Webinaire sur la cybersécurité

FSRA
Financial Services Regulatory Authority of Ontario

Date : 29 novembre 2022

Ontario

Nos conférenciers

Caroline Blouin
ARSF
Vice-présidente directrice,
Régimes de retraite

David Bartucci
ARSF
Directeur, Relations avec les intervenants du secteur des régimes de retraite et projets spéciaux

Ted Harman
Accent Solutions
Assurances
Président

Ryan Wilson
Partenaire EY Canada
en matière de
cybersécurité

Ordre du jour

- Présentations et règles de base
- Témoignages d’experts – Ted Harman partage son expérience
- Faits saillants de l’enquête menée auprès du secteur des régimes de retraite de l’Ontario – Conclusions majeures de l’enquête
- Approche réglementaire – Aperçu des nouvelles directives de l’ACOR
- Témoignages d’experts – Ryan Wilson présente sa vision des cybermenaces, les raisons pour lesquelles il est important de les comprendre et ce à quoi les administrateurs devraient penser.

FSRA
Financial Services Regulatory Authority of Ontario

Ontario

Témoignages d’experts – Ted Harman partage son expérience

- Future Electronics c. Chubb
- Cybermenace d’extorsion personnelle
- Ressources

Témoignages d'experts – La tentative d'extorsion de Ted Harman

Expéditeur : ted.harman@accentassurance.com
Envoyé : Vendredi 21 octobre 2022, 17 h 40
Destinataires : Ted Harman
Objet : Vous avez des créances impayées.

Bonjour !

Malheureusement, de mauvaises nouvelles vous attendent.
Depuis quelques mois, je me suis procuré l'accès aux appareils que vous utilisiez pour naviguer sur Internet. Après quoi, les activités que vous avez menées sur Internet ont fait l'objet d'un suivi de ma part.

Veuillez consulter la séquence des événements passés :
Dans le passé, je me suis procuré auprès de pirates informatiques l'accès à de nombreux comptes de messagerie (de nos jours, il s'agit d'une tâche très simple pouvant être effectuée en ligne).
De toute évidence, je me suis connecté sans effort à votre compte de messagerie (ted.harman@accentassurance.com).

Une semaine après, j'ai réussi à installer le virus Trojan (cheval de Troie) sur les systèmes d'exploitation de tous vos appareils que vous utilisez pour accéder à vos courriels.
En réalité, c'était plutôt simple (parce que vous cliquiez sur les liens dans les courriels de votre boîte de réception). Toute chose intelligente est plutôt simple. (^-^)

Le logiciel que j'utilise me permet de contrôler toutes les commandes de vos appareils, comme la caméra vidéo, le microphone et le clavier.
Et j'ai réussi à télécharger sur mes serveurs toutes vos données personnelles, l'historique de votre navigation sur Internet et vos photos. Je suis capable de lire tous vos messages, vos courriels, les pages de vos réseaux sociaux, votre liste de contacts et même l'historique de vos conversations.
Le virus réactualise sans cesse ses signatures (puisqu'il est basé sur un programme de gestion de périphériques) et

demeure invisible à votre antivirus. Vous devriez donc déjà comprendre la raison pour laquelle mes activités sont restées

inaperçues jusqu'à ce moment précis...

On peut résoudre cela comme suit :

Il vous suffit d'effectuer un virement de 1450 $ US sur mon compte (équivalent en bitcoins en fonction du taux de change au moment de votre virement). Quand la transaction sera validée, je procéderai à la suppression de tous ces éléments pervers sans délai.
Après quoi, nous pourrons prétendre que nous ne nous sommes jamais rencontrés auparavant. Je vous assure en outre que tous les logiciels nuisibles seront supprimés de tous vos dispositifs. Rassurez-vous, je tiens mes promesses.

Voilà un accord plutôt équitable à un prix bas, sachant que j'ai consacré beaucoup d'efforts à parcourir votre profil et votre trafic pendant une longue période.
Il suffit de chercher toutes les informations nécessaires en ligne pour savoir comment acheter et envoyer des bitcoins. Ci-

dessous mon portefeuille de bitcoins : 17kmbhxxMsrFhmQNim1jbjD6AeBUQ2SbYp

Le délai accordé est de 48 heures après l'ouverture de ce courriel (2 jours pour être précis).

Faits saillants – Conclusions majeures de l'enquête sur la cybersécurité de l'ARSF

20

Réponses à l'enquête

L'enquête a été transmise de manière aléatoire à des régimes de taille variable et dans l'ensemble du secteur :

- **Régimes à prestations déterminées**
- **Régimes de retraite interentreprises**
- **Régimes à cotisations déterminées**

1. Contrôles en matière de cybersécurité

- Nombre de membres de l'équipe de cybersécurité variant entre 1 et 349.
- **Politique :** Quasiment toutes les entreprises ont adopté une politique, dont la moitié environ est révisée chaque année. Un petit nombre d'entre elles n'ont pas adopté de politique explicite.

Contrôles de la sécurité des points d'accès*.	Oui
Protection avancée contre les logiciels malveillants (notamment la protection contre les attaques au jour zéro)	17
Technologie de prévention de la perte de données	10
Détection et réponse aux points d'accès	13
Cryptage intégral du disque	12
Norme(s) de renforcement des systèmes recommandée(s) par le secteur (par exemple, services d'information CIS)	8 (1 en cours)
Protection traditionnelle contre les virus et les logiciels malveillants	18

*1 répondant supprimé du décompte

2. Tiers

- **Mécanisme d'examen des politiques commerciales (MEPC)** Près de la moitié des entreprises ont mis en place un MEPC. La plupart des MEPC sont intégrés programme de gestion des fournisseurs.
- **Résultats :** Dans la plupart des cas, les intervenants ayant recours à des fournisseurs tiers sont dotés d'un programme formel de réglementation, de législation et de conformité qui leur permet de partager leurs résultats ou leur attestation de conformité.

Faits saillants – Conclusions majeures de l'enquête sur la cybersécurité de l'ARSF

3. Rapport d'incident

- **Politique et plan de réaction aux incidents** La plupart ont adopté une politique, une est en cours de le faire, quelques-unes n'en ont pas encore.
- **Activités postérieures à l'incident :** Tous exécutent des activités relatives à l'incident

4. Exposition aux risques

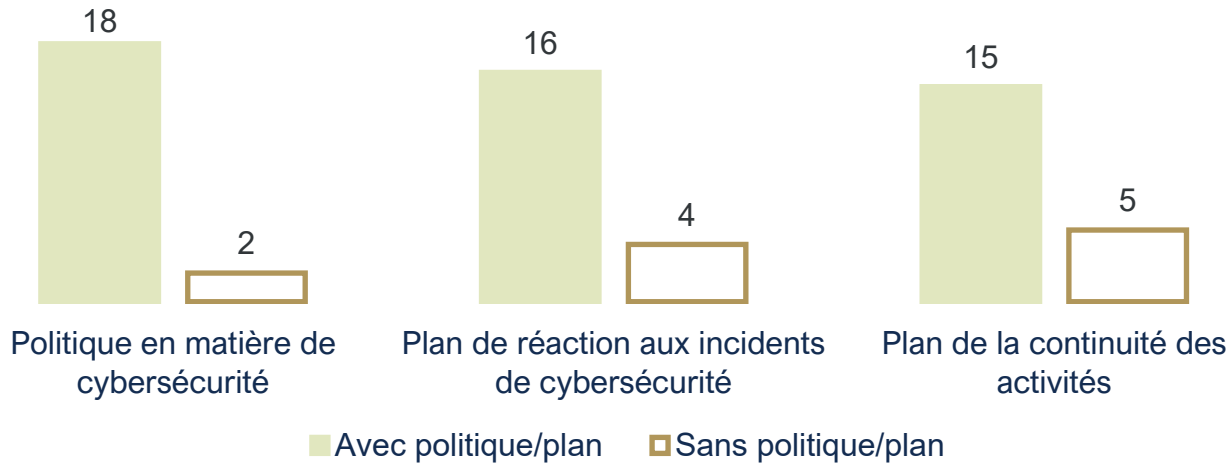
- **Évaluation des risques :** Plus de la moitié ont adopté une méthodologie normalisée pour évaluer les risques liés à la cybercriminalité et à la protection des renseignements personnels. Un peu plus de la moitié évalue les cyberrisques de manière formelle
- **Base de données de renseignements :** Toutes les entreprises collectent et stockent des renseignements personnels identifiables. Plus de la moitié d'entre elles recueillent des informations médicales ou de santé protégées.

5. Contrôles humains

- **Programme de formation :**
  - La majorité d'entre elles sont dotées d'un programme de formation à la vigilance en matière de sécurité
  - Près de la moitié d'entre elles ont suivi une formation spécialisée en matière de cyberrisque sur la manière d'administrer les fonds en toute sécurité.
- **Mise à l'essai :** Pratiquement toutes les entreprises effectuent des tests permanents d'hameçonnage et de prédisposition au risque des utilisateurs.

Faits saillants – Conclusions majeures de l'enquête sur la cybersécurité de l'ARSF

- La majorité des régimes ont adopté une politique en matière de cybersécurité. Vu la taille relativement réduite de l'échantillon, on ne peut pas déterminer la taille moyenne d'une équipe de professionnels en cybersécurité. Certaines entreprises ne comptent qu'un seul professionnel en cybersécurité.



- Les exigences réglementaires, juridiques et de conformité liées à la cybersécurité, à la protection des données et à la confidentialité peuvent varier et comporter un ou plusieurs des éléments suivants : BSIF, AMF, ICP, SAD, LPRPDE, RGPD
  - 15 ont répondu favorablement à l'idée de faire rapport sur les failles cybernétiques aux autorités réglementaires et requises ; 5 ont répondu défavorablement.

Faits saillants – Conclusions majeures de l'enquête sur la cybersécurité de l'ARSF

- La totalité des entreprises est en mesure de surveiller tous les systèmes informatiques (notamment les ententes d'impartition pour tous les systèmes et applications) contre les cyberattaques.
  - Dans certains cas, les contrôles ne sont effectués que pendant les heures de bureau.

- Les types les plus courants de cyberattaque réussie que les organisations ont subis au cours des 12 derniers mois :

1. Hameçonnage
2. Compromission d'informations d'identification
3. Attaque par déni de service
4. Rançongiciels

Approche réglementaire

- L'ARSF est membre de l'Association canadienne des organismes de contrôle des régimes de retraite (ACOR). L'ACOR a privilégié la gestion des risques et la cybersécurité.

- L'ACOR a publié une version préliminaire de lignes directrices en matière de cybersécurité aux fins de consultation publique en juin – les commentaires sont actuellement examinés. L'ACOR a également reçu des commentaires favorables en ce qui concerne son intégration dans une directive plus large sur la gestion des risques.

- Les nouvelles lignes directrices sur la gestion des risques, dont une section est consacrée à la cybersécurité, sont en cours d'élaboration, pour une consultation publique attendue au printemps 2023.

- Une version préliminaire des lignes directrices en matière de cybersécurité est disponible sur le site Web de l'ACOR. capsa-acor.org

Concepts clés de la version préliminaire des lignes directrices

- Le risque cybernétique représente un risque majeur pour tous les régimes, toutes tailles et caractéristiques confondues. Il faut régulièrement le revoir et l'évaluer pour s'assurer que des contrôles adéquats permettent au régime de maîtriser le risque. Les cyberrisques sont complexes et en constante évolution. Ils nécessitent une réponse adaptée.
- Les administrateurs de régimes doivent s'acquitter de leurs responsabilités fiduciaires et faire en sorte que le régime soit doté des compétences, de l'expertise et/ou de la formation nécessaires pour comprendre et faire face aux cyberrisques.
- Les rôles et les responsabilités en matière de cyberrisque des entreprises doivent être clairement définis, attribués et compris, notamment en ce qui concerne toute activité déléguée à des fournisseurs de services tiers (et tous les sous-traitants admissibles).
- Il convient que les administrateurs de régimes adoptent une stratégie pour répondre aux cyberincidents et les signaler.

Comprendre la cybermenace (méthodes et fondements)

Leçon à retenir : Il ressort des divulgations que les cyberattaques visent essentiellement des gains financiers, ce qui explique l'existence de deux axes majeurs : les rançongiciels et le vol de renseignements personnels ou de propriété intellectuelle.

Par ailleurs, les attaques visant à interrompre les systèmes clés d'une entreprise entraînent des pertes financières même si les données des clients ne sont pas exfiltrées.

Les cyberrisques sont présents dans toutes les entreprises, sans distinction de taille.

Qu’est-ce que la cybersécurité et pourquoi elle est essentielle pour vous ?

Le cyberrisque peut être étudié à travers

Risk = threat x vulnerability x impact

(prevalence of the threat) (likelihood vulnerability can be exploited) (the potential financial, operational, legal or regulatory effect)

- **Les cybermenaces sont toujours plus subtiles et plus sophistiquées**
  - Tous les jours, plus de 200 000 menaces sont disséminées dans le milieu informatique et seulement 56 % d’entre elles sont « détectables ».
  - Le personnel interne permet involontairement 95 % des attaques.
  - Les hacktivistes représentent à présent le deuxième groupe d’attaque le plus important.
- **La fréquence des vulnérabilités (surface d'attaque) augmente.**
  - La pandémie à la Covid a favorisé une évolution de 10 ans d’innovation en moins d’un an.
  - Interconnectivité avec les tiers
- **Les effets se diversifient également**
  - La proportion totale de ces attaques perturbatrices (rançongiciels) a augmenté de 59 % entre 2020 et 2021.
  - La cybersécurité constitue un thème ESG/durabilité toujours plus important.

Manchettes récentes

- Brèche dans les données personnelles d’un régime de retraite, un tiers est accusé.
- Une cyberattaque a coûté 3,5 millions de dollars à un régime de retraite.
- Une brèche de données frappe un prestataire de services de retraite et fait 50 000 victimes.
- Un régime de retraite (401k) déclenche une action en justice contre les fiduciaires du régime.

Leçon à retenir : La taille et la complexité des cyberattaques évoluent à grande vitesse.

Gouvernance du risque en matière de cybersécurité

Les meilleures pratiques pour le personnel de direction et les administrateurs

1. Identifier et établir

Définissez votre stratégie

Renforcer l'attention du conseil d'administration et/ou du comité sur ces points.

Restez à l'affût

Répondre aux nouveaux problèmes et menaces découlant de la transition au travail à distance.

Calculer la valeur à risque

Confronter la valeur à risque en dollars au seuil de tolérance au risque du conseil d'administration.

2. Évaluer et sécuriser

Intégrer la sécurité dès le départ

Adhérer au principe de la « confiance dès la conception » au moment de la conception de nouvelles technologies, de nouveaux produits et de nouveaux arrangements commerciaux.

Évaluer le programme cybernétique

Recourir à une évaluation indépendante du programme cybernétique

Comprendre le protocole permettant de passer rapidement à l'échelon supérieur

Prévoir un plan de communication précis indiquant quand le conseil d'administration doit être informé.

3. Gérer et surveiller

Gérer les risques liés aux tiers

Maîtriser les processus d'identification, d'évaluation et de gestion des risques liés aux fournisseurs de services et à la chaîne d'approvisionnement.

Capacités d'intervention d'urgence et de rétablissement

Augmenter la capacité de réaction par des simulations et en établissant des protocoles avec des professionnels tiers, et ce, bien avant une éventuelle crise.

Observer l'évolution des pratiques

Se tenir à l'affût des informations publiées par les pairs pendant les deux ou trois dernières années et les comparer à celles-ci.

Questions

Mot de la fin

Merci de votre participation.

Pour toute question supplémentaire découlant du webinaire, veuillez la faire parvenir par courriel à l'adresse suivante Karima.Shajani@fsrao.ca