BOMA Canada

Guide du bien-être cybernétique 2019

Comment gérer les risques présents dans le domaine de l'exploitation d'immeubles commerciaux

Ce guide est commandité par :

MNP LLP

QuadReal

CAPREIT

Nous sommes fiers de vous présenter ce guide du bien-être cybernétique qui consiste en un outil pour aider les propriétaires et les gestionnaires d'immeubles à se préparer à plonger dans l'univers de la cybersécurité.

Chers amis,

Au fil des années, les cybermenaces se sont multipliées en matière de fréquence et de types de violations.

Les entreprises ont réagi en instaurant des mesures visant à protéger leurs informations et leurs systèmes. Les menaces existent également dans le domaine de l'exploitation d'immeuble et, tout comme pour les systèmes des entreprises, il faut prendre ces menaces plus au sérieux, car elles peuvent avoir d'importantes ramifications en matière de perte de données, de sécurité humaine, de compétitivité et de réputation.

Pour vous aider à mieux comprendre ces risques et savoir comment vous préparer en ce qui concerne les activités des immeubles avant qu'un incident ne se produise, nous avons créé ce guide du bien-être cybernétique. La cybersécurité est un sujet souvent complexe et technique, mais nous nous sommes efforcés de l'adapter à l'état de préparation actuel du secteur et nous avons puisé des idées dans une variété de sources.

Qui devrait lire ce guide?

Ce guide vise principalement à présenter le concept de planification de la cybersécurité pour les gestionnaires et les dirigeants d'exploitation dans le domaine de l'immobilier. Nous croyons que ce guide sera utile à toute personne travaillant directement ou indirectement dans le domaine de l'exploitation immobilière commerciale et institutionnelle ou y occupant un poste de gestionnaire ou toute personne étant exposée à des systèmes connectés à Internet.

Comment ce guide doit-il être utilisé?

Ce guide tient lieu d'introduction pour mieux comprendre les risques en matière de cybersécurité présents dans l'industrie de l'immobilier commercial. Il contient une liste de vérification relative à la cybersécurité pour les immeubles. Cependant, celle-ci doit uniquement servir de guide général, car elle ne consiste pas en une stratégie ou une norme complète en soi. De ce fait, les renseignements qu'elle 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 vous trouvez notre Guide du bien-être cybernétique utile et qu'il permettra de vous aider à entamer votre aventure visant à protéger les activités de votre immeuble contre les cybermenaces. Puisque les risques et les réglementations relatifs à la cybersécurité ne cessent d'évoluer, nous souhaitons vous tenir au courant de ces changements en publiant des éditions régulièrement.

Veuillez agréer l'expression de nos sentiments distingués.

Benjamin Shinewald
président et directeur général,
BOMA Canada

Lee Thiessen
Dirigeant national, service immobilier,
MNP

Cheryl Gray
vice-présidente directrice,
innovation des entreprises,
QuadReal Property Group

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.

Introduction

Aujourd'hui, les systèmes intelligents ou connectés à Internet permettent de soutenir les activités commerciales et d'augmenter l'efficacité des immeubles de l'industrie de l'immobilier commercial. Que ce soit en ayant permis d'améliorer l'efficacité des systèmes d'ascenseurs ou bien de surveiller et d'optimiser le rendement des CVCA, ils se sont avérés être une aide très précieuse dans le domaine de l'immobilier. Cependant, ils ne sont pas dépourvus de risque.

Le piratage, les logiciels malveillants et d'autres défis connexes à la cybersécurité affectent les systèmes d'information des immeubles. Êtes-vous bien armé pour détecter ces menaces et y répondre? Puisque le nombre d'immeubles intelligents et d'appareils intelligents installés dans des immeubles ne cesse d'augmenter, les incidents relatifs à la cybersécurité d'un immeuble pourraient affecter considérablement la propriété et ses activités.

Ces systèmes intelligents commerciaux, ce que nous appelons « Internet des objets industriel » (IIoT), collectent souvent, en fin de compte, beaucoup de données. De plus, ceux-ci sont connectés à Internet, et parfois, les responsables du fonctionnement des immeubles ne le savent même pas. Ces systèmes sont donc à risque, tout comme des ordinateurs dans des bureaux. Cependant, ils le sont encore plus, car les mesures de protection en matière de cybersécurité ne sont souvent pas appliquées à ces systèmes avec autant de rigueur et moins de personnes sont sensibilisées à ces risques.

Les systèmes intelligents commerciaux du marché actuel sont axés sur l'utilisateur. Cependant, personne ne les a nécessairement examinés en prenant en compte de la cybersécurité. De ce fait, la responsabilité des gestionnaires immobiliers a augmenté : ils doivent impérativement concevoir un plan solide pour prévenir et traiter les problèmes relatifs à la cybersécurité.

En plus du réseau en expansion des appareils intelligents, les criminels sont aussi devenus plus persistants et patients, que ce soit pour demander des rançons ou faire des ravages. Sans compter les pirates informatiques locaux qui pourraient faire des tentatives d'hameçonnage ou utiliser un logiciel rançonneur pour causer des dommages potentiels, il ne faut pas non plus oublier les menaces internationales : lorsqu'il est question de risques liés à la sécurité, celle-ci n'a aucune frontière. Par conséquent, aucun secteur n'est à l'abri.

L'augmentation du nombre de systèmes intelligents a aussi accru les risques liés à la cybersécurité

1 Portes automatisées
2 Lecteurs de carte
3 Contrôleurs de gestion d'accès
4 Contrôle des produits chimiques utilisés pour le traitement des eaux
5 Refroidisseurs et chaudières
6 Pompes
7 Appareils de traitement d'air des salles informatiques
8 Poste de l'opérateur
9 Panneaux de commande d'alarme incendie
10 Support/serveur répartiteur intermédiaire >PDU
11 Accès au garage
12 Thermostats et humidostats
13 Systèmes d'eau
14 Distributeur automatique
15 Électricité, gaz, chauffage
16 Caméras
17 Diffuseurs
18 Unités VAV
19 Système d'extinction d'incendie au halon
20 Unités de chauffage
21 Éclairage
22 Panneaux de contrôle de zone
23 Ascenseurs
24 Tours de refroidissement
25 Détecteurs de fumée
26 Panneaux solaires
27 Ventilateurs aspirants
28 Ventilateurs
29 Serpentins de refroidissement
30 Contrôleurs de traitement de l'air
31 Filtres à air
32 Services de qualité de l'air intérieur
33 Clapets

Le rythme d'adoption et de changement des systèmes intelligents commerciaux est rapide, tout comme celui de l'évolution des risques qui ne cesse d'augmenter. Comme mesure de protection, il est impératif que les propriétaires et les gestionnaires d'immeubles commerciaux conçoivent un programme de cybersécurité qui prend en compte cette nouvelle norme.

Puisque nous manquons de cadres conçus précisément pour tenir compte de la cybersécurité opérationnelle à l'échelle de la propriété, nous avons créé ce Guide du bien-être pour vous aider tout au long du processus.

« Puisque l'industrie de l'immobilier commercial ne cesse d'intégrer des technologies dans ses activités commerciales, il est alors important pour notre industrie de prendre connaissance des risques connexes à la cybersécurité. Ce guide a pour but d'aider les gestionnaires de propriété à concevoir des stratégies pour contrer les risques en matière de cybersécurité à l'échelle de la propriété. »

– Cheryl Gray, première vice-présidente de l'innovation des entreprises, QuadReal Property Group

Les répercussions des cyberattaques sur votre organisation

Tout incident malicieux survenant à tout niveau de l'immeuble peut avoir des conséquences mineures ou désastreuses sur votre organisation. Si un pirate informatique a pris le contrôle de votre système, la sécurité des personnes et de votre propriété pourrait alors être compromise. Celui-ci pourrait exiger une rançon monétaire, mais même si vous la payez, il se peut qu'il ne vous lâche pas. Les systèmes intelligents peuvent aussi donner accès aux systèmes de données de l'immeuble ou des sièges sociaux. Les renseignements relatifs aux personnes et aux entreprises qu'ils renferment pourraient alors être utilisés à mauvais escient.

Les incidents relatifs à la cybersécurité survenus dans votre immeuble peuvent poser de nombreux risques et entraîner beaucoup de conséquences :

- La sécurité des personnes pourrait être compromise par l'entremise des systèmes de contrôle externes.
- Vous pourriez perdre votre réputation s'il s'est produit une violation de données ou bien si vous n'avez pas pu fournir de service en raison de défaillances du système.
- Des locataires ou des clients pourraient perdre confiance en vous. Par conséquent, vos revenus en seront affectés.
- Vous pourriez être tenu responsable de la mauvaise utilisation des données des personnes et des organisations.
- Des actions judiciaires pourraient être intentées contre vous. Vous devrez alors assumer les coûts associés à celles-ci.
- Vous pourriez devoir payer des frais de résolution de conflit relatifs à une brèche.
- Vous pourriez devoir payer des frais de vendeur pour rétablir les systèmes.
- Vous pourriez devoir payer des coûts pour réparer les dommages matériels.

Partout dans le monde, de graves incidents connexes à la cybersécurité se sont produits et ceux-ci ont causé des coûts et des dommages considérables. Divers canaux ont été utilisés par les pirates pour causer ces incidents, y compris un anti-maliciel qui a été envoyé et utilisé involontairement par des vendeurs. Selon une étude de 2018 qui a été menée par Ponemon relative aux coûts engendrés par une brèche de données, le coût moyen global engendré par une brèche de données serait de 3,86 millions de dollars américains, soit 148 dollars américains par bloc de données. Depuis 2017, ce chiffre a augmenté de 6,4 %. Ce ne sont pas tous les incidents qui sont graves, mais chacun d'entre eux affecte votre organisation.

Scénarios : Donner vie aux risques

Afin de vous aider à mieux comprendre les risques, nous vous présentons trois scénarios qui se sont réellement produits.

Scénario 1 : Utilisation de données à des fins d'extorsion

Une personne travaillant à l'entreprise XYZ a reçu par courriel une facture en format PDF d'un fournisseur tiers fiable. Celle-ci semblait normale. Cependant, celle-ci était en fait un fichier malveillant qui a été envoyé par des pirates sous forme de facture. Une fois que le paiement a été effectué, les cybercriminels ont pu accéder à l'ordinateur de l'utilisateur. Les authentifiants des administrateurs locaux et des utilisateurs ont été ensuite récoltés et utilisés dans l'environnement réseau. Puisque toutes les copies de sécurité étaient accessibles et publiées en ligne, les pirates ont supprimé toutes les copies de sécurité actives et ont désactivé le système.

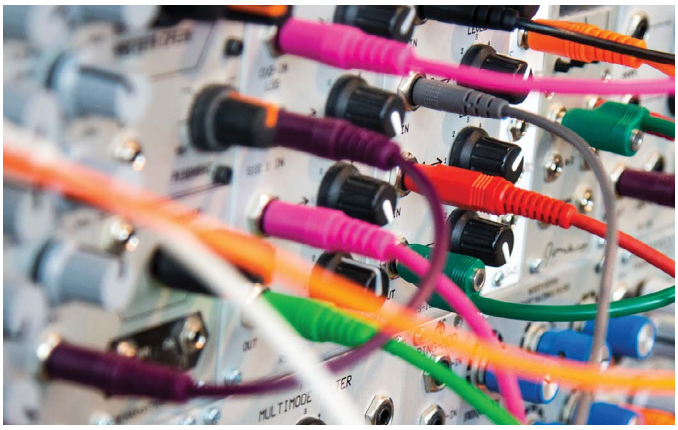
Une campagne de logiciel rançonneur et de cryptages de fichiers subséquente a commencé à 3 h, un samedi soir, et a affecté toutes les stations de travail et les serveurs de l'environnement. Le fournisseur de services TI a été appelé pour résoudre le problème seulement après que le personnel ne pouvait plus accéder au réseau.

Malheureusement, après évaluation, la récupération des images du système et des dossiers n'a pas pu être effectuée en raison du manque de copies de sauvegarde.

Une fenêtre est apparue sur tous les postes de travail et les serveurs. Celle-ci indiquait qu'il fallait payer une rançon et que toute l'organisation a été compromise. Dépourvus d'un plan de réponse aux incidents, tous les employés de l'entreprise ont paniqué et ont fait appel à une entreprise spécialisée en cybersécurité pour obtenir de l'aide. Pour remettre ses systèmes d'intercommunication en ligne, l'entreprise devait payer une rançon s'élevant à six chiffres, évitant ainsi l'interruption de ses services. Les coûts et les pertes de profits engendrés par cette menace ont été très importants. Désormais, les dirigeants de l'entreprise sont en train de concevoir de meilleures mesures de protection, de créer un plan de réponse aux incidents et d'offrir de la formation aux utilisateurs relative à la cybersécurité.

Scénario 2 : Brèche de renseignements par l'entremise d'un entrepreneur de CVCA

Un détaillant important a été confronté à une brèche à grande échelle. Lorsqu'un vendeur tiers de CVCA s'est branché au système de l'un des établissements qu'il dessert pour effectuer un entretien routinier, des pirates qui avaient réussi à infiltrer le système, ont alors pu accéder à ses systèmes.



Puisque les systèmes réseau et les renseignements du détaillant n'avaient pas été correctement séparés, les criminels ont pu étendre leur accès aux systèmes de paiement, soit l'endroit où les renseignements des cartes des clients sont stockés. Le détaillant n'a pas été capable de détecter la brèche, par conséquent, il n'a pas pu la contrecarrer : des millions de cartes de crédit et de renseignements appartenant à des personnes ont été compromis.

Beaucoup d'aspects ont été négligés : le degré d'accès des personnes et des vendeurs, le manque de séparation entre les différents systèmes et la ségrégation des renseignements essentiels et l'incapacité à détecter ou à désamorcer adéquatement les tendances inhabituelles.

Après avoir fait face à des poursuites, il a été largement rapporté qu'il a dû payer des règlements à l'amiable excédant les 18 millions de dollars américains, sans compter les frais de procès, de coupures, de dommage et de rétablissement, et sans mentionner la perte de réputation et de confiance. Au total, cette situation lui a coûté des centaines de millions de dollars.

« un vendeur tiers de CVCA s'est branché au système de l'un des établissements qu'il dessert pour effectuer un entretien routinier, des pirates qui avaient réussi à infiltrer le système ont alors pu accéder à ses systèmes. »

Scénario 3 : Une brèche survenant dans les systèmes de l'immeuble a compromis la sécurité de celui-ci

Un pirate informatique a décelé une vulnérabilité dans un serveur Web public et s'est servi de ses outils pour l'exploiter.

Une fois qu'il a réussi à s'infiltrer dans l'environnement, il a ensuite trouvé d'autres serveurs de fichiers, des systèmes d'exploitation d'immeubles, et bien d'autres choses.

Il est aussi tombé sur un système de commande industriel qui servait autrefois à contrôler le système d'échappement du garage. Celui-ci venait tout juste d'être automatisé, alors le pirate s'en est servi pour arrêter le système d'échappement. Ensuite, il a envoyé un courriel au personnel de l'entreprise pour lui demander de lui virer un montant inconnu de Bitcoins, en échange de quoi, il remettrait en marche les ventilateurs d'extraction. Une fois que le personnel de l'entreprise a pris connaissance de cette demande de rançon, il a tenté de se connecter directement au système pour découvrir qu'il ne pouvait pas y accéder, car les pirates avaient changé les mots de passe.

Alors, il a appelé un fournisseur de système d'échappement, qui possédait une copie de sauvegarde en ligne, afin de rétablir le système, et le personnel d'une entreprise spécialisée en cybersécurité pour résoudre le problème d'accès au service. Une fois que la menace immédiate a été neutralisée, le prochain défi était alors de trouver les autres systèmes et portes arrière qui avaient été infiltrés par le pirate.

Le personnel de l'entreprise spécialisée en cybersécurité a mené une enquête et des balayages de sécurité pour trouver d'autres faiblesses dans l'organisation, et quelques-unes d'entre elles ont été immédiatement rectifiées. Étant donné que l'organisation avait bien été préparée pour contrer ce genre de menace, il a été possible de contrôler l'accès au système et de résoudre cette situation sans subir de dommages importants tout comme de limiter son exposition.

Ces situations se sont déjà produites et peuvent encore arriver dans l'industrie immobilière, et ce, n'importe où. Puisque le problème n'est pas causé par un mauvais fonctionnement du système en soi, mais bien par des brèches de contrôle, vos employés, et même, vos vendeurs, peuvent éprouver de la difficulté à diagnostiquer le problème et à reprendre le contrôle des systèmes.

Évolution des réglementations relatives à la protection des renseignements permettant d'identifier une personne

Alors que le public et les intervenants sont de plus en plus inquiets, les membres des conseils d'entreprises publiques exigent davantage de rapport en matière de cybersécurité, tout comme les compagnies d'assurance.

Les exigences réglementaires connexes à la protection des renseignements permettant d'identifier une personne existent aussi et sont conçues ici, au Canada. Ces exigences auront des répercussions sur vos immeubles si vous stockez des renseignements relatifs à vos clients, vos locataires, vos employés, etc. Il est important que vous compreniez bien les risques associés à ceux-ci et de quelle manière une atteinte à la vie privée peut affecter votre immeuble.

Le gouvernement du Canada exigera bientôt que des rapports relatifs à l'atteinte à la vie privée soient produits, en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), conformément aux nouvelles exigences en matière de tenue de registres. Le Règlement général sur la protection des données (RGPD) de l'Union européenne touche de nombreuses organisations dans le monde, et il est fort probable que les autres pays rédigent bientôt eux aussi leur propre version de ce règlement.

Puisque le nombre de réglementations et de règlements visant à protéger les renseignements personnels ne cesse d'augmenter, il se peut que vous deviez adapter votre établissement pour vous conformer à ceux-ci. En vous préparant, vous pouvez atténuer les risques liés à la cybersécurité, et même, prendre de l'avance sur les exigences qui pourraient être établies dans le futur. Bien que cet aspect ne soit pas abordé dans ce document, nous vous recommandons de vous tenir informé sur les modifications réglementaires et d'ajuster vos pratiques d'entretien en matière de cybersécurité en fonction de celles-ci.

> “Le gouvernement du Canada exigera bientôt à ce que des rapports relatifs à l'atteinte à la vie privée soient produits, en vertu de la Loi sur la protection des renseignements personnels et les documents électroniques (LPRPDE), conformément aux nouvelles exigences en matière de tenue de registres.”

Être préparé : Une liste de vérification

Nous comprenons que votre immeuble ou votre groupe d'immeubles précis peut être unique, et que chaque propriété est gérée différemment. Au lieu de vous offrir des recommandations universelles et prescriptives, nous avons créé une liste de vérification qui vous permettra d'évaluer et ensuite de traiter les vulnérabilités les plus fréquentes relatives à la cybersécurité qui ont été trouvées dans l'exploitation de votre immeuble.

Nous vous présentons une approche générale pour gérer les risques qui est divisée en trois phases : la préparation, la résolution et le compte-rendu. Cette liste de vérification est aussi divisée par ces trois phases :

> « Désormais, un incident cybernétique impliquant un IIoT n'est plus "imprévisible ". Bien que l'industrie soit incapable d'empêcher tous les risques liés à la cybersécurité, la planification et le dévouement des employés de votre entreprise envers la cybersécurité peuvent permettre d'atténuer les divers risques inhérents à ce domaine. »
>
> **– David Sulston, directeur de la sécurité, Oxford Properties Group**

1 Se préparer > **2 Résoudre le problème** > **3 Effectuer un compte-rendu**

1. Se préparer

Les cybercriminels d'aujourd'hui attendent patiemment de trouver un maillon faible dans toute votre chaîne d'approvisionnement. Que ce soit par l'entremise du réseau d'exploitation de votre immeuble ou bien d'un vendeur tiers, ils peuvent trouver un point d'entrée et causer des dommages. Il faut déployer beaucoup d'efforts pour les contrecarrer et se préparer à faire face à leurs menaces. S'ils éprouvent de la difficulté ou en viennent à la conclusion qu'il s'avère très coûteux de vous attaquer, il est fort probable qu'ils laissent tomber.

Lors de la phase de préparation, vous devez prendre des mesures proactives pour éviter un accident, mais aussi vous préparer à faire face à un problème que vous pourriez tout de même rencontrer. Cette phase est très longue, mais elle doit impérativement être effectuée au complet, et ce, de la bonne façon. Une première phase solide vous permettra de vous munir de plans et de dispositifs de protection efficaces. Nous avons divisé cette phase en trois niveaux, soit les bases, les fondations et l'organisation, pour vous aider à l'effectuer systématiquement et à définir votre niveau actuel.

> « Avec l'émergence et le déploiement de l'analyse des données, de l'IIoT et de l'intelligence artificielle qui permettent d'avantager l'industrie et les communautés, chaque organisation devra améliorer ses capacités de protection en matière de cybersécurité pour répondre aux nouvelles demandes. Ces nouvelles demandes exigeront d'établir de nouvelles stratégies pour se protéger contre le comportement malveillant se produisant dans les activités quotidiennes et dans la planification à long terme. »
>
> **– Stephen Adams,directeur général, Cushman Wakefield Asset Services**

Les bases

Dans le cadre de ce niveau, vous devrez évaluer et comprendre les responsabilités ainsi que les risques particuliers associés à votre immeuble et dresser une liste des sources potentielles de risques.

- Qui est responsable de la cybersécurité opérationnelle? Cette personne connaît-elle les menaces qui pourraient se propager par l'entremise de l'IIoT?
- Si applicable, veuillez vous assurer que tout le personnel des sièges sociaux connaît bien les politiques applicables.
- Examinez tous les systèmes de l'immeuble, majeurs et mineurs. Définissez ceux qui sont connectés à Internet et ceux qui servent à recueillir des données de toute sorte.
  - Pour les systèmes qui sont connectés à Internet :
    - > Des mesures de sécurité cybernétique ont-elles été établies pour protéger les systèmes, comme des mesures de sécurité relatives aux points d'accès, des pare-feu, des antivirus et des anti-maliciels? Sont-ils bien protégés?
    - > Existe-t-il des façons de protéger davantage ces systèmes ou bien de séparer tous les systèmes réseau?
  - Si des données sont recueillies :
    - > Quels types de données les systèmes recueillent-ils? Des renseignements? Des photos?
    - > Classez les données et déterminez celles qui sont essentielles et confidentielles.
    - > Trouvez où les données sont stockées.

Ce guide de haut niveau conçu pour ces trois sous-niveaux a été adapté d'un document du Center for Internet Security.

> Qui est le propriétaire des données et qui d'autre peut y accéder? Si aucun propriétaire n'a été mentionné dans les contrats signés, vous pourriez alors devoir prendre contact avec les autres partis concernés pour répondre à cette question.

> Comprenez et conservez la politique de destruction de données. Pendant combien de temps les données sont-elles stockées et de quelles manières sont-elles éliminées?

- Faites une liste des vendeurs tiers et même des vendeurs sous-traitants, y compris le personnel d'entretien, qui ont accès à votre réseau ou à vos systèmes qui sont connectés à Internet. Définissez tous les points d'accès sans fil.
- Menez une évaluation interne du personnel de votre immeuble, y compris leur conscience des risques. Vous devez entre autres vérifier que vos employés comprennent que des événements, bien qu'ils semblent être banals, comme l'apparition d'un écran noir à l'ordinateur ou bien un redémarrage du système, pourraient en fait être causés par un incident lié à la cybersécurité.
- Vos systèmes et votre matériel informatique se trouvent-ils dans un endroit sécurisé ou contrôlé?

« Vous ne pouvez pas gérer ce que vous ne mesurez pas. »

- Ken J Cowan, vice-président des programmes nationaux, Morguard Investments Limited

Cybersécurité

Outils

Il existe différents types d'outils qui permettent de protéger vos systèmes connectés au réseau contre les cybermenaces. Les types les plus fréquents sont présentés ci-dessous :

La sécurité de point terminal : Tous les dispositifs à distance, y compris les ordinateurs portables et d'autres appareils mobiles et sans fil, pouvant se connecter à distance à un réseau peuvent servir de point d'entrée pour les pirates, mettant ainsi en péril la sécurité. La sécurité de point terminal a été conçue pour sécuriser chaque point terminal du réseau qui a été créé par ces appareils. Cette sécurité s'installe par elle-même sur les appareils et peut habituellement être contrôlée de manière centralisée.

Les pare-feu : Les pare-feu réseau sont fréquemment utilisés pour empêcher les utilisateurs non autorisés d'accéder à des réseaux privés, particulièrement des intranets. Habituellement, les pare-feu comprennent deux interfaces réseau : un pour le côté externe du réseau et un autre pour le côté interne. Ils servent à contrôler ce qui est autorisé à passer d'un réseau à l'autre. Tous les messages entrants ou sortants passent par le pare-feu installé. Celui-ci les examine tous et bloque ceux qui ne respectent pas les critères de sécurité établis. Les pare-feu peuvent être incorporés au niveau matériel ou logiciel, ou aux deux niveaux à la fois. Après que des menaces ont été identifiées, ils peuvent activer entre autres un antivirus, un anti-maliciel ou bien un réseau zombie pour assurer la protection du réseau.

Les antivirus : Un antivirus est généralement un logiciel qui effectue un balayage des disques durs à la recherche de virus. Lorsqu'il en détecte, il les détruit. Celui-ci peut être mis à jour à partir d'un compte pour pouvoir détecter de nouveaux types de virus.

Anti-maliciels : Les anti-maliciels sont des programmes logiciels qui ont été conçus pour identifier des logiciels malveillants (maliciels) et empêcher qu'ils infectent des systèmes informatiques ou bien des appareils électroniques. Des outils anti-maliciels permettent aussi de retirer des maliciels.

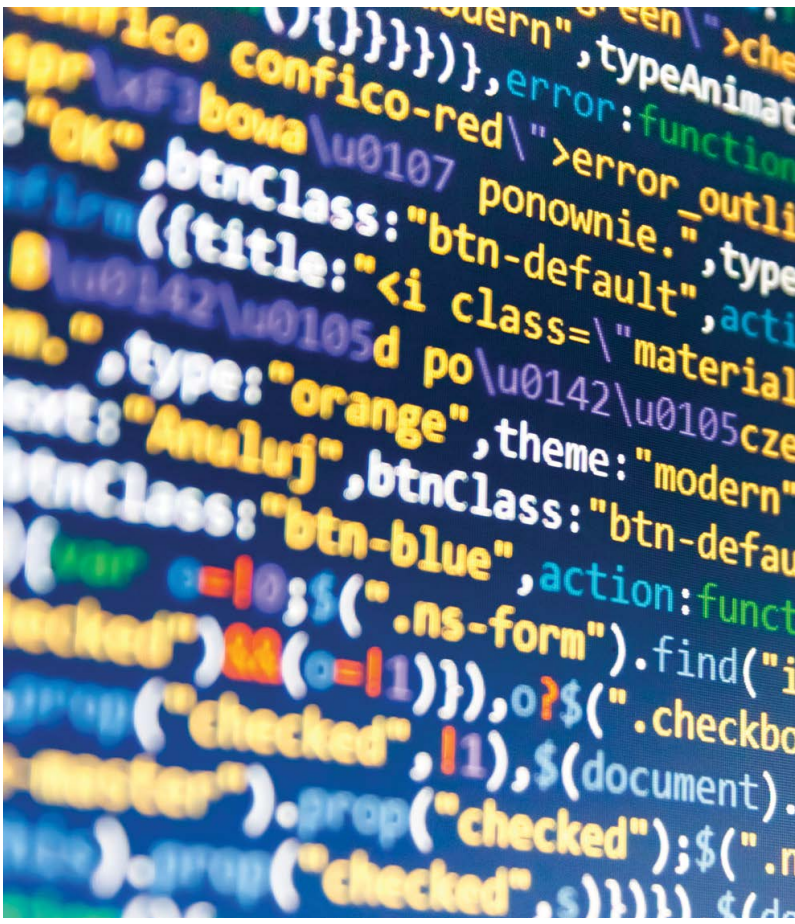
Les fondations

À cette étape, vous commencez à rassembler les ressources dont vous avez besoin pour créer un plan solide et combler certaines lacunes que vous avez trouvées au niveau de base du processus de préparation.

- Si vous avez besoin d'aide supplémentaire pour concevoir un plan de réponse et une stratégie de cybersécurité solides, pensez à engager un consultant et un spécialiste en cybersécurité qui pourraient vous guider.
- Effectuez une vérification approfondie des vendeurs tiers, entre autres en :
  - > Relisant tous les contrats signés avec les vendeurs tiers pour vérifier s'ils respectent vos politiques en matière de cybersécurité relatives aux assurances, à la confidentialité, au réseau, à l'Internet, à l'application de correctifs, etc.
  - > Travaillant avec les vendeurs pour comprendre leurs mesures de protection, s'il y a lieu, et s'ils veulent travailler avec vous pour veiller à ce que les normes soient respectées.
  - > Redéfinissant les contrats ou retravaillant les futurs contrats avec des spécialistes dans le domaine de la cybersécurité, des opérations et du droit travaillant dans ou à l'extérieur de votre organisation pour qu'ils tiennent compte des normes et des politiques minimales en matière de cybersécurité.
- Avez-vous alloué un budget réservé à la cybersécurité à l'échelle de la propriété? Si possible, envisagez d'établir un budget selon les risques et les exigences propres à votre propriété.
- Prenez connaissance de quelques normes et cadres fréquents comme les normes ISO/IEC 27000 ou bien celles de la National Institute of Standards and Technology (NIST) et du Centre for Internet Security (CIS).
- Dressez une liste fondamentale solide de tous les actifs connexes aux données et à la cybersécurité qui appartiennent et qui sont gérés par des tiers ainsi que des renseignements de base relatifs à ceux-ci qui se rapportent entre autres à la propriété, au contrôle et aux mots de passe. Conservez cette liste dans un endroit très sécuritaire pour éviter qu'elle soit volée ou piratée.
- Définissez les répercussions que tous ces systèmes peuvent causer en cas de brèche.
- Définissez et installez tous les outils et logiciels dont vous aurez besoin pour surmonter les vulnérabilités relevées.
- Créez une hiérarchie d'accès et établissez des protocoles de mots de passe.

« Tous les programmes efficaces reposent sur les efforts déployés en équipe, la pratique et l'expérience, particulièrement lorsqu'il existe un esprit de partage. De nombreuses initiatives sur la cybersécurité qui ont été déployées par des entreprises sont déjà bien amorcées. Aller au-delà de l'industrie immobilière pour parfaire ses connaissances constitue un excellent point de départ pour se lancer dans l'univers de la cybersécurité. »

- Giselle Gagnon,vice-présidente directrice, ressources stratégiques, Group Bentall Kennedy (Canada) LP



L'organisation

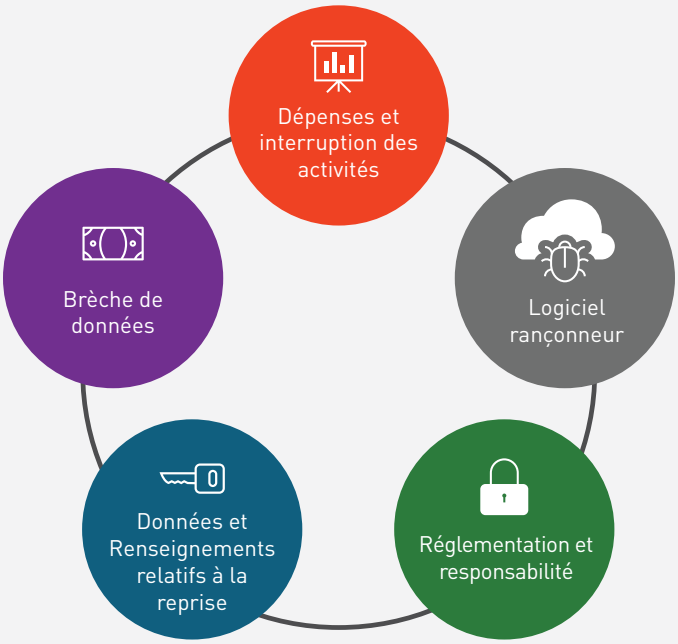
À ce niveau, vous devez créer un plan solide et vous préparer à faire face à tout incident relatif à la cybersécurité qui pourrait se produire.

- Offrez de la formation aux employés pour les aider à comprendre et à atténuer les risques liés à la cybersécurité ainsi que pour résoudre des problèmes de brèches.
- Vous pouvez aussi vous informer si votre entreprise possède une cyberassurance ou si elle envisage de mettre en place une politique d'assurance en cas de brèche, même à l'échelle de l'immeuble.
- Enfin, mettez en œuvre un plan solide au cas où il se produirait un incident, même si toutes les précautions ont été prises. Ce plan doit comprendre :
  - > Les différentes sortes de situations qui pourraient survenir.
  - > Une liste des priorités principales, comme la sécurité des personnes, les renseignements des locataires, les logiciels rançonneurs et le contrôle du système, pour pouvoir répondre à une situation de façon stratégique et s'attaquer en premier lieu aux problèmes les plus graves.
  - > Votre procédure de réponse selon la situation.
  - > Les personnes-ressources externes ou internes à alerter en cas d'urgence. Selon votre situation, celles-ci pourraient faire partie des services juridiques, des communications, de l'application de la loi et des technologies de l'information.
  - > La procédure d'escalade.
  - > Le plan de communication interne et externe, y compris les réponses à donner aux médias, si applicable.
  - > Le processus de reprise.
- Effectuez des exercices sur table et des essais de pénétration pour découvrir à quel point votre plan de cybersécurité et de réponse est robuste. L'essai de pénétration consiste à simuler une attaque pour vérifier à quel point le système est sécuritaire. Comblez toutes les lacunes définies.

Utilisation de l'intelligence artificielle pour détecter des brèches

Souvent, les organisations déploient des processus manuels pour détecter les brèches causées par des cyberattaques. Cette méthode est restreinte par le nombre d'heures de travail que les employés effectuent afin de détecter les brèches et par l'erreur humaine, mais aussi par les ressources offertes. Les employés doivent manuellement passer par les registres et les applications de cybersécurité pour entrer dans les systèmes.

L'intelligence artificielle (IA) peut grandement contribuer à détecter les cybermenaces. Elle permet de réduire considérablement les lacunes existantes dans le niveau de détection. De plus, elle peut se fonder sur les exigences propres à un bâtiment ou à une organisation. Ces systèmes d'intelligence artificielle s'exécutent de manière permanente en arrière-plan. Ils détectent et comprennent les tendances et évoluent au fur et à mesure qu'ils collectent davantage de renseignements. Toutes les entreprises peuvent désormais avoir accès à des systèmes d'intelligence artificielle pour aider à détecter des brèches. Grâce au déploiement de ces systèmes, vous pouvez vous concentrer à répondre aux menaces, au lieu d'avoir recours à une détection manuelle.



Toutes les entreprises doivent comprendre une stratégie de gestion des risques complète. Une cyberassurance pourrait être un élément central à ajouter.

Comprendre la cyberassurance

Quels éléments sont couverts par une cyberassurance?

La cyberassurance doit idéalement être adaptée en fonction d'un profil unique d'entreprise pour prendre en compte ses propres risques liés à la cybersécurité. Pour ce faire, il faut avoir recours à la technologie utilisée par l'agence pour ses activités, interagir avec les vendeurs, les fournisseurs, les clients et d'autres tiers pour connaître la façon dont ils collectent, traitent, entreposent et transmettent des renseignements confidentiels.

Cependant, habituellement, la majorité des politiques en matière de cybersécurité comprennent toute une gamme de couvertures de base pouvant être personnalisées pour inclure des couvertures supplémentaires, comme pour se protéger contre les dommages physiques ou corporels découlant d'une cyberattaque ayant affecté les systèmes opérationnels.

De plus, les titulaires de police ont souvent accès à des services connexes comme des conseils techniques, des conseillers en atténuation des risques, des outils de détection de vulnérabilité, des renseignements relatifs à la cybersécurité et une planification de réponses aux incidents.

2. Réponse et reprise

Bien que vous ayez tout fait pour éviter et atténuer les risques de cyberincidents, ceux-ci pourraient tout de même se produire. Si tel est le cas, vous devez être prêt à agir immédiatement pour minimiser ses répercussions. Tout délai ou toute inefficacité peuvent entraîner d'énormes conséquences. Dans cette phase, vous devez traiter systématiquement l'incident.

Si vous avez bien effectué la Phase I, la Phase II ainsi que la Phase III devraient se dérouler beaucoup plus rapidement et en douceur.

- Définissez les éléments qui affectent les systèmes et quels autres systèmes qui pourraient être touchés par ceux-ci.
- Revenez au plan que vous avez créé à la Phase I, et définissez toutes les priorités et la bonne stratégie de réponse à employer.
- Avisez toutes les personnes et tous les membres de l'équipe qui doivent l'être.
- Demandez au bon personnel de déconnecter ou d'isoler le système.
- Si possible, passez en mode « opération manuelle ».
- D'abord, déployez des efforts pour assurer la sécurité des personnes si celle-ci est compromise.
- Selon le plan que vous avez créé à la phase précédente, au besoin, prenez contact avec les membres des équipes à l'interne où à l'externe des services juridiques et d'assurances ou des communications nécessaires.

3. Compte-rendu et combler les lacunes

Après que la menace immédiate a été contenue et que le processus de reprise est en cours, il est désormais temps de penser à ce qui a bien été tout comme ce qui a mal tourné pour que ces éléments soient pris en compte dans les prochains plans.

- Rassemblez les membres de l'équipe de réponse et tentez de trouver la raison pour laquelle il s'est produit une brèche.
- S'il existe des lacunes dans votre planification, comblez-les et solidifiez votre plan pour éviter que d'autres brèches similaires surviennent.
- Analysez toutes les lacunes, et si nécessaire, investissez pour les résoudre.
- Évaluez la façon dont vous avez répondu à l'incident pour voir si vous pouvez vous améliorer si d'autres problèmes surviennent dans le futur.
- Inscrivez les leçons apprises et partagez-les à tous les partis pertinents.

Conclusion

Bien que le processus de création d'un plan de cybersécurité pour votre immeuble puisse s'avérer décourageant, vous devez impérativement vous adapter à la réalité d'aujourd'hui et réduire vos risques d'être victime de cyberattaques.

Il est très important de gérer les risques liés à la cybersécurité à l'échelle de l'immeuble, car ceux-ci peuvent affecter la compétitivité de votre propriété sur le marché. C'est pourquoi beaucoup d'éléments doivent être couverts, par exemple, en allant chercher les bonnes personnes pour vous aider, en suivant des formations appropriées et en vous assurant. Plus vous commencez tôt à vous préparer, plus vous avez de chance d'atténuer ces menaces et d'être bien préparé à y faire face.

Ce guide a été conçu pour vous aider à commencer, à bien penser aux étapes à suivre et à servir de liste de vérification pour votre immeuble. En faisant preuve de diligence, en utilisant la bonne approche et en ayant recours à l'aide appropriée, vous pouvez avoir des systèmes plus sécuritaires et plus résistants ainsi qu'un plan de réponse efficace.

Lectures

LPRPDE : https://www.priv.gc.ca/en/privacy-topics/privacy-laws-in-canada/the-personal-information-protection-and-electronic-documents-act-pipeda/

RGPD : https://www.eugdpr.org/

NIST: https://www.nist.gov/

Échange canadien de menaces cybernétiques (ECMC) : https://cctx.ca/

ISO/IEC 27000 : https://www.iso.org/isoiec-27001-information-security.html

CIS Center for Internet Security®: https://www.cisecurity.org/

Remerciements

Nous sommes très reconnaissants envers le soutien financier de MNP LLP, de CAPREIT et de QuadReal, et pour l'expertise fournie par MNP LLP et MARSH.

Nos contributeurs, qui ont partagé leurs perceptions et ont investi du temps précieux pour concevoir ce guide :

Stephen Adams
Directeur général
Cushman Wakefield Asset Services

Ken J. Cowan
Vice-président des programmes nationaux à Morguard Investments Limited

Randal Froebelius
Président et directeur général de Equity ICI Real Estate Services Inc.

Giselle Gagnon
Vice-présidente directrice, ressources stratégiques, Group Bentall Kennedy (Canada) LP

Cheryl Gray
Vice-présidente directrice, innovation des entreprises, QuadReal Property Group

David Sulston
Directeur, Security Oxford Properties Group

Sonny Thind
Vice-président des technologies de l'information à QuadReal Property Group

Danny Timmins
Dirigeant national, cybersécurité, MNP

Lee Thiessen
Dirigeant national, service immobilier, MNP LLP

Lachlan MacQuarrie
Vice-président des programmes nationaux à Oxford Properties Group

Terry Chowanec
Vice-président des opérations de sécurité nationale à Cadillac Fairvview

Trevor Cleveland
Directeur des opérations à Colliers International

Gregory Eskins
Chef de la sécurité nationale et des pratiques en matière de cybersécurité du service immobilier de MARSH

Sue Klinner
Vice-présidente, processus commerciaux et gestion des risques à Firset Capital Realty

Aaron Pais
DPI, Morguard Investments

Bob Riddell
Directeur, sécurité et sécurité des personnes à Ivanhoe Cambridge

Jonathan Fleischer
Premier vice-président des opérations, Capreit

Senad Cehajic
Directeur de la continuité des activités à Ivanhoe Cambridge

Gabriel Hebert
Directeur des technologies de l'information à Ivanhoe Cambridge

Kristy Kent
Vice-présidente directrice, MARSH

Michael Chin
Vice-président des technologies de l'information à Triovest

Kendall Peart
Directice générale de l'immobilier à MARSH

Scot Adams
Vice-président national des services à Colliers International

Brian Claman
Directeur de la sécurité nationale et des services de la sécurité des personnes à GWLRA

Michele Walkau
Vice-présidente directrice des services corporatifs et responsable de favoriser l'excellence à GWLRA

Naveli Thomas
Directrice à Nyox

Michael di Grappa
Vice-président directeur de la gestion immobilière à Canderel

Robert Gordon
Directeur administratif, Échange canadien de menaces cybernétiques

L'équipe de BOMA Canada

Benjamin Shinewald
président et directeur général de BOMA Canada

Michael Parker
Consultant en marketing et en communications de BOMA Canada

Le personnel de BOMA Canada regrette sincèrement les erreurs ou les omissions mentionnées dans la liste ci-dessus et souhaite remercier tous nos bénévoles et collaborateurs pour leur soutien.

Ce rapport est disponible en anglais.

BOMA Canada
www.bomacanada.ca