la | Événements
les affaires

Cybersécurité

Mieux gérer le risque dans un environnement informatique de plus en plus ouvert

25 mars 2015
Montréal

BÉNÉFICIEZ DE L'EXPÉRIENCE DE

AIG · Association de la sécurité de l'information du Québec · Borden Ladner Gervais
Caisse de dépôt et placement du Québec · Chubb · École de criminologie de l'Université de Montréal
École Polytechnique de Montréal · GoSecure · Intrasecure · ISACA Montréal
Rona · SANS Institute · Securitycompass.com · Université McGill · Xittel

Jusqu'à 600 $ * de rabais
avant le 29 janv.
* EN MENTIONNANT LE CODE PROMO WEB

www.lesaffaires.com/evenements/cybersecurite ou 514 392-4298

En partenariat avec : BFL CANADA Cabinet de services financiers

Avec le soutien de : ASIQ Association de la sécurité de l'information du Québec ; ISACA Fiabilisez, optimisez et rentabilisez les systèmes d'information Section de Montréal

la | Événements les affaires

Cybersécurité

Mieux gérer le risque dans un environnement informatique de plus en plus ouvert

25 mars 2015
Montréal

Des études récentes de Cisco révèlent que **60 % des entreprises canadiennes ne se sont pas dotées d'une stratégie ou d'une politique de sécurité informatique.** Selon une recherche de PwC, **117 000 cyberattaques** sont commises chaque jour dans le monde, ce qui représente que **29 % de tous les incidents**. Selon une enquête de *Global State of Information Security*, le coût global estimé de la cybercriminalité pour 2014 dépasse les **23 milliards de dollars américains**, et ce, pour les seuls incidents détectés. Ce constat en dit long sur la capacité des entreprises à intégrer des outils de cybersécurité efficaces.

Ne niez plus l'évidence et assurez vos arrières ! Participez cet événement *Les Affaires* sur la cybersécurité le **25 mars** prochain. Nous avons réuni pour vous des experts en cybersécurité et en gestion du risque, des membres de conseils d'administration et des gestionnaires TI, marketing, ressources humaines et finances, afin de vous assister dans l'implantation des meilleures pratiques de gestion du risque cybernétique dans votre organisation.

Venez échanger avec des professionnels d'organisations telles que :

AIG · Association de la sécurité de l'information du Québec
Borden Ladner Gervais · Caisse de dépôt et placement du Québec
Chubb · École de criminologie de l'Université de Montréal
École Polytechnique de Montréal · GoSecure · Intrasecure · ISACA Montréal
Rona · SANS Institute · Securitycompass.com · Université McGill · Xittel

La conférence sur la cybersécurité met en avant vos préoccupations en matière de **gouvernance**, de **cyber-assurance** et de **gestion du risque cybernétique**. Nos experts présenteront les nouvelles **stratégies en cybersécurité** et les meilleures pratiques de **protection des données personnelles**. Écoutez et échangez avec nos conférenciers, et développez dans votre organisation une politique des **meilleures pratiques** qui contribueront à réduire les dommages d'une éventuelle cyberattaque.

Au plaisir de vous rencontrer le 25 mars prochain,

Gaëtan Bourgoin
Gestionnaire de projets, contenu, sénior
Événements *Les Affaires*

Poussez plus loin votre gestion de risque en cybersécurité en participant à nos ateliers pratiques !

Jusqu'à 600 $* de rabais avant le 29 janv.
CODE PROMO requis

5 bonnes raisons de participer

- **Apprenez à mieux évaluer et à gérer le risque lié à la cybersécurité grâce à des pratiques qui ont fait leurs preuves**
- **Sensibilisez tous les employés de votre organisation au risque de cyberattaque**
- **Donnez les bons outils de gestion à vos équipes TI, afin qu'elles puissent contrer les invasions de systèmes**
- **Démystifiez les risques de brèches de sécurité, de compromission de la confidentialité, de menaces avancées et de hameçonnage**
- **Voyez comment développer une vision commune avec le CA de l'organisation en matière de gestion du risque informatique**

Inscription : lesaffaires.com/evenements/cybersecurite ou 514 392-4298

Cybersécurité

Conférence

mercredi 25 mars 2015

8 h 00 ACCUEIL DES PARTICIPANTS

8 h 30 MOT D'OUVERTURE DU COPRÉSIDENT D'HONNEUR

Louis Plourde
Président
ASSOCIATION DE LA SÉCURITÉ DE L'INFORMATION DU QUÉBEC (ASIQ)

8 h 45 ÉTUDE DE CAS

Obtenez une meilleure gouvernance grâce à une vision commune de la gestion du risque informatique

Marc Lafrance
Vice-président Planification, Architecture et Gouvernance
CAISSE DE DÉPÔT ET PLACEMENT DU QUÉBEC

Avez-vous l'impression de ne pas parler la même langue que les membres du CA ou du comité de vérification lorsque vous abordez les questions de cybersécurité ? Pourquoi l'inaction peut s'avérer dangereuse en matière de cybercriminalité ? Apprenez d'une organisation qui a placé la gestion des risques au cœur de ses pratiques, et sachez :

- Démontrer aux membres du CA les avantages d'une gestion hyperprudente de la cybersécurité ;
- Aligner la gestion du risque TI sur les menaces que représente le cybercrime.

« *Le taux de détection des incidents liés à la cybersécurité au Canada a diminué de 15 % en 2014.* »

Source : Étude Price Waterhouse Cooper, 2014

9 h 30 EXPERTISE

Développez des stratégies de sécurité efficaces pour contrer les nouvelles tendances d'attaques et d'intrusions

Michel Cusin
Mentor
SANS INSTITUTE

La réalité des cyberattaques et de la sécurité de l'information a beaucoup changé. Face à des menaces constamment renouvelées, les moyens de défense traditionnels ne sont désormais plus suffisants. Quels que soient les mécanismes de défense mis en place, ils sont contournés par les pirates qui compromettent systématiquement vos infrastructures. Le risque évolue et vous devez en faire autant.

- Quel est le portrait actuel des différents types de menaces ?
- Comment les cybercriminels parviennent-ils à s'introduire dans vos systèmes ?
- Quelles stratégies devriez-vous mettre en place afin d'effectuer une surveillance adéquate de vos infrastructures technologiques, une meilleure détection d'intrusion et une réponse plus efficace aux incidents ?

10 h 15 PAUSE RÉSEAUTAGE

« *Les entreprises de taille moyenne ont augmenté leur budget de cyberdéfense de 74 % en 2014.* »

Source : Étude Price Waterhouse Cooper, 2014

10 h 30 ÉTUDE DE CAS

Post-mortem d'une attaque : le dur apprentissage d'une entreprise qui ne se sentait pas menacée

Robert Proulx
Président et chef de la direction
XITTEL

Sylvain Gélinas
Vice-président Opérations
XITTEL

Victime en 2013 d'une cyberattaque considérée comme l'une des plus virulentes en Amérique du Nord, Xittel a su mettre en œuvre toutes les ressources dont elle disposait pour sortir gagnante de cette épreuve. Voyez comment un concurrent a causé à Xittel des pertes financières considérables au moyen d'un outil d'attaque par saturation (*Distributed Denial of Service*) obtenu sur le Web pour quelques centaines de dollars seulement. Rencontrez les dirigeants de Xittel et :

- Développez une capacité de détection et de gestion des incidents dans votre organisation afin de répondre plus efficacement aux attaques ;
- Contrez le faux sentiment de sécurité (ça n'arrive qu'aux autres) à l'échelle de votre organisation ;
- Évaluez adéquatement la courbe d'apprentissage de votre organisation afin de développer des solutions de sécurité informatique adaptées à vos besoins ;
- Apprenez les meilleures pratiques pour reconstruire votre organisation à la suite d'une cyberattaque.

11 h 15 ÉTUDE DE CAS

Améliorez et évaluez vos processus de gestion du risque afin de mieux contrer les brèches de sécurité et les menaces cybernétiques

Hugo Dominguez
Directeur infrastructure TI, technologie de l'information
UNIVERSITÉ MCGILL

Près de 7 entreprises sur 10, tous secteurs confondus, ont rapporté 5 866 attaques*, soit 16,5 attaques par jour environ. Or, seulement 22 % d'entre elles avaient mis en place des processus d'évaluation et de gestion des cyber-risques.

- Comment mettre en place des processus de gestion du risque efficaces afin d'assurer une gouvernance adéquate ?
- Sachez bien cerner les ressources matérielles et professionnelles qui vous soutiendront efficacement ;
- Évaluez judicieusement le degré de vulnérabilité de votre organisation et faites une gestion du risque *Lean* afin de maximiser vos investissements.

** Source : International cyber Protection Alliance*

12 h 00 DÎNER RÉSEAUTAGE

13 h 30 MOT DU COPRÉSIDENT D'HONNEUR

Vincent Milette
Président
ISACA MONTRÉAL

13 h 45 ÉTUDE DE CAS

Engagez tous les employés de votre organisation dans la lutte à la cybercriminalité

Adonis Sawan
Chef de service, sécurité de l'information
RONA

Selon une étude Telus-Rotman, plus du tiers des brèches informatiques sont causées par les employés. La clé du succès pour combattre les intrusions reste une politique interne bien encadrée en lien avec des solutions technologiques efficaces. Dans un environnement de plus en plus ouvert, il est primordial de sensibiliser les employés de votre organisation à la cybersécurité et de savoir :

- Comment développer un programme de sensibilisation au risque cybernétique à l'interne ?
- Quels éléments importants faut-il inclure à une formation sur la gestion du risque ?
- Quelles sont les stratégies les plus efficaces pour contrôler adéquatement la navigation Web du personnel ?
- Vulnérabilité de l'entreprise : comment la démontrer aux employés sans créer la panique ?

14 h 30 PAUSE RÉSEAUTAGE

« Le coût d'une assurance Data Risks est estimé entre 3 et 5 % du budget sécurité informatique d'une entreprise. »

Source : Hiscox France

« 50 % des attaques sont détectées plus de trois mois après l'intrusion initiale. »

Source : Trustwave Global Security Report, 2013

14 h 45 PANEL DE DISCUSSION

Assurance de dommages et cyberattaques : démystifiez la cyber-assurance afin d'éviter les mauvaises surprises.

Matthew Davies
Director – Professional, Media & Cyber Liability
CHUBB DU CANADA COMPAGNIE D'ASSURANCE

Jacqueline Detablan
Directrice régionale de souscription responsabilité professionnelle
AIG

Jean-François De Rico
Avocat, associé
LANGLOIS KRONSTRÖM DESJARDINS

Pascal Fortin
Président-directeur général
GOSECURE

La cyber-assurance donne des maux de têtes à ceux qui tentent de chiffrer le risque en cybersécurité. Dans son rapport de 2013, le *Ponemon Institute* évalue à 130 $ le coût par données subtilisées, ce qui amènerait à 14 G $ les pertes totales subies par Target des suites de la cyberattaque dont elle a été victime en 2013. Des entreprises comme Target ont appris à quel point les pertes sont phénoménales.

- Comment évaluer vos risques sur le plan monétaire, afin de bien calculer le montant de votre police d'assurance ?
- Comment atteindre l'équilibre entre garantie et coût ?
- Comment développer un modèle de calcul du cyber-risque ?
- Comment analyser une proposition de couverture d'assurance risques cybernétiques ?
- Déclarations frauduleuses volontaires ou involontaires : comment vous assurer que vos déclarations quant à l'état de votre système de sécurité n'annule votre assurance ?

Ce panel de discussion se déroulera en anglais et en français.

« *46 % des attaques ont été menées selon un mode opératoire inconnu.* »

Source : Trustwave Global Security Report, 2013

« *La cybercriminalité augmente sans cesse au Canada.* »

Source : Global State on Information Security Survey, 2014

15 h 45 EXPERTISE

Soyez prêts : dotez-vous d'un plan de gestion de crise efficace et adapté à votre entreprise

Éric Parent
Enseignant au programme de cybersécurité/ cyberterrorisme
ÉCOLE POLYTECHNIQUE DE MONTRÉAL

Lors d'une attaque ou d'une infiltration, les rôles et les responsabilités de chacun doivent être sans équivoque et défini afin d'apporter un maximum d'efficacité. Sachez développer des processus rigoureux de réaction afin de minimiser les effets négatifs d'une infiltration sur votre organisation.

- Comment développer un protocole de gestion des incidents de sécurité ?
- Comment gérer le risque que représente une attaque cybernétique sur le plan de la réputation de l'organisation ?
- Comment minimiser l'accumulation de données personnelles afin de réduire le risque d'une cyberattaque ?
- Aussi, découvrez les erreurs les plus fréquentes en gestion de crise et les actions à éviter.

16 h 45 MOT DE CLÔTURE

« *Dans le monde, les incidents qui fragilisent la sécurité informatique et les cyberattaques ont augmenté de 48 % en 2014, et sont au nombre de 42,8 millions.* »

Source : Étude Price Waterhouse Cooper, 2014

« *En 2014, le coût global estimé de la cybercriminalité dépasse 23 G $ US, et ce, pour les incidents détectés seulement.* »

Source : Global State on Information Security Survey, 2014

À PROPOS DE BFL CANADA
Cabinet de services financiers

BFL CANADA est la plus importante société de gestion de risques, de courtage d'assurance commerciale et de services conseils au Canada qui soit détenue et gérée par ses propres employés. Notre société est présente dans neuf villes à travers le pays, et nos spécialistes œuvrent dans tous les grands secteurs d'activité.

Ateliers pratiques

jeudi 26 mars 2015

8 h 30 ACCUEIL DES PARTICIPANTS

9 h 00 ATELIER B

Développez des outils efficaces de gestion du risque de cybercriminalité qui seront compris à l'échelle de l'entreprise

Nicolas-Loïc Fortin
Architecte sécurité
INTRASECURE

Patrick Mathieu
Analyste de sécurité, cofondateur, Hackfest Communication
SECURITYCOMPASS.COM

Développer une politique de sécurité efficace dans votre entreprise ne peut se faire sans une gestion du risque rigoureuse et adaptée à vos activités. De même, sans la capacité d'évaluer les risques encourus, vous ne pourrez pas déterminer les points sensibles à protéger. La question reste toujours : quelle est la formule qui vous permettra de mettre en œuvre une gestion du risque qui optimisera votre budget sécurité ?

Pourquoi participer :
- Pour réaliser une analyse critique et constructive de votre gestion du risque liée à la cybercriminalité ;
- Pour découvrir les nouvelles pratiques de gestion du risque et les adapter à vos processus internes ;
- Pour développer des formations adaptées pour les employés de votre organisation.

Objectifs de l'atelier :
- Comment développer un registre de sécurité efficace et sur mesure pour vos activités ?
- Comment faire une gestion judicieuse des actions correctrices en intégrant des dispositifs de mémoire du risque et des contrôles intégrés ?
- Comment remettre en question les hypothèses utilisées dans vos analyses du risque afin d'améliorer vos décisions opérationnelles ?

12 h 00 DÎNER RÉSEAUTAGE POUR LES PARTICIPANTS INSCRITS À LA JOURNÉE COMPLÈTE

13 h 00 ATELIER C

Équilibrez vos contrôles de sécurité afin de protéger adéquatement vos données

Pascal Fortin
Président-directeur général
GOSECURE

La sécurité des données personnelles est un enjeu de gouvernance qui exige une maîtrise absolue de vos contrôles. Savez-vous intégrer efficacement des mesures de contrôle en fonction de la gravité du risque que représentent vos données ? Cet atelier pratique de trois heures vous aidera à atteindre l'équilibre entre les risques encourus, les coûts et la sensibilisation au risque dans votre organisation.

Pourquoi participer :
- Pour améliorer significativement la surveillance de vos activités afin de contrôler les risques à la base ;
- Pour développer des outils et des incitatifs afin que vos équipes TI effectuent les mises à niveaux de vos mesures de protection efficacement et dans des délais plus rapprochés ;
- Pour faire le point sur la manière dont vous gérez les contrôles de sécurité et pour déterminer les faiblesses de l'organisation en matière de cybersécurité.

Aussi, sachez :
- Comment développer des tests techniques basés sur des hypothèses crédibles et pertinentes à vos activités ?
- Comment développer des tests de robustesse sur vos applications maison et autres ?

Objectifs de l'atelier :
- Cernez avec précision les menaces extérieures et celles que représentent vos informations les plus sensibles et les plus critiques dans votre environnement.
- Évaluez avec plus de précision l'utilité de préserver ou d'éliminer des contrôles de sécurité informatique.

16 h 00 FIN DE LA JOURNÉE DES ATELIERS

Atelier préconférence

mardi 24 mars 2015

12 h 30 ACCUEIL DES PARTICIPANTS

13 h 00 ATELIER A

Mieux comprendre pour mieux protéger : apprenez les différentes facettes de la cybersécurité et évaluez adéquatement les impacts légaux de la protection des données

Éloïse Gratton
Associée
BORDEN LADNER GERVAIS LLP

Benoît Dupont
Professeur titulaire,
ÉCOLE DE CRIMINOLOGIE DE L'UNIVERSITÉ DE MONTRÉAL,
titulaire de la Chaire du recherche du Canada en sécurité, identité et technologie et directeur du Centre international de criminologie comparée

La plupart des organisations, quels que soient leur taille, leur réputation ou les efforts qu'elles déploient, seront à un moment ou à un autre confrontées à un bris de sécurité qui compromettra les renseignements personnels dont ils ont la garde. Ainsi, la capacité des organisations de réagir efficacement et de prendre les mesures qui s'imposent dans un tel contexte est primordiale.

Participez, afin de :

- Connaître le profil des cybercriminels ;
- Découvrir les stratégies généralement utilisées par les cybercriminels pour pénétrer dans les systèmes de votre organisation, et déterminer les ports d'entrée les plus vulnérables et les plus souvent ciblés par les hameçonneurs ;
- Comprendre l'impact juridique d'une cyberattaque.

La première partie de l'atelier vous permettra d'approfondir vos connaissances sur les différents types de cyberattaques et de vous sensibiliser au mode d'exécution des cybercriminels. **La deuxième partie** de l'atelier traitera plus précisément :

- De la marche à suivre à la suite d'un bris de sécurité informatique, notamment l'évaluation des dommages, les mesures d'urgence à imposer, les répercussions de l'incident et les risques de préjudice pour les individus, l'organisation et le public.
- De la politique de communication en cas de cyberattaque, c'est à dire qui informer, comment le faire et dans quel contexte, ainsi que l'information à inclure dans une notification.
- Du type d'assistance qui peut être offert aux individus touchés par la cyberattaque, ainsi que des meilleures pratiques dans l'élaboration d'un plan de communication.
- Des aspects de prévention et des différentes stratégies d'atténuation de dommages qui peuvent être mis en œuvre à l'échelle de l'organisation victime d'un bris de sécurité informatique.

Les objectifs de l'atelier :

- Comprendre le but des divers types de cyberattaques ainsi que les motivations des cybercriminels ;
- Acquérir une compréhension globale des solutions de protection contre les cyberattaques ;
- Connaître les différentes stratégies à adopter dans le cas d'un bris où plusieurs juridictions ou plusieurs parties sont visées.

Nous vous présenterons des cas concrets, et nous discuterons de la mise en place des outils proposés.

16 h 30 FIN DE L'ATELIER PRÉCONFÉRENCE

Cybersécurité

Jusqu'à 600 $* de rabais avant le 29 janv.
CODE PROMO requis

MARCHÉ CIBLE[1]

Je souhaite m'inscrire à :		Prix promotionnels - CODE PROMO requis		Prix réguliers
		Jusqu'au 29 janv.	Jusqu'au 26 fév.	
25 MARS	Conférence	● **495 $**	● **645 $**	● 795 $
24-26 MARS	Atelier (ch.)	● **+295 $**	● **+345 $**	● +395 $

FOURNISSEURS[1]

Je souhaite m'inscrire à :		Prix promotionnels - CODE PROMO requis		Prix réguliers
		Jusqu'au 29 janv.	Jusqu'au 26 fév.	
25 MARS	Conférence	● **595 $**	● **745 $**	● 895 $
24-26 MARS	Atelier (ch.)	● **+345 $**	● **+395 $**	● +445 $

[1] Cette conférence s'adresse principalement aux vice-présidents, vice-présidents adjoint, directeurs, chefs, responsables, conseillers, coordonnateurs et gestionnaires de projet TI, vérification interne qui constituent le **marché cible**. Tandis que les assureurs, les fournisseurs de solution de sécurité informatique, les avocats et les conseillers en gestion de système correspondent aux **fournisseurs**.

Veuillez prendre note que les ateliers ne peuvent pas être vendus individuellement. Ces activités sont offertes uniquement à l'achat de la conférence

*** Pour bénéficier des prix promotionnels vous devez mentionner le CODE PROMO WEB.**

Invitez vos collègues et profitez de rabais avantageux !

3 à 5 personnes → 20 %
6 personnes et + → 30 %

Rabais applicable sur les prix réguliers, non-cumulables aux prix promotionnels.

Cet événement s'adresse aux :

Vice-présidents, directeurs, chefs, responsables, gestionnaires, conseillers technologies de l'information, audit, vérification interne, base de données, gestion du risque, conformité et architecte de système. Vice-présidents marketing, finances, ressources humaines et membres de CA.

Inscrivez-vous en ligne :

lesaffaires.com/evenements/cybersecurite

Prochainement

18 FÉV. — **E-commerce**
Du clic à la livraison : offrez une expérience client optimale grâce à votre stratégie logistique

24 FÉV. — **Marque employeur**
De l'attraction jusqu'à l'engagement : faites vivre votre promesse employeur dans tous les cycles de vie de l'employé

24 MARS — **Transfert d'entreprise**
Le rendez-vous des entrepreneurs et de la relève du Québec inc.

8 AVRIL — **Adjointes administratives – 5e édition**
Positionnez-vous à titre de partenaire stratégique, crédible et en contrôle

OPPORTUNITÉS DE COMMANDITES

Cette conférence peut vous fournir une occasion unique de visibilité auprès de décideurs dans ce domaine et d'exposer vos produits et services.

Plusieurs forfaits de commandites sont disponibles : cocktail, exposant, petit-déjeuner...

Pour plus d'information, communiquez avec Patrick Savoy à patrick.savoy@tc.tc ou 514 290-0159.

CONTACTEZ-NOUS :

T 514 392-4298 ou 1 855 392-4298 evenements@tc.tc

ÉCHANGEZ SUR NOS COMMUNAUTÉS EN LIGNE :

Suivez-nous sur Twitter : **@la_evenements**
Tweetez avec le **#LesAffaires**

Joignez-vous à notre groupe LinkedIn :
Groupe Événements Les Affaires

MODALITÉS D'INSCRIPTION

Les prix promotionnels sont valides jusqu'au 29 janvier et 26 février 2015 inclusivement en mentionnant votre CODE PROMO. Les rabais de groupe s'appliquent sur les prix réguliers et ne sont pas cumulables aux prix promotionnels. Les frais de participation comprennent la documentation de la conférence rendue disponible par les conférenciers, le repas du midi et des collations et boissons aux pauses-café selon votre inscription. Notez que vous ne pouvez participer à cette conférence que si vous effectuez votre paiement au plus tard le jour même de la conférence. Vous pouvez vous inscrire par téléphone ou en ligne, par chèque ou par carte de crédit Visa, American Express ou Master Card. Veuillez faire parvenir votre chèque à l'ordre de MÉDIAS TRANSCONTINENTAL SENC, en indiquant votre numéro de facture débutant par les lettres «CF», à l'adresse suivante : 400, avenue Ste-Croix, Suite 300, Montréal (Québec) H4N 3L4.

UNE POLITIQUE D'ANNULATION FLEXIBLE

Toute demande d'annulation doit obligatoirement être envoyée par courriel à evenements@tc.tc au plus tard dix jours ouvrables avant l'événement pour remboursement. Le fait de ne pas participer à la conférence ne vous libère en aucune façon de l'obligation d'acquitter les frais exigibles. Cependant, vous pouvez en tout temps vous faire remplacer par une personne de votre choix en nous en avisant par écrit. Les organisateurs se réservent le droit de modifier en tout ou en partie la programmation, et ce, sans préavis.

LIEU DE LA CONFÉRENCE

Centre-ville Montréal.

PARTICIPANTS DU QUÉBEC

Le coût de la formation peut constituer une dépense de formation admissible en vertu de la Loi favorisant le développement et la reconnaissance des compétences de la main-d'œuvre.