BOMA Canada

2021 Guide de Cybersécurité

Le rôle de la gestion des relations avec les fournisseurs en cybersécurité

Ce Guide est commandité par :

FIRST CAPITAL · Genetec · MNP LLP · QuadReal

Nous sommes fiers de présenter ce guide sur le rôle de la gestion des relations avec les fournisseurs (GRF) en cybersécurité, conçu pour aider les propriétaires et les gestionnaires d'immeubles dans leur cheminement de cybersécurité en ce qui concerne leurs fournisseurs.

Chers amis,

BOMA Canada cherche à offrir un enseignement et des outils précieux à ses membres par l'intermédiaire de sa série de connaissance. Au cours des dernières années, la cybersécurité a été un sujet de préoccupation grandissant dans les immeubles commerciaux et résidentiels, et notre série de guides sur la cybersécurité vise à mettre en lumière ce sujet critique.

Le Guide du bien-être cybernétique 2019 de BOMA Canada – le premier de la série – a présenté les menaces pour la cybersécurité et a fourni un point de départ au cheminement des immeubles vers la cybersécurité. L'année suivante, le Guide de cybersécurité – Approvisionnement de BOMA Canada approfondissait davantage les pratiques de cybersécurité relatives à l'approvisionnement. Puisque les fournisseurs tiers deviennent souvent le point d'entrée des auteurs d'incidents et d'infractions liés à la cybersécurité, il était nécessaire d'approfondir la cybersécurité relativement à la gestion des relations avec les fournisseurs (GRF), ce qui est le but de ce guide.

Cordialement,

Benjamin Shinewald
Président-directeur général
BOMA Canada

Comment ce guide doit-il être utilisé?

Ce guide a été conçu afin de présenter aux gestionnaires et aux propriétaires d'immeuble les programmes de GRF qui peuvent les aider à réduire les risques liés à la cybersécurité. Il est préférable de l'utiliser en combinaison avec le plan de cybersécurité général, et il suit nos guides précédents liés à la cybersécurité, afin que les lecteurs puissent lier les décisions associées quant à la manière dont ils gèrent leurs relations avec leurs fournisseurs du point de vue de la cybersécurité.

Bien que ce guide ait été conçu dans le but de vous aider avec votre cheminement, il ne représente pas en soi une stratégie ou une norme complète. Les renseignements qu'il contient doivent être complétés par d'autres lectures complémentaires, utilisés selon les normes précises ou bien à l'aide d'autres professionnels pour pouvoir créer des plans d'atténuation solides.

Nous espérons que ce guide vous soit utile dans votre cheminement de cybersécurité, et nous accueillerons vos suggestions avec plaisir pour de prochains guides.

Droit d'auteur

Exonération de toute responsabilité légale

En lisant le présent guide, vous acceptez de respecter, sans restriction ni limitation de quelque nature que ce soit, les modalités de cette clause de non-responsabilité.

Les membres de l'Association des propriétaires et des administrateurs d'immeubles du Canada, y compris tous ses dirigeants, ses directeurs, ses employés, ses conseillers, ses consultants, ses membres du comité, ses membres du groupe de travail, ses agents, ses bénévoles et ses membres, ci-après désignés collectivement « BOMA », ont rassemblé le matériel dans ce document à des fins d'exercices potentiels de démarrage pour traiter des incidents relatifs à la cybersécurité qui pourraient se produire. L'information présentée est unique et sans exception, expresse ou implicite, à cette fin. BOMA n'émet aucune déclaration ou garantie, expresse ou implicite, indiquant que les informations présentées sont actuelles ou exactes à tout moment, que ce soit présentement, précédemment ou à tout moment dans le futur.

Les renseignements compris dans ces documents ne sont pas fournis dans l'intention de préconiser, d'encourager ou de suggérer une

ou plusieurs méthodes particulières pour faire face à un incident cybernétique. Si l'utilisateur est confronté à un tel incident, il doit demander de l'aide à un professionnel. Tous les problèmes connexes au droit, aux finances, aux urgences, à la gestion, au développement, à la conception structurelle, à la sécurité ou bien au commerce doivent être signalés a un professionnel qui peut correctement évaluer les risques inhérents à ceux-ci et suivre tout plan pour résoudre un problème donné. Les renseignements ci-après ne remplacent pas la consultation d'un professionnel expérimenté.

BOMA, ses partenaires et sociétés affiliées ou organismes apparentés, ne déclarent ni ne garantissent, tant implicitement qu'explicitement, qu'aucun risque n'est associé à l'information contenue ci-après. Au demeurant, aucune de ces parties n'est responsable des actes ou omissions consécutifs à l'utilisation, dans son ensemble ou en partie, du présent document. Les mêmes parties ne peuvent être tenues pour responsables envers toute personne, que ce soit sur la base d'un contrat, de l'équité, de la responsabilité délictuelle, d'un règlement ou d'une loi quelconque, de toute perte directe ou indirecte, maladie ou blessure, ou de tout dommage spécial, accessoire, indirect, punitif ou autre, consécutif à l'utilisation de ce guide.

Les renseignements contenus dans ces présents documents ne prétendent pas couvrir toutes les situations. Des renseignements détaillés pouvant être pertinents pour le cas particulier d'un utilisateur ont pu être omis. Il est recommandé aux utilisateurs d'obtenir un avis professionnel avant d'appliquer tout renseignement contenu dans le présent document à leur propre situation. Les utilisateurs devraient toujours obtenir un avis professionnel approprié sur les questions relatives à la sécurité et à la santé publique, d'ordre juridique, structurel, organisationnel, personnel, exclusif, professionnel ou bien connexes à autre chose.

Les renseignements sont présentés « tels quels ». Ce guide, ou bien une partie de celui-ci, y compris, notamment, les appendices ou les trousses à outils et ses ressources connexes, n'a pas été conçu pour établir d'une quelconque manière des relations ou des obligations de diligence entre le personnel de BOMA (toutes les personnes ou les partis compris dans BOMA, comme définis) et toute autre personne ou entité, y compris, sans restreindre le caractère général de ce qui précède, toute personne ou entité qui aurait pu lire, réviser, utiliser

le présent guide ou en prendre connaissance ou bien toute partie de celui-ci, désignée collectivement comme « l'utilisateur » tout au long du présent avis de non-responsabilité. L'utilisateur reconnaît aussi qu'aucune relation de cette nature n'est établie entre lui et les partis ayant participé à la préparation, à la production ou à la diffusion du présent document. Il reconnaît en outre que, du fait du présent avis de non-responsabilité, BOMA n'aura jamais aucune obligation de diligence à son égard, sur la base d'une règle, d'une loi, de l'équité ou d'un règlement quelconque, y compris une obligation de tenir à jour et de valider l'information ci-après, et de vérifier son exactitude, et que l'utilisation de ce guide en tout ou en partie ne peut constituer de base pour aucune réclamation ou poursuite judiciaire intentée à l'encontre de BOMA.

Pourquoi les fournisseurs sont importants en cybersécurité

De nos jours, les menaces liées à la cybersécurité proviennent de sources inattendues, et les attaquants chercheront le maillon faible de votre chaîne d'approvisionnement. Leur point d'entrée est souvent à l'insu des fournisseurs, dont les systèmes ou les processus peuvent ne pas être aussi efficaces que les vôtres. Le risque peut aussi se situer au niveau de leur chaîne d'approvisionnement, où un pirate peut s'introduire par l'intermédiaire de leurs fournisseurs afin de trouver une entrée dans votre système.

Les fournisseurs dans les immeubles commerciaux sont souvent diversifiés et peuvent inclure, entre autres, des fournisseurs de services de technologie, des intégrateurs de système, des sous-traitants qui ont accès à votre immeuble ou à Internet, des techniciens invités et même du personnel d'entretien sous-traitant.

Généralement, les fournisseurs principaux, bien qu'ils soient essentiels à votre organisation, peuvent augmenter vos risques dans divers domaines :

- les finances;
- l'accès au site;
- la continuité des opérations;
- la capacité de récupération;
- les activités quotidiennes.

Plus récemment, les préoccupations liées à la cybersécurité ont étendu ces risques et donné lieu à plusieurs nouveaux risques associés aux fournisseurs. Les organisations doivent maintenant inclure certaines considérations supplémentaires dans leurs évaluations du risque, telles que :

- le processus que les fournisseurs suivent afin de vérifier leur propre personnel qui a accès à vos données, à vos systèmes ou à vos installations;
- la façon dont vos vendeurs vérifient les pratiques de sécurité de l'information de leurs fournisseurs de service et de produits afin de s'assurer que ce qu'ils font ne présente pas de risque potentiel;
- les sauvegardes de cybersécurité que les vendeurs incorporent dans les produits et les logiciels qui seront intégrés dans vos systèmes;
- les sauvegardes contre le matériel informatique de contrefaçon ou le matériel informatique comportant des programmes malveillants intégrés;
- l'entreposage de données ou les outils et pratiques d'agrégateur de données par une quatrième partie.

La gestion des relations avec vos fournisseurs est plus importante que jamais, avant même de chercher à réduire ces risques et à fournir les services que vos clients et vos locataires veulent dans un environnement sécuritaire.

L'importance et le choix du sujet

Dans notre premier guide, nous avons présenté un aperçu initial et une liste de vérification destinés aux propriétaires et les gestionnaires d'immeuble afin qu'ils puissent commencer leur cheminement de cybersécurité. Les trois phases principales de la planification en cybersécurité étaient exposées dans ce guide : la préparation, la résolution et le compte-rendu. Dans notre deuxième guide, nous avons approfondi les aspects de l'approvisionnement de la phase critique de « préparation », puisqu'un élément important de la cybersécurité consiste à réduire les points faibles dans votre chaîne d'approvisionnement. Ce guide mettait l'accent sur la cybersécurité dans le secteur de l'approvisionnement, y compris des aspects comme l'embauche et la création de meilleures demandes de propositions (DP). Au fur et à mesure que nous approfondissions notre conversation à propos de la cybersécurité pour les propriétaires et les gestionnaires d'immeubles, un sujet de préoccupation important a fait surface : gérer et bâtir les relations avec les fournisseurs tiers afin de permettre, de façon proactive, une meilleure collaboration en matière de cybersécurité. Le présent guide approfondit cet aspect essentiel de la cybersécurité.

Donner vie aux risques : une étude de cas

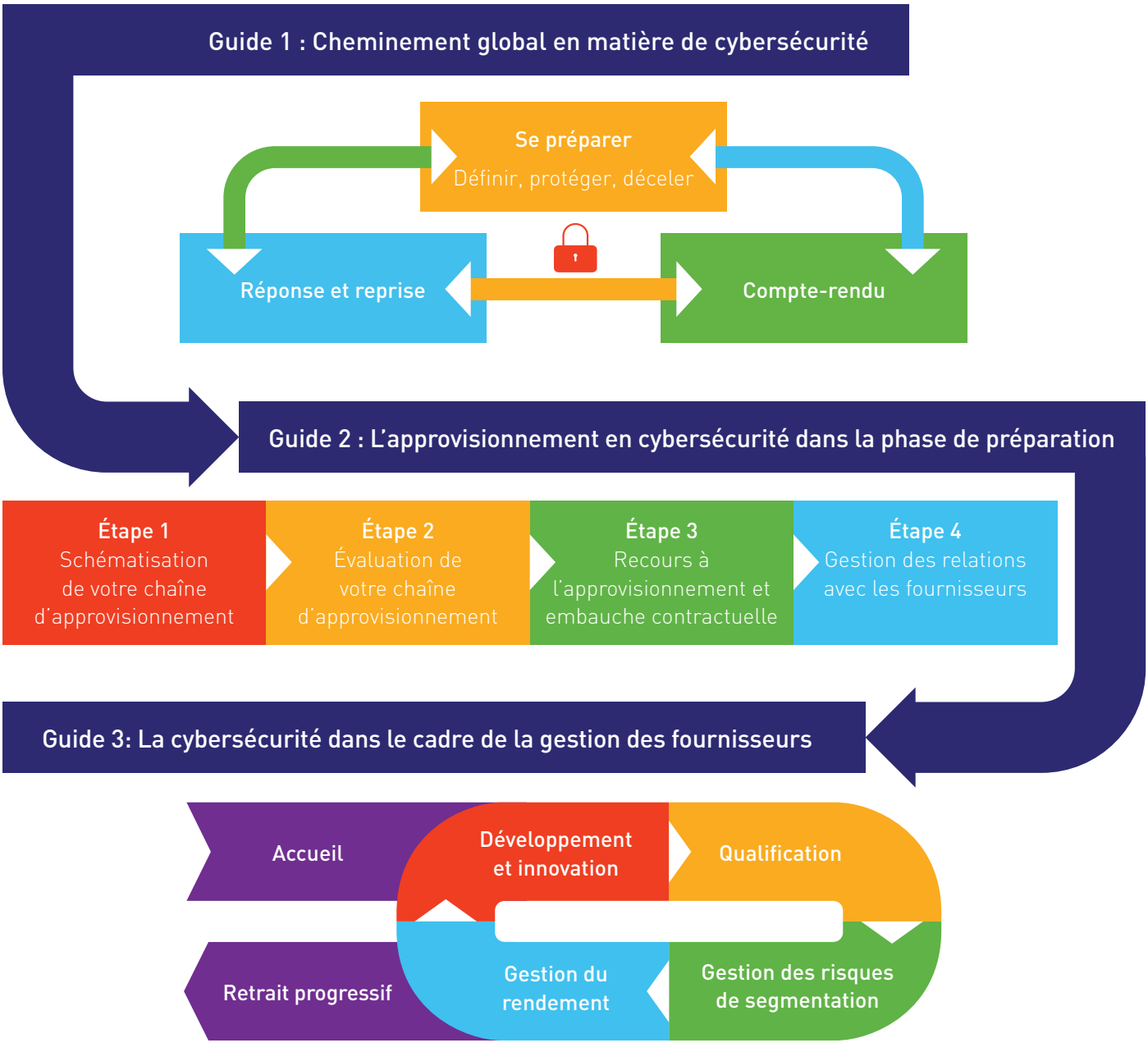
Comment est-ce que des contrats et des relations plus solides avec les vendeurs aident à gérer les risques liés à la cybersécurité? Prenons une situation récente en exemple.

Une entreprise de gestion immobilière a changé de vendeur d'appareils électroniques. Lorsque le contrat a pris fin, un nouveau vendeur a été choisi. Même si le vendeur précédent n'avait plus le contrat, il pouvait encore changer les affichages visuels. Une analyse plus approfondie a révélé que les contrôles et les contrepoids pertinents n'avaient pas été conçus pour gérer le vendeur et le contrat du vendeur, et le vendeur précédent disposait encore des privilèges administratifs pour accéder aux affichages par l'intermédiaire d'une connexion Wi-Fi non sécurisée. Une meilleure gestion de la relation et une évaluation de sécurité sur la manière dont l'accès est accordé et est désactivé auraient aidé à réduire le risque pour l'entreprise de gestion immobilière.

Ce qui est évident dans cet exemple, c'est qu'une menace liée à la cybersécurité peut émerger de n'importe où, et alors qu'elle peut présenter un risque relatif à l'information, elle peut aussi compromettre tout système à l'intérieur d'un immeuble – qu'il soit grand ou petit. Il est devenu essentiel de prendre les mesures nécessaires sur plusieurs fronts, y compris la gestion des relations avec les fournisseurs (GRF) et la cybersécurité, afin de réduire les risques et d'y remédier sans tenir compte de la catégorie d'immobilisations et de la technologie.

Comprendre la gestion des relations avec les fournisseurs (GRF)

Vos activités à titre de propriétaire ou de gestionnaire d'immeubles commerciaux dépendent de plusieurs fournisseurs et vendeurs. La gestion des relations avec vos vendeurs est essentielle pour que vous puissiez mener vos activités sans heurts, puisqu'ils sont souvent fortement intégrés dans votre organisation et que vous avez besoin de leur coopération. Dans un monde qui tend toujours plus vers le numérique, vos fournisseurs perfectionnent continuellement leur technologie et, par



conséquent, leurs sous-vendeurs et leurs fournisseurs également. Cela nourrit le besoin de bâtir des relations de collaboration solides afin de réduire les risques associés à la cybersécurité tout en vous permettant de tirer un meilleur parti des avancées technologiques dans vos immeubles. C'est ici que la gestion des relations avec les fournisseurs (GRF) entre en ligne de compte.

La gestion des relations avec les fournisseurs, parfois appelée la gestion des fournisseurs ou des vendeurs, est une approche globale de la gestion des interactions d'une organisation avec les vendeurs qui fournissent des produits et des services, dans le but d'améliorer la coopération, la coordination, la communication et la gestion des risques. Exactement comme les organisations gèrent et améliorent les relations avec les clients par l'intermédiaire de programmes de gestion des relations avec les clients, le recours à un programme de GRF est essentiel.

Les avantages de la GRF

La GRF stratégique est l'un des moyens les plus importants de stimuler l'innovation, et dans le cas des propriétaires et des gestionnaires d'immeubles commerciaux, de les aider à fournir des services haut de gamme aux clients et aux locataires.

Il y a plusieurs avantages à la GRF, et développer des relations mutuelles basées sur la confiance avec les fournisseurs stratégiques importants peut aider à harmoniser les efforts et à procurer des avantages importants, par exemple :

- un meilleur accès à l'innovation de produits par les fournisseurs;
- un risque lié à l'approvisionnement réduit grâce à une meilleure coopération;
- la coordination d'une chaîne d'approvisionnement simplifiée;
- la réduction des coûts à court, moyen et long termes;
- la détermination de processus d'approvisionnement plus efficaces;
- l'amélioration des résultats fondamentaux et des avantages concurrentiels.

La collaboration et l'établissement de relations de confiance

La fonction d'approvisionnement de nos jours cherche à dégager une valeur d'entreprise significative des relations avec les fournisseurs. Ce qui était davantage des relations basées sur des transactions entre les fournisseurs et l'organisation a cédé la place à des partenariats plus collaboratifs.

Les organisations qui échouent commencent souvent par des programmes de GRF en misant davantage sur le court terme, s'attendant à des avantages immédiats, et puis abandonnent leurs efforts à mi-chemin ou mettent en place une stratégie faible et une exécution ne donnant aucun avantage ou aucun profit. Les programmes de GRF devraient être vus comme des engagements à long terme, avec une approche transversale et coordonnée, une structure de gouvernance solide, et des méthodes innovantes pour suivre et mesurer la valeur.

Voici quelques-unes des meilleures pratiques en matière de GRF dont les propriétaires et les gestionnaires d'immeubles peuvent grandement bénéficier :

L'amélioration de la segmentation des fournisseurs

Souvent, les fournisseurs sont segmentés en fonction de leur incidence sur l'entreprise ou de la complexité du lien approvisionnement-marché. Selon ces deux paramètres, ils se classent dans diverses catégories : stratégiques, critiques, leviers et simples. Toutefois, cette segmentation conduit souvent à des erreurs d'exécution et à de mauvais rendements. Un troisième paramètre essentiel consiste à mesurer la compatibilité à long terme entre l'organisation et les fournisseurs. Cette segmentation aide davantage dans la conception d'un programme de GRF efficace. **La cybersécurité ajoute une autre dimension à votre segmentation selon laquelle vous pouvez segmenter vos vendeurs par niveau d'accès à des données et des systèmes critiques.**

Un modèle clair pour les fournisseurs principaux

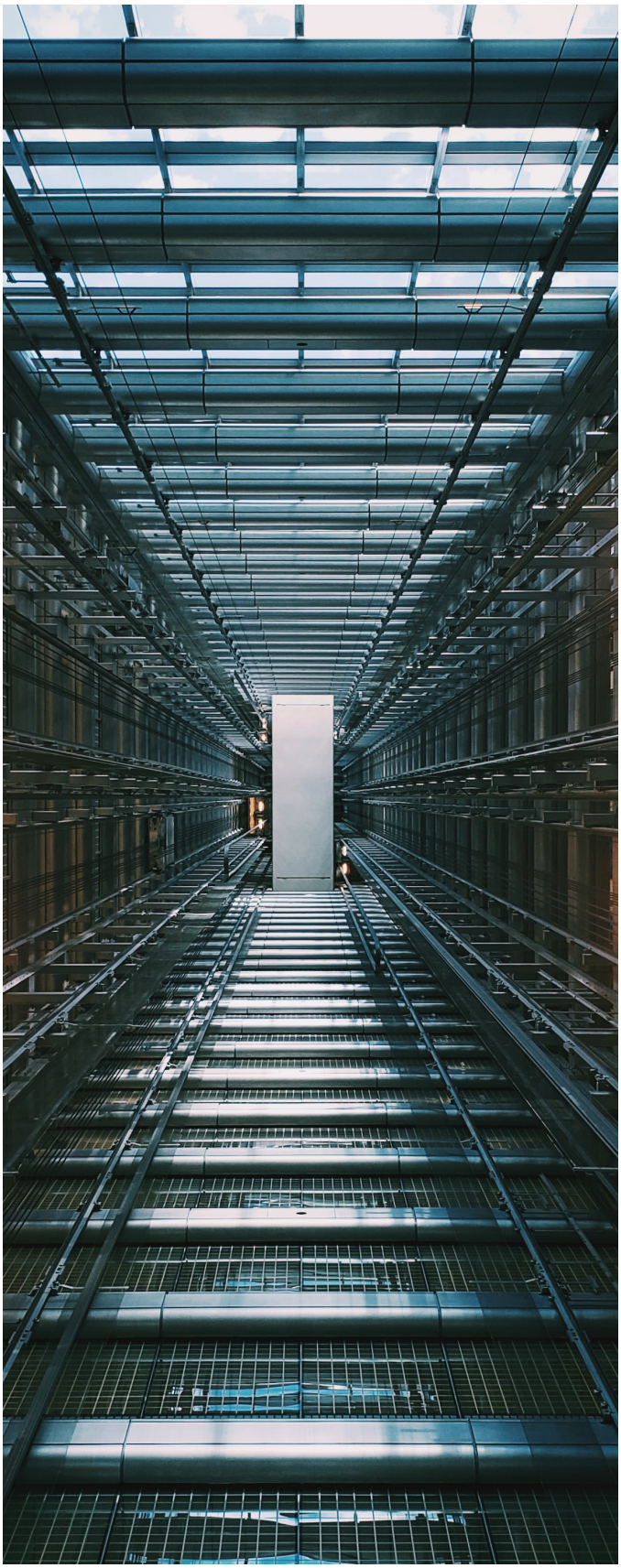
Une fois que les fournisseurs ont été segmentés, un modèle clair devrait être établi afin d'aider les organisations à assurer le suivi de la relation dès le début et pendant toute sa durée. Ce modèle pourrait inclure des facteurs tels que la responsabilité de gérer

régulièrement la relation, et de la gérer lorsque la haute direction doit intervenir. Le plus important est de s'assurer que l'organisation et le fournisseur visent le rendement afin que l'entreprise puisse atteindre ses objectifs opérationnels. Les fournisseurs principaux qui revêtent une importance stratégique nécessitent davantage de supervision et de surveillance que les autres. **Un élément essentiel sur le plan de la cybersécurité est d'assurer qu'il y a un plan clair pour la prévention des cyberincidents et l'intervention. Ce plan devrait découler d'une planification de haut niveau, ainsi que de mises à niveau en matière de suivi et de surveillance et de correctifs relatifs à la technologie que vos fournisseurs ont intégrée dans vos opérations.**

Une communication efficace

Il est important de traiter un fournisseur comme un partenaire, de maintenir une excellence communication afin de bâtir une relation mutuellement bénéfique à long terme, et d'agir de façon stratégique pendant toute la durée de la relation. Une communication claire et transparente ainsi que des séances de rétroaction sont cruciales, spécialement lorsque vous traitez avec des plans d'intervention en cybersécurité et avec l'exécution de ces plans en cas d'incident.

La façon dont les organisations gèrent les relations avec les fournisseurs peut faire la différence entre des fournisseurs qui peuvent les aider à réussir et des fournisseurs qui ne coopèrent pas lorsqu'elles en ont besoin. C'est seulement lorsque votre organisation est systématiquement investie dans sa relation avec les vendeurs principaux que vous pouvez coopérer et avoir confiance de pouvoir compter sur la cybersécurité, entre autres choses.



Les caractéristiques principales des bons programmes de GRF

La GRF implique d'adopter une stratégie, d'effectuer des évaluations et de planifier les mesures à prendre afin d'améliorer de façon continue les relations à long terme avec les fournisseurs stratégiques. Il existe plusieurs modèles, et chaque organisation a besoin d'évaluer quel modèle ou quelle combinaison de modèles convient à sa situation particulière. Intégrer des éléments liés à la cybersécurité dans votre modèle de GRF comporte des coûts pour vous et pour vos fournisseurs. Par conséquent, il est nécessaire de bien comprendre les avantages réciproques de la relation, et d'établir une confiance mutuelle, une équité et une communication honnête et ouverte.

Les facteurs principaux pour intégrer votre programme de GRF

Concevoir un programme qui vous convient

De nos jours, les organisations qui adoptent des pratiques exemplaires ont un programme de gestion des relations avec les fournisseurs en place qui convient à leur taille et qui peut être facilement adapté en prévision d'une croissance future. Un peu comme avec n'importe quel autre aspect de votre entreprise, des stratégies sont nécessaires pour établir une relation structurée avec vos principaux fournisseurs. Créez un plan avec des objectifs de GRF et des échéanciers clairement définis, énumérez les activités et les processus afin d'atteindre les objectifs, établissez les rôles et les responsabilités, et pour la cybersécurité, identifiez les systèmes et les données à haut risque qui doivent être pris en compte. Votre plan devrait être mesurable et réalisable, et assurer l'équité de ce que vous espérez de vos fournisseurs principaux.

Gérer le rendement

Un programme de GRF efficace devrait inclure des processus et des paramètres définis dans le but de gérer le rendement. Sur le plan de la cybersécurité, cela devrait inclure des réunions régulières avec les hauts responsables afin de discuter des plans de prévention et d'intervention liés à la cybersécurité, ainsi qu'avec les responsables des stratégies tactiques afin de vous assurer que les aspects plus techniques tels que les points d'intégration, les mises à niveau et les correctifs sont bien compris et gérés. Un engagement avec les différents niveaux de la direction et des opérations assurera que le programme fonctionne au quotidien et qu'il continue de satisfaire les objectifs à long terme des deux parties.

Bâtir des relations avec les fournisseurs stratégiques

Il est important d'accorder une plus grande valeur aux fournisseurs fortement intégrés qu'aux vendeurs réguliers, et de ne pas imposer des exigences purement transactionnelles ou basées sur les coûts. Ces relations de confiance nécessitent du temps et sont basées sur les avantages réciproques. Le niveau de connectivité technologique et d'intégration des données est une exigence principale reliée à la cybersécurité qui devrait être évaluée lorsque vient le temps de déterminer les fournisseurs stratégiques.

Adopter de bons comportements

Il incombe à la fois au fournisseur et à l'acheteur de favoriser les comportements souhaités dans le but d'assurer une situation d'avantages réciproques. La clé est de sélectionner des fournisseurs suffisamment investis – des activités purement opportunistes ou un manque de vision à long terme pourraient indiquer que le fournisseur ne vous convient pas. Si un fournisseur détermine de manière proactive vos cyberrisques potentiels dans le cadre de ses processus d'intégration, c'est un signal clair qu'il vise des avantages réciproques à long terme.

Initier des contrats solides

Créez un contrat clairement établi sur lequel vous êtes d'accord, dans lequel les modalités et les responsabilités selon le niveau de service sont définies. Vous éliminerez ainsi les conflits et les désaccords en cas de problème. Assurez-vous que les exigences et les attentes relatives à la cybersécurité sont clairement décrites dans vos contrats.

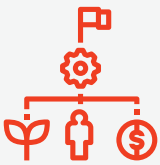
Offrir une formation adéquate

La formation est essentielle dans l'établissement d'un programme de GRF, afin d'informer vos employés sur les avantages et sur leur rôle, de manière à assurer la réussite du programme. Par exemple, une formation basée sur des mises en situation destinée au personnel de première ligne qui devra se préparer à intervenir en cas de cyberincidents devrait être un élément clé du programme.

S'attaquer aux obstacles

Il est indispensable de discuter ouvertement avec les fournisseurs principaux et de prendre en considération leurs rétroactions en ce qui concerne les obstacles. Y a-t-il des problèmes de communication avec lesquels ils doivent traiter lorsqu'ils travaillent avec votre organisation? Des logiciels incompatibles? S'attaquer aux obstacles initiaux est crucial pour résoudre les problèmes avec vos fournisseurs principaux, et cela sera particulièrement pratique en cas d'intrusion.

Investir dans la bonne technologie



Selon la taille de votre organisation et l'envergure de votre programme de GRF, l'établissement de systèmes et de processus de GRF solides avec les fournisseurs vous permettra de mieux visualiser l'état des relations et d'analyser vos facteurs de risque. La technologie peut vous fournir une vue d'ensemble exhaustive de ce qui touche votre chaîne d'approvisionnement, ce qui facilite la réduction des risques, y compris ceux qui découlent de la cybersécurité.

Éléments de la GRF associés à la cybersécurité

L'un des aspects évolutifs de la GRF consiste à travailler avec les vendeurs non seulement pour assurer l'innovation, mais aussi pour le faire de manière sécuritaire grâce à l'instauration de mesures de cybersécurité. La coopération et l'établissement de relations solides et saines avec les fournisseurs deviennent cruciaux dans le cadre de la gestion et de l'atténuation des risques, et quand l'intervention en cas d'atteinte à la cybersécurité doit se faire rapidement.

Même si plusieurs modèles et structures ont été créés, la meilleure approche reste de comprendre les besoins de votre organisation en fonction de votre situation et de votre envergure, plutôt que d'adopter une approche uniformisée. Dans cette section, nous avons tenté d'illustrer de quelle manière vous pouvez concevoir les éléments de cybersécurité à intégrer à votre programme de gestion des relations avec les fournisseurs.

Concevoir les éléments associés à la cybersécurité dans les processus de GRF

Certaines pratiques clés aident les entreprises à gérer leurs fournisseurs de manière plus efficace, ce qui permet par le fait même de renforcer leurs efforts liés à la cybersécurité. Nous avons fourni une liste de vérification que les propriétaires et les gestionnaires d'immeuble peuvent utiliser afin de mettre en place des pratiques exemplaires en matière de GRF, qui sont encore meilleures lorsqu'elles sont utilisées avec notre guide de la cybersécurité liée à l'approvisionnement :

Privilégiez ce qui est le plus important

- ☐ Classez les risques spécifiques à votre organisation, et créez des niveaux de priorité en fonction de vos actifs les plus importants et les plus vulnérables, c'est-à-dire ce que vous devez le plus protéger.
- ☐ Précisez l'intégrité de votre marque – comment vos clients vous perçoivent – et concentrez-vous sur cet élément, et non pas seulement sur la protection de la marque. Cette perspective facilitera la modélisation des menaces, ce qui à son tour vous permettra de détecter et de résoudre de façon proactive les vulnérabilités critiques dans votre chaîne d'approvisionnement.

Mobilisez votre organisation

- ☐ Élaborez des processus d'approvisionnement et de sélection avec l'avis du personnel des TI, de la sécurité, de l'ingénierie et de l'exploitation, afin que les décisions de sélection soient prises conjointement avec plusieurs intervenants et qu'elles tiennent compte de diverses exigences.
- ☐ Donnez aux échelons supérieurs la propriété et la responsabilité formelle de toutes les exceptions intégrées aux lignes directrices de cybersécurité et de toute incidence sur l'organisation qui en découle.
- ☐ Élaborez conjointement un organigramme des responsabilités qui définit clairement qui (entre vous et vos fournisseurs) est responsable de la gestion et de la surveillance des principaux points d'intégration des systèmes et de la sécurité des données et des systèmes sensibles.

Effectuez des évaluations globales du risque

- ☐ Si les vendeurs ont divers niveaux d'accès et posent différents niveaux de risque, concevez les évaluations de manière à mesurer les risques critiques et attribuez un niveau de risque approprié à chaque vendeur. Par exemple, vos évaluations pourraient révéler que le niveau de risque attribué à un concierge est différent de celui attribué à un technicien ayant accès aux systèmes.
- ☐ Songez à recourir à des processus de vérification et de validation des évaluations du risque sur place. Les fournisseurs offrent souvent des autoévaluations, mais celles-ci devraient être gérées globalement par le personnel de cybersécurité et de GRF de votre côté.
- ☐ Si nécessaire, offrez une formation croisée à votre personnel afin qu'il soit davantage intégré aux activités des fournisseurs. Cela leur permettra de surveiller les critères de sécurité exigés.

Travaillez avec les vendeurs sur la cybersécurité

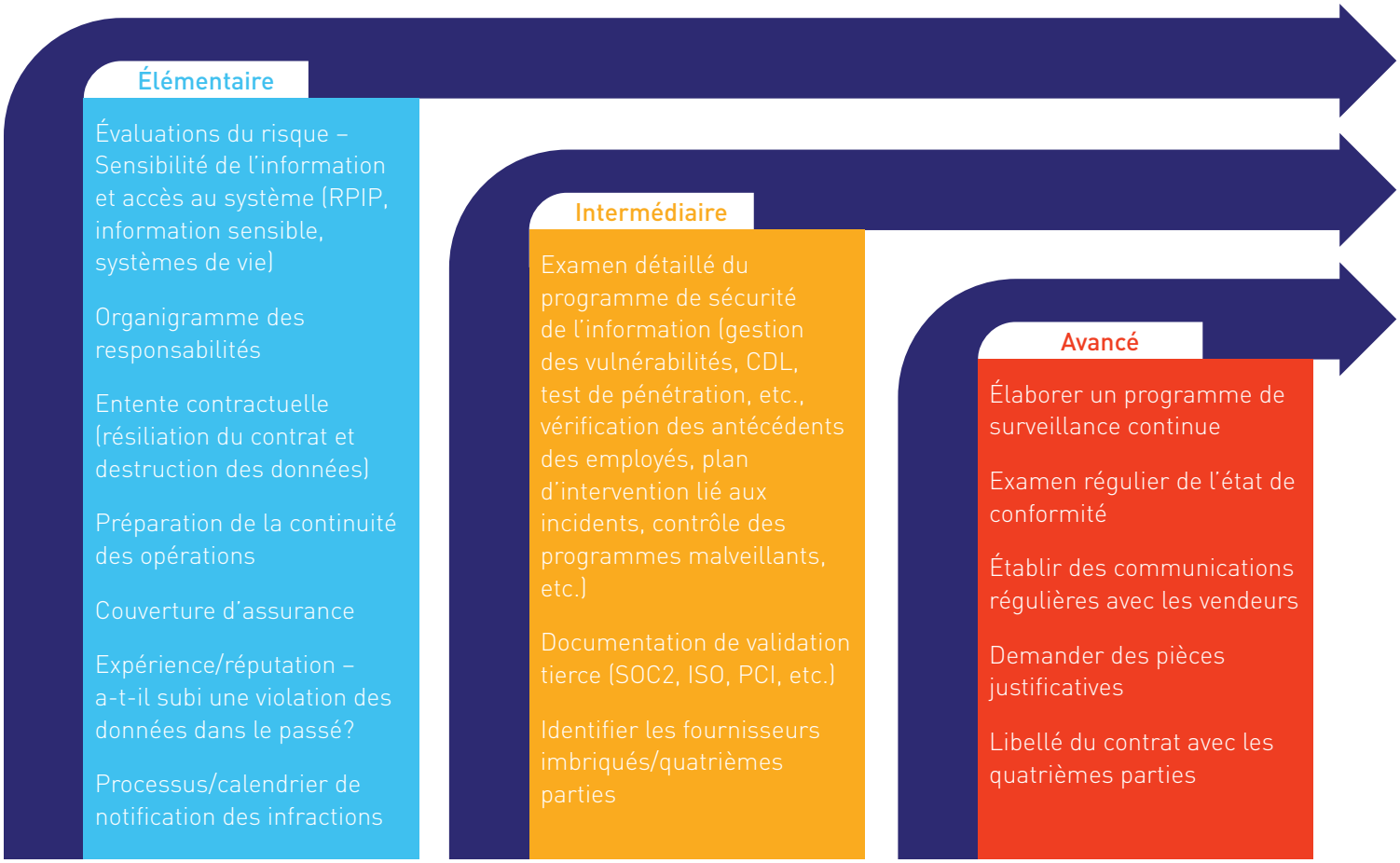
- ☐ Créez des listes de vendeurs approuvés, qui sont reconnus et qui se conforment à votre organisation, ainsi que des lignes directrices claires à propos des exigences et des processus pour les exceptions qui doivent être approuvées. Ce faisant, gardez à l'esprit la compatibilité des relations.
- ☐ Élaborez des modalités de sécurité standard – incluses dans toutes les demandes de propositions (DP) et tous les contrats – adaptées au type de contrat et aux besoins organisationnels. Consultez notre ancien guide de la cybersécurité liée à l'approvisionnement pour connaître les recommandations liées aux DP et à la conclusion de contrats.
- ☐ Pour les nouveaux fournisseurs, effectuez une période d'essai et d'évaluation – afin de tester les aptitudes des fournisseurs, ainsi que leur conformité et leur compatibilité avec diverses exigences – avant qu'ils ne rejoignent activement la chaîne d'approvisionnement. Dans des secteurs à haut risque, par exemple, un fournisseur pourrait passer par une série de pilotes rigoureusement contrôlés avant d'intégrer complètement la chaîne d'approvisionnement.
- ☐ Exigez des fournisseurs à haut risque et des principaux fournisseurs d'exiger les mêmes normes de leurs propres fournisseurs.
- ☐ Procédez à des examens trimestriels du rendement et des relations des fournisseurs menées par un groupe d'intervenants détenant les connaissances et l'expertise appropriées.
- ☐ Organisez des réunions annuelles avec les fournisseurs afin de vous assurer qu'ils comprennent les besoins, les préoccupations et les priorités en matière de sécurité de votre organisation.
- ☐ Offrez des programmes de mentorat et de formation aux fournisseurs, surtout dans des domaines d'intérêt clés ou difficiles liés à la cybersécurité.
- ☐ Créez une trousse sur la diligence appropriée à remettre aux nouveaux vendeurs potentiels ou à d'autres partenaires tiers afin qu'ils fournissent des renseignements clés sur la cybersécurité.
- ☐ Effectuez une évaluation continue et ponctuelle des relations des vendeurs sur le plan de la cybersécurité.

Certification des vendeurs : établir des critères et un programme pour certifier les vendeurs existants et nouveaux

Dans le secteur des immeubles commerciaux et résidentiels, la gestion des relations avec les fournisseurs sur le plan de la cybersécurité n'est pas un processus universel. La manière dont une organisation gère ses risques liés à la cybersécurité dépend grandement du portefeuille de propriétés et du niveau de technologie intégré dans ses opérations. Pour répondre à ces besoins particuliers, les organisations ont récemment commencé à élaborer des programmes de certification des vendeurs internes conçus afin de tenir compte des aspects uniques de leur profil de fournisseur. La création de programmes de certification aide à :

- évaluer rapidement le portefeuille du vendeur et établir les priorités pour un examen approfondi;
- obtenir des analyses pour des vendeurs qui n'étaient pas encore évalués;
- alerter l'organisation dès qu'une modification importante est apportée en ce qui concerne les fournisseurs individuels;
- repérer les changements de pointage au fil du temps afin de définir des habitudes, qui montrent des tendances positives et négatives;
- trier les vendeurs potentiels durant la DP ou le processus de sélection;
- surveiller de manière continue les fournisseurs qui présentent un risque de moyen à élevé;
- définir rapidement les problèmes spécifiques que les nouveaux fournisseurs doivent régler durant les négociations liées au contrat;
- autoriser des processus d'intervention en cas d'incident lié à la cybersécurité lorsque de nouvelles vulnérabilités sont relevées.

Comme c'est le cas pour votre programme de gestion des relations avec les fournisseurs, le programme de certification des fournisseurs intégré peut évoluer. Le diagramme ci-dessous illustre la marche à suivre pour lancer votre programme de certification et l'adapter au besoin avec le temps.



CDL : cycle de développement des logiciels

ISO : Organisation internationale de normalisation

PCI : Norme de sécurité des données de l'industrie des cartes de paiement

RPIP : renseignements permettant d'identifier une personne

SOC2 : Contrôle d'organisation de services 2, décrit divers contrôles organisationnels liés à la sécurité, à la disponibilité, à l'intégrité du traitement, à la confidentialité ou à la vie privée

Centre d'excellence

Toutes les organisations se doivent de créer une source d'information centralisée en lien avec la cybersécurité qui sera accessible à tous au sein de l'organisation. Il peut s'agir d'une personne ou d'un service qui se consacre à cette question d'une importance cruciale, ou d'une base de connaissances d'un tiers externe que vous pouvez consulter lorsque c'est nécessaire. L'option qui vous convient le mieux dépend de l'étendue de vos activités ainsi que de votre cheminement spécifique en matière de cybersécurité.

Votre centre d'excellence devrait assumer certaines responsabilités clés, exposées ci-dessous.

Répertoire des meilleures pratiques : Le centre d'excellence devrait garder un registre central des meilleures pratiques de cybersécurité pour vos immeubles, lesquelles sont déployées et évoluent à mesure que les menaces évoluent. La gestion des fournisseurs et les aspects des relations devraient être coordonnés par les personnes ou l'équipe responsables de la GRF.

Formation : Il est essentiel de planifier des formations de sensibilisation à la cybersécurité à des intervalles réguliers pour les gestionnaires d'immeubles de

première ligne, les équipes de l'exploitation et quiconque a accès aux données ou aux systèmes et a la responsabilité de collaborer avec les fournisseurs. Vous pouvez également, selon votre relation avec les fournisseurs, inclure les fournisseurs principaux.

Inventaire lié à la cybersécurité : L'établissement et la tenue à jour d'un inventaire des appareils et de la technologie utilisant Internet sont essentiels à la cybersécurité, et cet inventaire devrait être centralisé afin de surveiller les risques.

Listes et certifications des vendeurs : Une liste des vendeurs et de leur niveau d'accès aux données, à la technologie ou aux systèmes devrait être centralisée. Les normes, les certifications et les recertifications en matière de cybersécurité que votre organisation demande à vos vendeurs dans le cadre de votre protocole de cybersécurité devraient être contrôlées et surveillées de manière centrale, et établies en collaboration avec les personnes ou l'équipe responsables des relations avec les fournisseurs.

Protocoles relatifs aux nouvelles technologies : Les protocoles dont vous avez besoin en matière de cybersécurité doivent être gérés de manière cohérente en ce qui a trait à l'installation de nouvelles technologies, et pour les vendeurs qui proposent un test bêta ou de contrôle pour une nouvelle technologie. Les installations, les correctifs, les mises à niveau et les pilotes doivent respecter les normes et l'autorisation centralisées, et la personne ou l'équipe centrale devrait travailler avec tout le monde au sein de l'organisation afin de s'assurer que les fournisseurs s'y conforment.

Exigences en matière d'approvisionnement : Dans notre dernier guide, nous avons approfondi la cybersécurité en matière d'approvisionnement, y compris dans les contrats, les demandes de propositions (DP) et les demandes de renseignements (DR). Le centre d'excellence devrait être une ressource centralisée afin que vous puissiez uniformiser et contrôler ces exigences.

Conserver une source centrale et normalisée pour assurer l'excellence de la cybersécurité peut aider de manière significative à repérer et à réduire les nombreux maillons faibles qui peuvent exister dans votre chaîne d'approvisionnement. Le centre d'excellence, associé à la coordination et à la communication dans l'organisation afin d'assurer un programme de GRF solide, peut aider à réduire les risques dans toute l'organisation.

Préparation et collaboration des fournisseurs

Auparavant, l'approvisionnement a souvent été considéré comme une fonction transactionnelle – il s'agissait de définir les prix et les modalités de livraison, et de créer et de renouveler les contrats avec les fournisseurs. L'accent était mis sur la réduction des coûts plutôt que sur la recherche d'occasions qui génèrent de la valeur. Aujourd'hui, cette vision a changé avec la reconnaissance de la valeur que la GRF apporte. Des relations basées sur la confiance avec des fournisseurs stratégiques clés entraînent des progrès importants dans le domaine de la préparation et de la collaboration des fournisseurs dans l'éventualité d'un incident de sécurité. Planifier et gérer de manière proactive et stratégique les interactions essentielles avec les fournisseurs clés pendant et après l'incident aide à gagner un avantage significatif sur les cybercriminels et réduit de manière significative les dommages et la durée de l'indisponibilité.

Détermination, communication et intervention

Lorsqu'un incident survient, votre vendeur devrait avoir mis en place un plan afin de vous informer immédiatement si l'infraction est survenue de son côté. Il devrait travailler avec vous, en collaboration avec votre équipe, afin de s'attaquer à tout problème lié à cet incident.

Vous devriez bien comprendre et parfaitement approuver la façon dont il prend en charge la détection des incidents et ses interventions. Dans le cadre de votre programme de GRF, vous pouvez parvenir à une solide compréhension de la capacité de votre fournisseur à détecter les incidents et à intervenir en faisant ce qui suit :

- ☐ Incluez une obligation juridique dans le contrat afin que le fournisseur vous avertisse dans l'éventualité d'un incident.
- ☐ Évaluez son plan de gestion des incidents afin de vous assurer qu'il est compréhensible et qu'il comprend des outils de protection contre les intrusions, des pare-feu, des protections contre les programmes malveillants, un programme de gestion des correctifs et des détails concernant son délai et ses processus d'intervention en cas d'incident.
- ☐ Vérifiez si le vendeur a souscrit une assurance en matière de cybersécurité qui correspond à vos exigences.
- ☐ Incluez des vendeurs stratégiques (dans la mesure nécessaire) lorsque vous préparez des mises en situation pour l'intervention en cas d'incident.
- ☐ Planifiez des séances de débreffage détaillées afin d'évaluer la qualité des interventions en cas d'incidents et de viser l'amélioration continue.

Conclusion

La technologie nous conduit souvent dans des territoires inconnus, puisque les occasions et les menaces changent constamment. Alors que les menaces évoluent, les tendances liées à la cybersécurité en font autant. Les meilleures pratiques en matière de GRF doivent maintenir la cadence, et les vendeurs doivent jouer un rôle crucial dans la réduction des cyberrisques. Une GRF efficace permet à votre organisation de saisir des occasions et de profiter d'économies majeures, et elle peut vous aider à éliminer les risques liés à la chaîne d'approvisionnement, à améliorer les services des fournisseurs et à aider à améliorer l'expérience des clients et des locataires.

Il est important de ne pas simplement commencer votre cheminement de GRF et de cybersécurité, mais de vous demander continuellement comment vous progressez vers la mise en œuvre de pratiques exemplaires. Même si votre stratégie est la bonne pour vous aujourd'hui, elle pourrait ne plus convenir à vos besoins demain, surtout compte tenu de la rapidité avec laquelle les changements technologiques surviennent.

Remerciements

We are grateful for the financial support of QuadReal and First Capital, and for the expertise provided by MNP LLP.

Our contributors, who shared their insight and spent valuable time on this guide:

Scot Adams
National Services
Colliers International

Stephen Adams
General Manager
Cushman Wakefield Asset Service ULC

Trent Bester
Senior Vice President, Consulting and Public Sector
MNP

Ken J. Cowan
Vice President, National Programs
Morguard Investments Limited

Nada Ebeid
Business Development Manager – Canada
Genetec

Sam Flis
Director, Property Technology
BentallGreenOak

Michael Di Grappa
Senior Vice-President, Property Management
Canderel

Cheryl Gray
Head of Special Projects, Operational Excellence
QuadReal Property Group

Sue Klinner
Vice President, Business Process and Risk Management
First Capital

Victor Lauer-Martin
Information Security Architect
Ivanhoé Cambridge

Lachlan MacQuarrie
Vice President, National Programs
Oxford Properties Group

Kendall Peart
Managing Director, Real Estate
MARSH

David Sulston
Director, Security
Oxford Properties Group

Lee Thiessen
National Leader, Real Estate and Construction
MNP

Naveli Thomas
Director
Nyox

L'équipe de BOMA Canada

Benjamin Shinewald
President & CEO
BOMA Canada

Michael Parker & Natalie Rekai
Marketing and Communications Consultants
BOMA Canada

BOMA Canada sincerely regrets any errors or omissions in the list above and thanks all our volunteers and contributors for their support.

This report is availble in English

BOMA Canada

www.bomacanada.ca