Deloitte.

Réponse aux cyberincidents

Préparez-vous à l'inévitable.
Réagissez à l'évolution rapide des menaces.
Reprenez rapidement vos activités.

« Aujourd'hui, aucune entreprise canadienne n'est à l'abri d'une attaque potentielle. La question n'est plus de savoir *si* votre entreprise sera la cible d'une attaque, mais plutôt quand elle le sera. »

Conserver une longueur d'avance pour déjouer vos adversaires

Les nouvelles cybermenaces continuent de proliférer. Les rangs des cyberattaquants augmentent de jour en jour, tout comme leur niveau de sophistication et le nombre de leurs cibles.

Pour être prêt à faire face aux cyberincidents inévitables, il ne suffit pas de se préparer à réagir simplement pour neutraliser une attaque isolée. Cela nécessite la capacité d'intervenir efficacement et de manière répétitive pour planifier proactivement, défendre énergiquement vos systèmes et vos actifs informationnels vitaux, devancer l'évolution des menaces, et assurer une reprise complète des activités après les attaques.

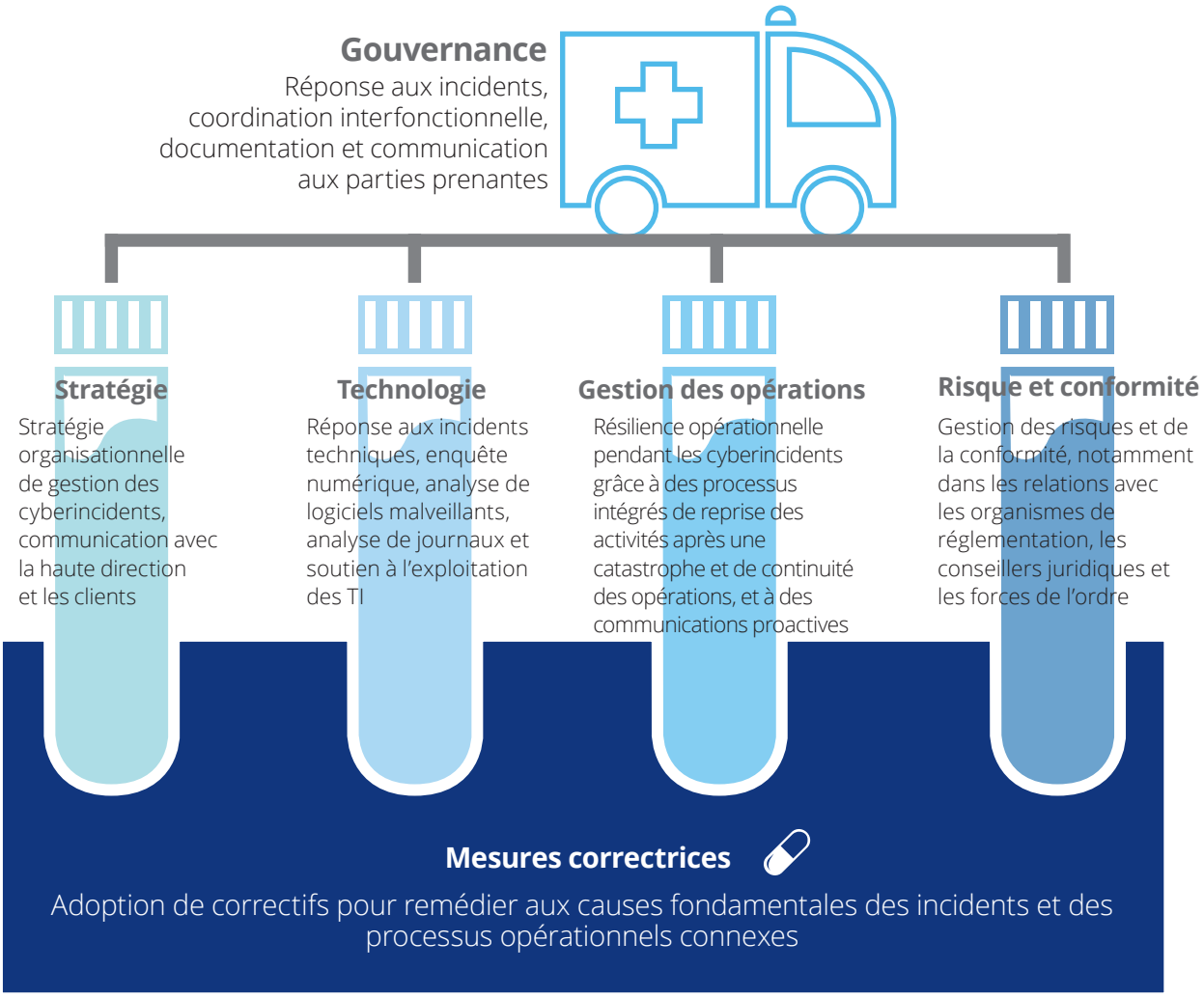
Dans un contexte où, de plus en plus, les cyberattaques grèvent les résultats financiers et ternissent la réputation des grandes sociétés, la mise sur pied d'une solide capacité d'intervention en cas de cyberincident (ICC) devient impérieuse pour les entreprises qui tiennent à sauvegarder leur sécurité, leur vigilance et leur résilience. Une solide capacité d'intervention en cas de cyberincident peut aider votre entreprise à faire ce qui suit :

- Comprendre rapidement la nature d'une attaque pour mieux faire face aux questions quoi, où, comment et combien, et y répondre
- Réduire le plus possible les coûts – en temps, en ressources et en perte de confiance des clients – associés à la perte de données
- Instaurer un niveau accru de gestion et de contrôle pour renforcer les TI et les processus opérationnels et, ainsi, pouvoir vous concentrer sur vos activités de base génératrices de valeur

« Deloitte est la seule organisation au Canada qui offre des services complets de réponse en cas d'incident (y compris la gestion de crise, les services-conseils en matière de protection de la vie privée, des enquêtes et des analyses numériques) et travaille en étroite collaboration avec les clients, les cabinets d'avocats et les compagnies d'assurance tout au long de l'incident. L'expérience que nous avons acquise dans le traitement de certaines des plus importantes brèches de sécurité au monde a permis à nos clients de reprendre leurs activités de manière efficiente et efficace à la suite de cyberincidents. »

Faire le nécessaire

La constitution d'une capacité d'ICC qui peut outiller votre entreprise pour faire face aux menaces changeantes nécessite un cadre opérationnel et la compréhension du cycle de vie des cyberincidents. L'établissement de ce cadre – le « centre » de vos ICC – et l'acquisition de connaissances sur les phases de la gestion des menaces procurent à votre entreprise les outils essentiels pour réagir proactivement aux cyberincidents.



Cycle de vie de réponse aux incidents

Le cycle de vie de réponse aux incidents commence avant même qu'un incident survienne. Les entreprises vigilantes peuvent se doter d'un ensemble de capacités proactives et réactives qui leur permettent de s'adapter aux cyberincidents, d'y réagir rapidement et de poursuivre leurs activités avec des répercussions limitées sur leurs opérations.

Proactivité	**Préparation**	• Englobe la conception et l'établissement d'un programme de réponse aux incidents couvrant l'organisation, les processus et les procédures • Implique la conception et la mise en œuvre d'une infrastructure des TI résiliente pour soutenir la gestion des opérations • Inclut des exercices proactifs de piratage électronique pour tester les processus et procédures de réponse aux incidents
	Détection	• Met à profit les capacités des renseignements sur les cybermenaces et d'autres méthodes d'ICC pour établir un programme complet de cybersurveillance et soutenir en permanence les activités de surveillance et de détection • Inclut l'évaluation des cybercompromissions afin de détecter les compromissions inconnues ou de valider la santé de l'environnement du réseau
	Analyse	• Consiste à recueillir de l'information, puis à établir l'ordre de priorité de chacun des incidents et les mesures d'intervention à prendre • Comprend l'analyse et la préservation judiciaires des données des clients pour déterminer l'étendue et les répercussions de l'incident
	Contrôle	• Consiste pour l'essentiel à prendre des mesures d'atténuation des risques afin d'empêcher d'autres répercussions ou dommages sur l'entreprise
Réactivité	**Élimination**	• Consiste essentiellement à prendre des mesures visant à éliminer les menaces existantes connues sur le réseau
	Reprise	• Met l'accent sur les mesures correctrices à court terme, la stratégie de correction et l'établissement d'une feuille de route • Consiste essentiellement à assurer la reprise du cours normal des activités ainsi qu'à établir des mesures d'atténuation des risques à long terme et à documenter les leçons retenues • Inclut la gestion des réclamations, les services-conseils juridiques protégés par le secret professionnel et les consultations en matière de confidentialité

Un large éventail de capacités

Dans le domaine des services de réponse aux cyberincidents, Deloitte connaît l'éventail des capacités dont les entreprises ont besoin pour se doter d'une protection de bout en bout, de l'étape de la préparation à celle de la reprise des activités. L'adoption d'une attitude proactive, une intervention stratégique en cas d'incident et une reprise systématique des activités peuvent aider les entreprises à acquérir les qualités de *sécurité*, de *vigilance* et de *résilience* dont elles ont besoin pour combattre les cybermenaces en constante évolution.

	Capacité	Description
Proactivité	 • Gouvernance et stratégie • Architecture et exploitation • Détection des incidents	• Évaluation, conception et élaboration d'un plan de réponse aux incidents à l'échelle de l'entreprise, formation et mise en œuvre • Orientation de la direction de l'entreprise pour qu'elle comprenne l'incidence et la gestion des interventions • Prestation de services assujettis à une provision d'honoraires pour aider les clients à intervenir en cas d'incident • Simulations de cyberattaques • Renseignements sur les cybermenaces et échange de renseignements avec les pairs • Piratage électronique et évaluations des compromissions • Services-conseils en matière de protection de la vie privée
Réactivité	 • Triage • Intervention	• La direction de l'entreprise dirigera l'intervention en cas d'incident selon ses impératifs stratégiques, opérationnels et techniques • Analyse technique pour trier les incidents, déterminer leur incidence et faire enquête sur leurs causes fondamentales • Soutien pour circonscrire l'incident • Soutien aux relations publiques après l'incident • Soutien en matière de gestion des risques et de conformité pour gérer les incidences de droit, de réglementation et de répercussions sur les clients • Assistance pour gérer l'interruption des activités
	 • Reprise • Maintien	• La direction de l'entreprise met sur pied et gère les activités de reprise en fonction des impératifs stratégiques, opérationnels et techniques • Correctifs, gestion postérieure aux événements et soutien à la reprise des activités après une attaque, quelle que soit son ampleur • Capacités techniques et opérationnelles intégrées pour assurer à la direction un soutien postérieur aux incidents

Avantages concrets

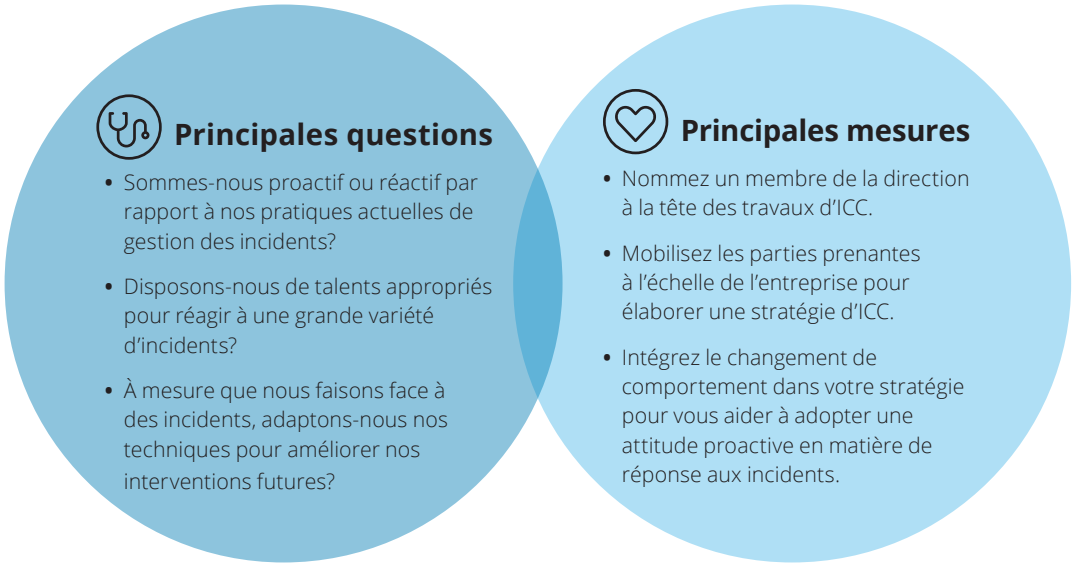
L'amélioration des capacités d'ICC de votre entreprise peut faciliter une détection et une gestion précoces des menaces et, par conséquent, la mise en place rapide de correctifs.

L'adoption d'une orientation claire en matière d'ICC peut aider votre entreprise à :

- Assurer la continuité des activités
- Empêcher la perte des actifs informationnels qui sont essentiels à la conduite de vos affaires
- Améliorer la sécurité globale de votre entreprise en renforçant la confiance de vos partenaires et de vos clients et en consolidant votre réputation
- Consacrer davantage de temps et de ressources aux améliorations fondamentales, à l'innovation et à la croissance

Questions et mesures

Le renforcement de votre position en matière d'ICC exige une stratégie complète qui s'appuie sur l'expérience. Cela exige également de savoir poser les bonnes questions et de prendre les mesures appropriées.



Communiquez avec nous

Pour amorcer le dialogue sur la manière dont votre entreprise peut commencer à se doter de capacités de réponse aux cyberincidents pouvant vous aider à déjouer les menaces, vous pouvez nous consulter en ligne ou nous joindre directement.

Toronto

Nathan Spitse
Associé
Services liés aux cyberrisques
nspitse@deloitte.ca
416-874-3338

Corey Fotheringham
Associé
Services liés aux cybercrimes et à l'administration de la preuve électronique
cfotheringham@deloitte.ca
416-618-4253

Ouest

Justin Fong
Associé
Services liés aux cyberrisques
jfong@deloitte.ca
403-503-1464

Est

Rob Masse
Associé
Services liés aux cyberrisques
rmasse@deloitte.ca
514-393-7003

Courriel de l'équipe de réponse aux cyberincidents :
increspons e@deloitte.ca

Si vous êtes actuellement victime d' un incident, veuillez composer le numéro :
1-800-CIC-HELP

www.deloitte.ca/cyber

Conçu et produit par le Service de conception graphique de Deloitte, Canada. 16-4161H