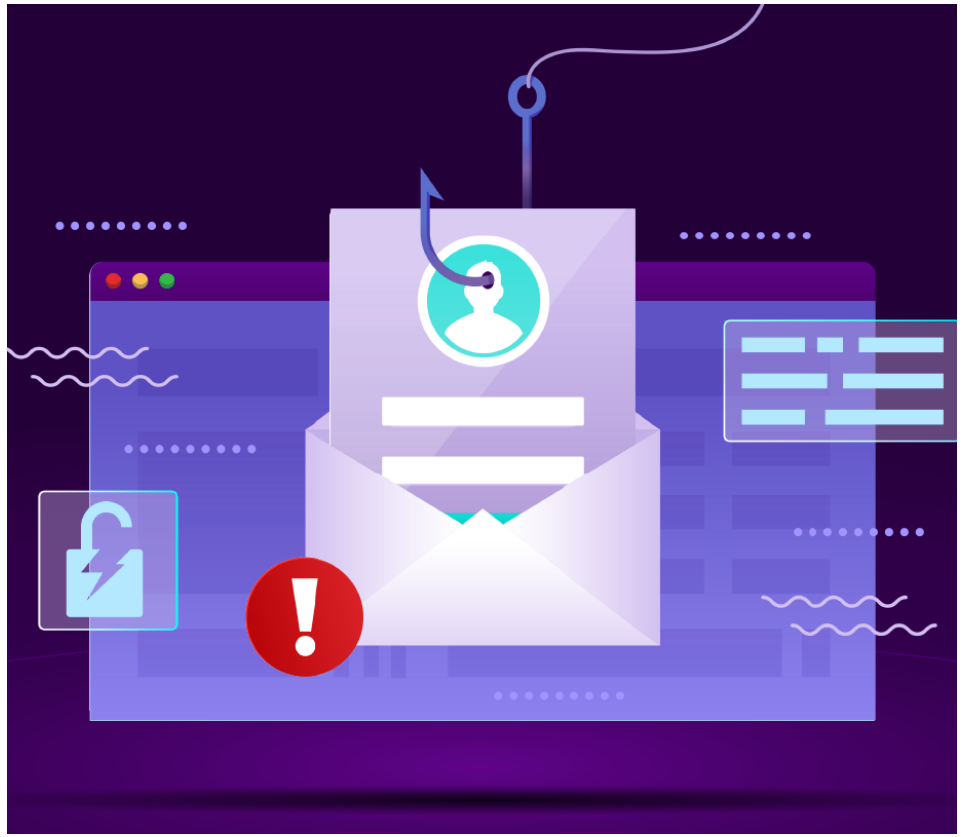
Ce que les gestionnaires financiers doivent rechercher

Provision dans le budget et le plan financier pour la cybersécurité.

Considérer le coût en cas de défaillance de la solution numérique due à une cyberattaque.

Tirer parti des solutions communes plutôt que des mesures propres à chaque service.

Responsabilité personnelle

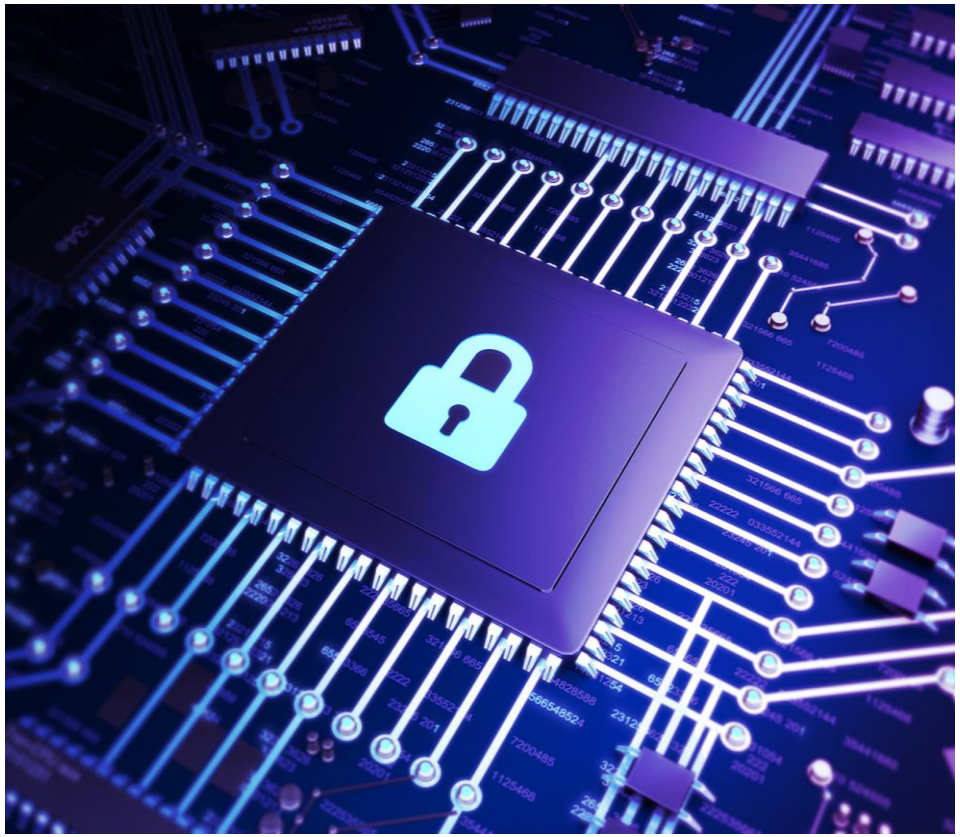


L’erreur humaine et les impulsions touchent grandement la sécurité du réseau (p. ex. l’hameçonnage).

Obtenez des ressources de formation et participez à l’élaboration d’un plan de conscientisation et de formation en matière de sécurité.

Communiquez avec les employés au sujet de leur rôle en matière de prévention des cyberattaques.

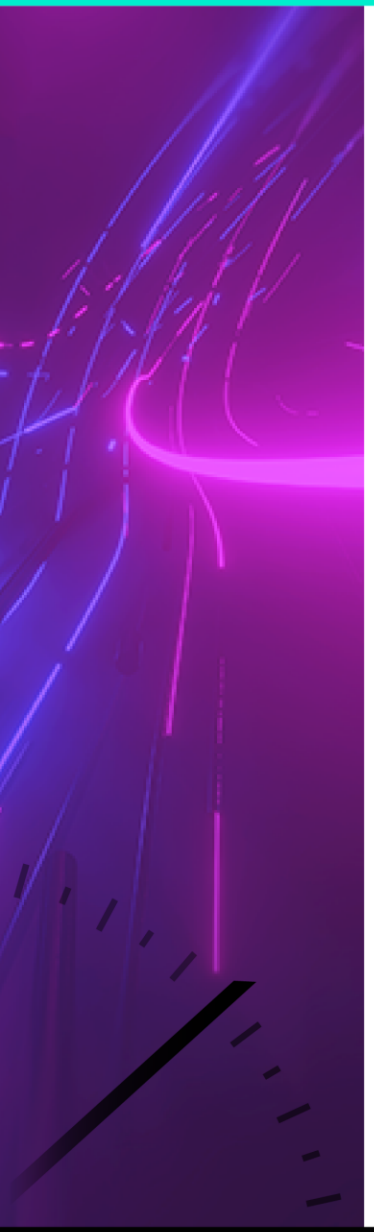
Points à retenir



SPC s’affaire à offrir un approvisionnement efficace des solutions, et la disponibilité des solutions et des plateformes d’hébergement.

Mon objectif est que l’approche d’entreprise de SPC en matière de cybersécurité devienne une feuille de route pour les services de cybersécurité d’entreprise.

Une approche d’entreprise ne concerne pas seulement SPC, elle nous concerne tous.



Questions?