Deloitte.

L'impératif de la cybersécurité

Protégez votre entreprise contre les cybermenaces

Table des matières

Les cybermenaces sont bien réelles et ne cessent d'augmenter

L'espionnage d'entreprises. L'activisme politique. La perturbation des marchés. Les gains financiers. Quelles que soient les motivations, la cybercriminalité est devenue monnaie courante et continue de gagner du terrain. De mai 2012 à mai 2013, les entreprises canadiennes ont subi des pertes de plus de 5,3 millions de dollars attribuables à des cyberattaques[1], que ce soit par le sabotage de données, la propagation de virus et de logiciels malveillants, le vol d'appareils, les fraudes financières et d'autres formes d'exploitation des vulnérabilités.

En plus d'infliger de lourdes pertes financières, les cyberattaques peuvent entraîner des sanctions réglementaires, l'interruption des activités, des poursuites en justice et une grave atteinte à la réputation.

Aucune entreprise ni aucun organisme du secteur public ne sont à l'abri. Tandis que les cybercriminels sont de plus en plus futés, les entreprises sont complètement dépassées lorsque les données confidentielles de leurs employés, de leurs clients ou de leurs parties prenantes – qu'il s'agisse de dossiers financiers et de mots de passe sécurisés ou de renseignements en matière de santé et même de leur identité – deviennent la cible de ces attaques concertées.

À mesure que les secteurs deviennent de plus en plus interdépendants, que le rythme du changement s'accélère et que la dépendance à l'égard du cyberespace s'accentue, le risque de dommages catastrophiques sur le plan physique et économique s'accroît. Pour se prémunir contre ces cybermenaces, les entreprises doivent mettre en place des solutions de cybersécurité plus puissantes, qui permettent de repérer les menaces en temps réel, de limiter les risques, de réduire les délais de reprise et de prévenir de futures attaques. Deloitte peut les aider.

Une gamme complète de solutions de cybersécurité

La plupart des entreprises reconnaissent l'importance de protéger leurs systèmes, leurs réseaux et leurs données contre les cybermenaces et les atteintes à la sécurité. Cependant, elles ont de plus en plus de difficulté à déjouer ces menaces si elles n'obtiennent pas l'aide qu'il faut. Kennedy Consulting Research & Advisory, un éminent cabinet d'analystes, a récemment publié un rapport portant sur la question. Le rapport fournit une évaluation des cabinets de consultation en cybersécurité en ce qui a trait à l'étendue relative de leurs services-conseils en cybersécurité. En particulier, Deloitte a été reconnu comme chef de file dans le palmarès Vanguard de Kennedy et désigné comme le fournisseur offrant l'éventail de compétences le plus complet en matière de cybersécurité[2].

Deloitte a perfectionné ces compétences en offrant des services de sécurité à certaines des plus importantes entreprises au monde. À l'échelle mondiale, nous comptons plus de 900 professionnels possédant la certification CISSP *(Certified Information Systems Security Professionals)*, 1 500 auditeurs possédant la certification CISA *(Certified Information Systems Auditors)*, 150 gestionnaires possédant la certification CISM *(Certified Information Security Managers)* et 65 professionnels possédant la certification CIPP *(Certified International Privacy Professionals)*. Nous avons également établi des centres de technologies en matière de sécurité dans des endroits stratégiques au Canada.

Afin d'aider les entreprises à profiter des avantages de l'environnement d'affaires numérique tout en atténuant les risques qui en découlent, nos services de cybersécurité englobent quatre éléments essentiels :

Sensibilisation

Pour repousser les menaces à la sécurité, vous devez savoir quelles menaces sont pertinentes à votre entreprise et quelle est leur provenance. La capacité de cybersensibilisation de Deloitte peut vous aider à cerner les cybermenaces actuelles et nouvelles et à prendre les mesures qui s'imposent pour corriger les failles dans votre cyberprofil.

Services connexes : renseignements sur les cybermenaces.

Préparation

À mesure que les cybermenaces s'intensifient, votre architecture technologique, vos processus de sécurité et votre stratégie culturelle doivent évoluer au même rythme. Les solutions de cyberpréparation de Deloitte peuvent vous aider à adopter les bons mécanismes de protection, à mettre vos plans à l'épreuve au moyen de cybersimulations et à apporter les modifications comportementales nécessaires pour consolider votre posture de cybersécurité.

Services connexes : sensibilisation aux cybermenaces, cybergouvernance et politiques sur la cybersécurité.

Détection

La prolifération des données massives continue de donner du fil à retordre aux équipes de sécurité, ce qui diminue leur capacité de déceler les violations potentielles, de les identifier et de réagir en temps opportun. Les solutions de détection offertes par Deloitte viennent soutenir vos ressources internes en leur donnant accès à des solutions analytiques qui facilitent la découverte de cyberfailles avant que des dommages ne soient causés.

Services connexes : services de sécurité gérés, gestion des informations et des événements de sécurité.

Réaction

Lorsqu'un cyberincident survient, la réaction doit être immédiate, exhaustive et décisive. Les services de cyberréaction de Deloitte vous donneront accès aux compétences, à l'expérience et aux connaissances qu'il vous faut en temps de crise. En plus de déterminer la nature de l'incident, nous collaborons avec vous pour calculer les dommages et les réduire au minimum, cerner les causes fondamentales de l'incident et apporter les correctifs nécessaires pour prévenir les pertes futures.

Services connexes : services de sécurité gérés, centre d'opérations et de renseignements de sécurité (CORS).

Services de sécurité gérés

Libérez vos ressources internes grâce à l'impartition

À mesure que les cybermenaces évoluent, les équipes de sécurité internes ont de plus en plus de difficulté à détecter et à contrer les menaces évoluées à toute heure du jour et de la nuit. La quantité de ressources nécessaires pour assurer efficacement la surveillance de l'ensemble des applications et des appareils, la mise en œuvre des nouveaux contrôles de sécurité ou même l'analyse des journaux de sécurité peut être ahurissante.

Les services de sécurité gérés allègent le fardeau en offrant des capacités évoluées de surveillance des incidents de sécurité, d'analytique, de gestion des cybermenaces et de réaction aux incidents.

Les avantages

- **Prévision et prévention des incidents de sécurité en fonction des événements passés et en cours**
- **Amélioration de l'efficacité de vos contrôles de sécurité**
- **Réduction des risques liés à la conformité et à la réglementation**
- **Prise de conscience dynamique des cybermenaces actuelles qui mettent vos actifs, vos réseaux et vos données en péril**
- **Amélioration de la détection des menaces et des moyens d'intervention**

Ces services comprennent ce qui suit :

- **Gestion et orientation du portefeuille de services :** un programme de cybersécurité efficace passe inévitablement par une planification stratégique. Les professionnels de Deloitte possèdent l'expérience requise pour vous aider à effectuer une analyse de rentabilité du CORS, évaluer votre état de préparation en cybersécurité et discuter des répercussions éventuelles des cybermenaces avec votre conseil d'administration;
- **Veille stratégique, observation et cybersurveillance :** afin de vous aider à demeurer à l'affût des cybermenaces, Deloitte effectue une surveillance approfondie des menaces ainsi qu'une analyse des indicateurs de menace et du cyberbavardage; il produit aussi des rapports de façon continue afin de vous tenir informés;
- **Surveillance de la sécurité et analytique avancée :** le centre de cyberrenseignements de Deloitte assure la surveillance de vos systèmes 24 heures sur 24, en tirant parti de techniques avancées telles que l'analyse prévisionnelle et la modélisation adaptative des risques pour détecter les menaces évoluées;
- **Analyse, enquêtes, intervention en cas d'urgence informatique et maîtrise :** afin de vous aider à vous préparer à une situation d'attaque, Deloitte collaborera avec vous pour exécuter des cybersimulations et élaborer un solide plan d'intervention. Si une attaque franchit vos défenses, nous pouvons également vous aider à réaliser la coordination de l'intervention, l'enquête juricomptable et l'analyse de la cause fondamentale;
- **Élaboration de contenu :** en surveillant des centaines de sources de renseignements, Deloitte dispose du plus récent contenu au sujet des menaces, et formulera des recommandations sur les nouvelles signatures et élaborera de nouveaux scénarios de détection;
- **Rapports opérationnels et à la haute direction :** obtenez des rapports détaillés sur les cas de menace, les améliorations apportées aux processus du CORS et aux configurations et un éventail d'autres paramètres qui s'appliquent à votre entreprise.

Renseignements sur les cybermenaces

Découvrez et corrigez les failles dans votre cyberprofil

Dans le contexte numérique d'aujourd'hui, l'approche traditionnelle en matière de sécurité ne fonctionne plus. Les pare feu ne tiennent pas compte des vecteurs d'infection tels que les attaques par hameçonnage et l'ingénierie sociale. Les logiciels malveillants et les techniques d'anonymisation peuvent contourner les contrôles de sécurité en place. Même les systèmes de détection des intrusions et les solutions antivirus tombent en désuétude.

Pour gérer les cyberrisques, vous avez besoin d'une approche axée sur les renseignements qui fait appel à la connaissance des cyberadversaires et des méthodes qu'ils utilisent, jumelée à la connaissance de votre propre posture de sécurité par rapport à ces adversaires et méthodes. Les renseignements sur les cybermenaces procurent des résultats en produisant des renseignements concrets que les entreprises peuvent utiliser pour prendre des décisions éclairées à l'égard des risques. Ce service comporte les éléments suivants :

- **Collecte de renseignements internes et externes :** Deloitte regroupe, tient à jour et gère un répertoire de plus de 300 sources de renseignements, y compris des renseignements issus de la surveillance des cybercriminels;
- **Normalisation** : consiste à analyser les renseignements recueillis afin d'identifier les menaces nouvelles et actuelles à la sécurité;
- **Enrichissement :** assure une compréhension globale de la capacité de l'entreprise à déjouer les cybermenaces;
- **Fusion :** permet de renforcer votre posture de sécurité globale au moyen de mises à jour des contrôles de sécurité, de décisions relatives à l'authentification, de renseignements sur l'évaluation des risques, de renseignements sur les investissements technologiques, et d'une aide pour la sélection des fournisseurs et les décisions relatives aux RH.

Les avantages

- **Accès à des renseignements utilisables en temps opportun pour assurer une protection contre des cyberattaques complexes**
- **Capacité de mettre ces renseignements en pratique dans votre environnement**
- **Identification et gestion des menaces internes avec possibilités de corrélation ciblée sur des cas d'utilisation**
- **Vue d'ensemble du profil de menaces internes et externes de votre entreprise**
- **Sensibilisation situationnelle aux menaces pour l'ensemble des secteurs, des techniques criminelles, des exploits et des vulnérabilités**

Centre d'opérations et de renseignements de sécurité (CORS)

Mettez en place et exploitez un CORS de calibre mondial

Le centre d'opérations et de renseignements de sécurité (CORS), une version évoluée du centre des opérations de sécurité (COS) traditionnel, recueille et fusionne les renseignements sur lesquels reposent les capacités de surveillance et de réaction aux menaces.

Fort de décennies d'expérience en mise en œuvre de CORS, Deloitte peut vous aider à relever ces défis. Notre méthodologie de cybersurveillance adaptative met à votre disposition les outils et accélérateurs qu'il vous faut pour évaluer, planifier et mettre en place un CORS hautement performant, axé sur l'entreprise.

Les services comprennent ce qui suit :

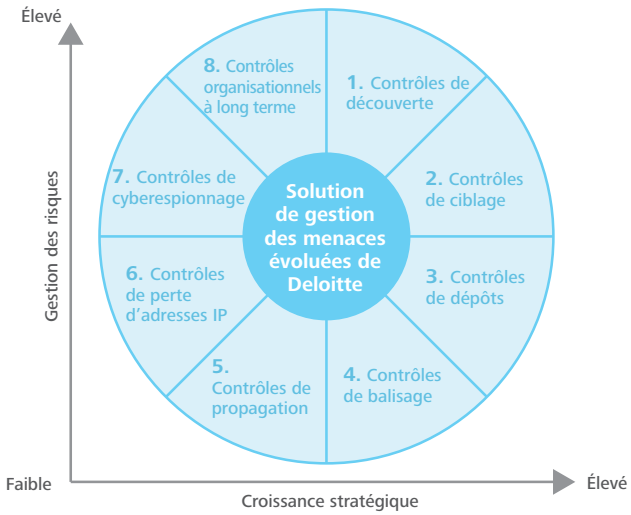
- **Élaboration de la stratégie du CORS :** à la suite d'une évaluation de l'état de préparation et d'une analyse de faisabilité, nous vous aidons à créer une feuille de route pour le CORS visant à assurer le rendement de votre investissement;
- **Préparation du CORS :** évaluez les solutions des fournisseurs, élaborez une charte de projet et un plan de gestion des risques, créez une structure de gouvernance et adoptez des contrôles appropriés;
- **Mise en œuvre du CORS :** définissez et mettez à l'essai l'architecture du CORS, établissez les protocoles de gestion de la sécurité et déterminez les gens, les processus et les technologies qui pourront vous aider à réussir;
- **Optimisation du CORS :** améliorez les processus de votre CORS à l'aide de cyberaccélérateurs, d'un programme de paramètres, de procédures de transmission aux échelons supérieurs et de l'intégration aux processus de l'entreprise.

Les avantages

- **Accès à des renseignements utilisables en temps opportun pour assurer une protection contre des cyberattaques complexes**
- **Capacité de mettre ces renseignements en pratique dans votre environnement**
- **Identification et gestion des menaces internes avec possibilités de corrélation ciblée sur des cas d'utilisation**
- **Vue d'ensemble du profil de menaces internes et externes de votre entreprise**
- **Sensibilisation situationnelle aux menaces pour l'ensemble des secteurs, des techniques criminelles, des exploits et des vulnérabilités**

Solution de gestion des menaces évoluées de Deloitte

Combattez les menaces évoluées, adaptatives et persistantes



Les entreprises sont de plus en plus exposées aux cybermenaces complexes et adaptatives – celles qui échappent aux contrôles de détection courants ou qui se cachent derrière un comportement apparemment normal. Malheureusement, la plupart des contrôles actuels visent des menaces que les cybercriminels ont abandonnées depuis longtemps. Plutôt que de s'adapter à un environnement polymorphe à évolution rapide, ces contrôles se concentrent sur les menaces ponctuelles et les cas d'utilisation connus.

La solution de gestion des menaces évoluées de Deloitte utilise un ensemble de contenus, de processus, d'accélérateurs, de renseignements, de flux de tâches et de catalyseurs pour vous aider à déjouer les menaces les plus évoluées. Fonctionnant à partir d'ArcSight, le moteur de cette solution est conçu pour éliminer les faiblesses des systèmes typiques de sécurité monolithiques.

Les avantages

- **Accès à des renseignements sur les cybermenaces auprès de 300 sources externes et internes**
- **Découverte et blocage automatiques des périphériques réseau malveillants**
- **Suivi de l'évolution des menaces grâce à un modèle de risques adaptatif**
- **Surveillance des menaces et des activités clandestines au moyen de l'analytique prévisionnelle**
- **Degré plus élevé de sensibilisation situationnelle**
- **Accélération des enquêtes grâce à des requêtes et au signalement des menaces**

Gestion des informations et des événements de sécurité

Accélérez la découverte des cybermenaces et la reprise

Même si la plupart des atteintes à la protection des données sont persistantes et soutenues, les entreprises ont souvent de la difficulté à les déceler. Les raisons sont variées : certaines entreprises n'ont pas de stratégie de gestion des journaux de sécurité, certains systèmes ne fonctionnent pas correctement et certains journaux ne sont tout simplement pas examinés. Par conséquent, les entreprises ne sont pas au courant des menaces externes et internes, du détournement ou de l'utilisation inappropriée des données, des éclosions de virus et d'autres incidents liés à la sécurité ayant un impact élevé.

Pour accélérer la découverte de cybermenaces et la reprise, les entreprises doivent renforcer leurs systèmes de gestion des informations et des événements de sécurité. Fort de son expérience en déploiement de tous les principaux outils de gestion des informations et des événements de sécurité et en intégration de ces outils aux processus de TI existants, Deloitte peut vous aider. Les étapes sont les suivantes :

- **Collecte des journaux :** recueillez des données à partir des dispositifs de sécurité à l'aide d'une variété de méthodes et de protocoles;
- **Normalisation et regroupement des données :** créez des formats de message standard et regroupez les données en fonction de divers critères;
- **Corrélation des données :** triez les données, établissez des liens entre les événements consignés dans les journaux et attribuez des valeurs pondérées à chaque événement constituant une menace;
- **Notification d'événements :** transmettez des avis par courriel à l'aide d'un bon de travail ou par d'autres moyens;
- **Production de rapports :** soumettez des requêtes portant sur les journaux enregistrés dans la base de données et visualisez les événements et les tendances.

Les avantages

- **Réduction de la gravité et du coût des atteintes à la sécurité en accélérant la réaction aux incidents et la reprise**
- **Suivi des menaces en temps réel grâce à la corrélation évoluée des métadonnées**
- **Amélioration de l'application de la politique sur la sécurité**
- **Capacité d'analyser les applications et de déceler les comportements anormaux**
- **Amélioration de la conformité de la sécurité**
- **Intégration de la gestion des informations et des événements de sécurité à votre architecture globale de gestion de la sécurité**
- **Réduction des risques de perturbation des systèmes attribuables aux cybermenaces**

Gestion du contenu et des appareils en fonction des menaces évoluées

Découvrez vos points faibles

Les cyberattaquants sont toujours à la recherche de vulnérabilités. Pour protéger vos actifs importants, vous devez évaluer et vérifier vos risques liés à vos vulnérabilités, déterminer les menaces qui sont pertinentes à votre entreprise et prendre des mesures pour améliorer la sécurité.

L'équipe de professionnels en gestion des vulnérabilités de Deloitte peut exécuter périodiquement des évaluations légères ou robustes des vulnérabilités, en parcourant les systèmes et processus de l'ensemble de votre entreprise afin de cerner les points faibles nouveaux et existants, puis en établissant la correspondance entre leur impact et vos activités. Les services comprennent ce qui suit :

- **Tests d'intrusion :** nos testeurs d'intrusion vous aideront à assurer la gestion de vos vulnérabilités au quotidien, en allant aussi loin que les pirates pour tenter d'infiltrer vos systèmes. En ayant une idée précise de vos vulnérabilités et de leur incidence potentielle, nous pouvons formuler des recommandations de mesures correctives afin de renforcer vos cyberdéfenses.
- **Prévention gérée des pertes de données :** afin d'augmenter l'efficacité de vos mesures de prévention des pertes de données, notre équipe peut prendre la relève de vos activités quotidiennes, ainsi qu'explorer tout incident repéré et y remédier.
- **Cybersimulations :** nos professionnels en simulation collaborent avec vous pour mettre à l'essai et peaufiner votre stratégie de gestion des cyberincidents en utilisant des scénarios réalistes afin de cerner les erreurs, les fausses hypothèses et les lacunes dans vos plans;
- **Solution de fusion de Deloitte :** le centre de fusion de la cybersécurité de Deloitte donne accès à des cyberrenseignements en temps quasi réel afin de vous tenir informés des nouvelles menaces qui touchent votre secteur, votre infrastructure ou la technologie déployée.

Les avantages

- **Amélioration des résultats de détection des menaces grâce aux tests manuels effectués dans votre environnement cible**
- **Compréhension de la façon de travailler des pirates et des dommages qu'ils pourraient occasionner à votre entreprise**
- **Protection des processus et systèmes essentiels à vos activités contre les vulnérabilités logicielles en constante évolution**
- **Amélioration de votre posture de sécurité globale ainsi que de vos capacités de détection des incidents menaces et des moyens d'intervention**
- **Identification et correction des points faibles exploitables**
- **Utilisation des meilleures pratiques internationales grâce à l'accès aux centres mondiaux des technologies en matière de sécurité de Deloitte**

Renforcez votre cybersécurité

À mesure que la dépendance à l'égard des technologies numériques s'accentue, les cyberadversaires rivalisent d'ingéniosité dans leurs façons d'attaquer. Les entreprises qui continuent de se fier à des mesures de sécurité dépassées deviennent de plus en plus vulnérables, s'exposant elles-mêmes, ainsi que leurs parties prenantes et toute l'économie, à un risque de dommages considérables.

Afin de déjouer ces menaces, les entreprises doivent maintenant perfectionner leur programme de cybersécurité. En plus de rehausser la conformité réglementaire, un programme de cybersécurité efficace peut aider les entreprises à faire face aux attaques dès qu'elles surviennent, à réduire le délai et le coût de reprise et à limiter les menaces à venir.

Peu importe où vous en êtes dans le cycle de vie de la cybersécurité, Deloitte peut vous aider à renforcer votre position en matière de sécurité. En recourant à une approche souple, pragmatique et indépendante à l'égard de la cybersécurité, nous pouvons collaborer avec vous – du réseau à la salle du conseil – pour relever les défis que présentent ces menaces en constante évolution.

Modèle de maturité pour la cybersécurité

Pour en apprendre davantage, communiquez avec un de nos leaders :

Personnes-ressources à l'échelle nationale :

Nick Galletto
Associé
Service des risques d'entreprise
416-601-6734
ngalletto@deloitte.ca

Mark Fernandes
Associé
Service des risques d'entreprise
416-601-6473
markfernandes@deloitte.ca

Personnes-ressources à l'échelle régionale :

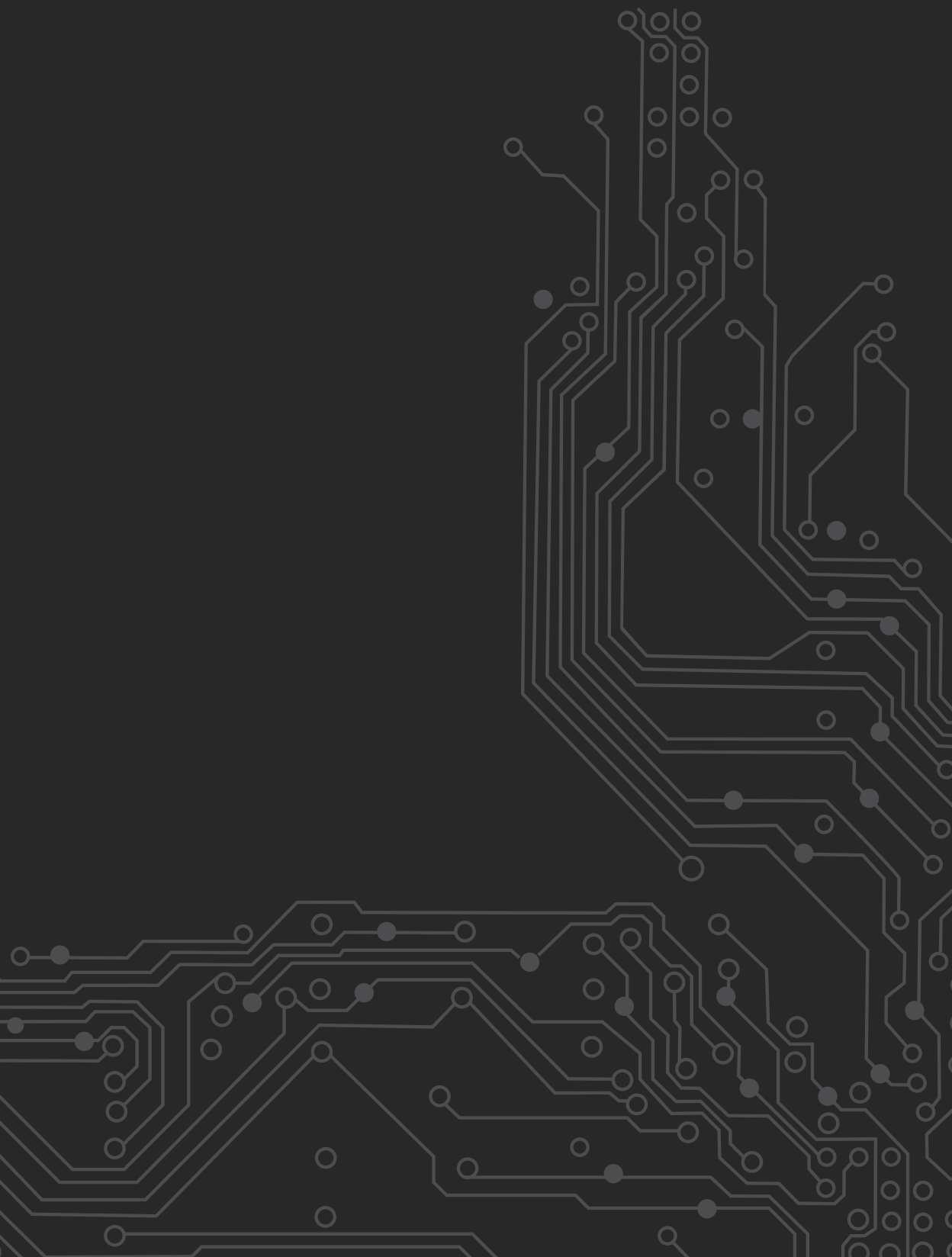
Amir Belkhelladi
Associé
Service des risques d'entreprise
514-393-7035
abelkhelladi@deloitte.ca

Alain Rocan
Associé
Service des risques d'entreprise
613-751-5386
arocan@deloitte.ca

Justin Fong
Associé
Service des risques d'entreprise
403-503-1464
jfong@deloitte.ca

Albert Yap
Associé
Service des risques d'entreprise
604-640-3279
ayap@deloitte.ca

Dina Kamal
Directrice principale
Service des risques d'entreprise
416-775-7414
dkamal@deloitte.ca



Notes de fin de document

1 International Cyber Security Protection Alliance, mai 2013.
Study of the Impact of Cyber Crime on Businesses in Canada (étude de l'incidence du cybercrime sur les entreprises du Canada).
Accessible à l'adresse https://www.icspa.org/fileadmin/user_upload/Downloads/ICSPA_Canada_Cyber_Crime_Study_May_2013.pdf

2 Source : Kennedy Consulting Research & Advisory; *Cyber Security Consulting 2013* (Services-conseils en cybersécurité, 2013); estimations de Kennedy Consulting Research & Advisory.

www.deloitte.ca

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 13-3694