BOMA Canada

BOMA Canada

2019 Cyber Wellness Guide

Addressing cyber risks in commercial real estate building operations

This Guide is Sponsored by:

MNP LLP QuadReal CAPREIT

We are proud to present this cyber wellness guide—a tool to help building owners and managers start thinking of their cyber security journey.

Dear friends,

Cyber security threats have been expanding in both frequency and types of breaches over the years. Companies have correspondingly responded with measures to protect their information and their corporate systems. Threats exist for building operations too, and like corporate systems need be taken more seriously due to the ramifications that can be extensive around data loss, human safety, competitiveness and reputation.

To create more awareness of these risks and help you understand how you can be prepared at the building level before any incident occurs, we have created this wellness guide. Cyber security is often a complex and technical subject, but we have tried to tailor it to the industry's current state of preparedness, and we have drawn on a variety of ideas and sources.

Who should read this?

This guide is primarily geared towards introducing the concept of cyber security planning for managers and operational leaders of real estate. We believe that anyone who works in or manages commercial and institutional building operations directly or indirectly, or has exposure to internet-connected systems would find it valuable.

How should this guide be used?

This guide is intended as an introduction to understanding cyber security risks facing the commercial real estate industry. It contains a cyber security checklist for buildings as general guidance only. It is not a complete strategy or standard on its own, and needs to be supplemented with further reading and adherence to specific standards or the help of professionals, to create robust mitigation plans.

We hope you find our Cyber Wellness Guide useful, and that it can get you started on your journey to protect your building operations from cyber threats. We aim to keep it up-to-date with regular editions, since cyber risks and regulations keep evolving.

Sincerely,

Benjamin Shinewald
President & CEO,
BOMA Canada

Lee Thiessen
National Leader, Real Estate
MNP

Cheryl Gray
EVP, Enterprise Innovation
QuadReal Property Group

Copyright

The Building Owners and Managers Association (BOMA) of Canada owns the trademark on the cover of this document. Use or reproduction of this trademark is prohibited for any purpose (except as part of an accurate reproduction of the entire document) unless written permission is first obtained. This document is subject to copyright protection. However, this document may be reproduced free of charge in any format or media without requiring specific permission, with the exception of its reproduction in whole or in part, in any media or format that is wholly or partially for the purpose of commercial gain. This permission is subject to the material being reproduced accurately and not being used in a derogatory manner or in a misleading context. If the material is being published or issued to others, the source and copyright status must be acknowledged. The permission to reproduce copyright protected material does not extend to any material in this document that is identified as being the copyright of a third party. Authorization to reproduce such materials must be obtained directly from the copyright holders concerned.

Disclaimer of Any Legal Liability

By reading this guide you hereby agree to abide, without restriction or limitation of any kind whatsoever, by the terms of this disclaimer.

The Building Owners and Managers Association of Canada, including all of its officers, directors, employees, advisors, consultants, committee members, task force members, agents, volunteers and members (hereinafter collectively referred to as "BOMA") has assembled the material in this document for the purpose of canvassing potential practices in dealing with the potential for a cyber security incident. The information presented is solely and without exception, express or implied, for that purpose. BOMA makes no express or implied representations, warranties, guarantees, or promises, that the information presented is current or accurate at any point in time, be it presently, previously, or at any time in the future. The information in these documents is not meant in any way to advocate, promote, or suggest any preferred method or methods for dealing with a cyber security incident. Should the user confront any such incident, the users should seek professional assistance. Any legal, financial, emergency, management, development, structural design, security or commercial issue whatsoever should be referred to a qualified professional who can properly assess any risks inherent in following any plan to address a given issue. The information provided is not a substitute for consulting with an experienced and qualified professional.

BOMA, its partners and affiliates or related organizations make no implied or express representation or warranty that the information contained herein is without risk. Furthermore, absolutely none of these parties accept any responsibility or liability for any acts or omissions done or omitted in reliance, in whole or in part, on this written report or any of its contents or inferences. The same parties disclaim all responsibility or liability to any person, whether in contract, equity, tort, statute, or law of any kind, for any direct or indirect losses, illness or injury, or damage, be it general, incidental, consequential or punitive or any other kind of damage, relating to the use of this Guide.

The information in these documents is not intended to cover every situation. Details which may be relevant to a user's particular circumstances may have been omitted. Users are advised to seek professional advice before applying any information contained in this document to their own particular circumstances. Users should always obtain appropriate professional advice on security, legal, structural, organizational, personal, proprietary, public health, professional or any other issues involved.

The information is presented "as is." This Guide or any part thereof, including without limitation, any appendices or related toolkits and/or resources, is not intended in any way, and is hereby expressly denied, to create any relationship of any kind whatsoever or any duty of care between BOMA (or any of the persons or parties included in BOMA as defined) and any other person or entity including without limiting the generality of the foregoing any person or entity that may read, review, use or become aware of this guide or any part thereof (collectively referred to as the "user" throughout this disclaimer). The user also acknowledges that no such relationship is created between it and the parties associated with this document's development, production or dissemination. The user also further acknowledges that this disclaimer prevents any possible duty of care owed by BOMA to the user from ever arising, either by rule of law, equity, or statute whatsoever including any obligation to keep this information current, validate it, ensure its accuracy, or update it in any way and that the use of this guide in whole or in part, cannot form the basis for any possible legal claims or proceedings whatsoever as against BOMA.

Introduction

Today, internet-connected or smart systems are helping operations and increasing efficiency within commercial real estate (CRE). From making elevator systems more efficient to monitoring and optimizing HVAC performance, they have found their value in buildings. Yet, they haven't come without risks.

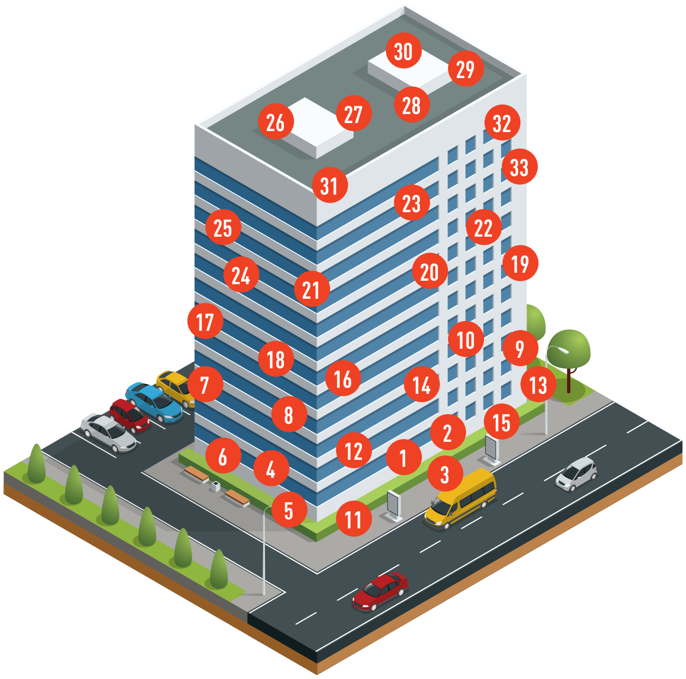
Hacking, malware and other cyber security challenges affect information systems in buildings. Are you geared up to detect and respond to these threats? Now that smart buildings and smart devices in buildings are growing, cyber security incidents at a building could have a significant impact on the property and its operations.

These commercial smart systems, which we refer to as the Industrial Internet of Things (IIoT), are often collecting a lot of data at the back end, and are connected to the internet, sometimes with the knowledge of building operators and managers, but sometimes without. These systems are at risk, like any computer in any office, and even more so since the same rigor for cyber security often hasn't been applied to these systems yet and awareness of these risks is lower.

The IIoT currently in the market are geared towards user value, and haven't necessarily been looked at from a thorough cyber security perspective. That increases the onus on building managers to have a robust plan to prevent and deal with cyber issues.

In addition to the expanding network of smart devices, attackers are also becoming more persistent and patient, whether it is to gain ransom from you or to cause other damage. In addition to local hackers who may use phishing attacks or ransomware to cause potential damage, there are international threats too as proximity does not matter when dealing with cyber risks, and no sector is immune.

Smart systems have expanded, increasing the cyber risk universe



1 Automated Doors
2 Card Readers
3 Access Management Controlers
4 Chemical Water Control
5 Chillers & Boilers
6 Pumps
7 Computer Room Air Handlers
8 Operator Station
9 Fire Alarm Panels
10 Rack/Server IDF > PDU
11 Garage Access
12 Thermostats / Humidistats
13 Water Systems
14 Vending Machines
15 Electric, Gas, Heating
16 Cameras
17 Diffusers
18 VAV Units
19 Halon System
20 Heating Units
21 Lighting
22 Zone Control Panels
23 Elevators
24 Cooling Towers
25 Smoke Detectors
26 Solar Panels
27 Exhaust Fans
28 Fans
29 Cooling Coils
30 Air Handling Controllers
31 Air Filters
32 Indoor Air Quality Services
33 Dampers

The pace of change and adoption of the IIoT is rapid, and with that the risk landscape is also expanding at an accelerated rate. It is imperative for commercial buildings to develop a cyber security program that accounts for this new normal as a protective measure.

With a lack of frameworks geared specifically towards operational cyber security at the property level, we have created this wellness guide to help you through the process.

> “As the commercial real estate industry is increasingly adopting technology into operations, awareness around cyber security risk is an important issue for our industry. This guide is intended to help property managers develop mitigation strategies to address cyber security risk at the property level.”
>
> **– Cheryl Gray, EVP of Enterprise Innovation, QuadReal Property Group**

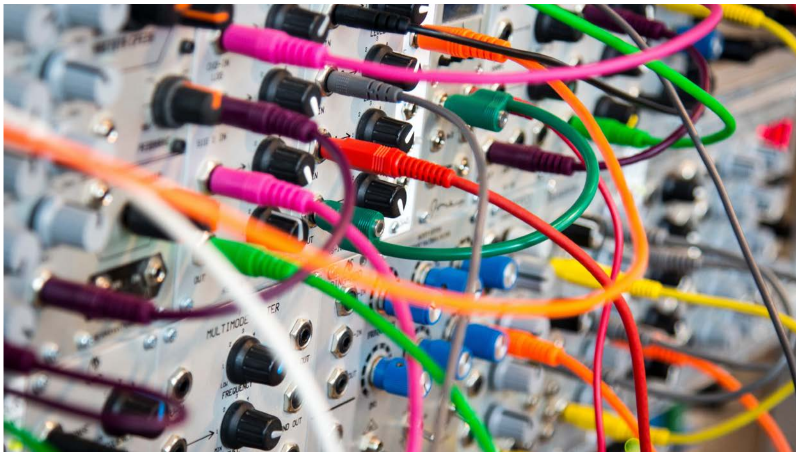
The impact on your organization

Any malicious incident at a building level can have an impact, ranging from minor to disastrous. If control over any system is lost to an attack, there can be risk safety of people and damage of property, or you could be held to monetary ransom (and even if you pay, you may not be released by your hackers). Smart systems can also provide an entry into data systems at the building or corporate offices, leaving information from both individuals and companies open to misuse.

Cyber security incidents at your building can pose many risks:

- Safety of people, through external control of systems
- Reputation loss, if data is breached or service is not delivered due to system failures
- Trust of tenants or consumers, and a resultant impact on revenue
- Liability for data of people or organizations being misused
- Legal action and associated costs
- Breach resolution costs
- Vendor costs to get systems back up
- Damage to property and related costs

There have been major incidents around the world related to cyber security, causing significant cost and impact. They have come through different channels including unintended malware from vendors. The 2018 Cost of Data Breach Study by Ponemon puts the global average cost at US$3.86 million, or US$148 per data record. That’s a 6.4% increase in the average cost since 2017. Every incident may not be major, but every incident does have an impact.



Scenarios: Bringing the risks to life

To help explain the risks better, we consider three actual scenarios drawn directly from real world incidents.

Scenario 1: Using data for extortion

An individual at ABC company received what appeared to be a standard PDF invoice by email from a trusted third-party supplier. This file however was malicious and simply disguised as an invoice by attackers. Once the payment was executed, the attackers gained access to the user's machine. Local administrative credentials and user credentials were then harvested and used within the network environment. Since all backups were online and accessible, the attackers deleted all active backups and disabled the system.

A subsequent ransomware and file encryption campaign began at 3:00 a.m. on a Saturday evening and affected every single workstation and server in the environment. The IT provider was brought in to troubleshoot the issue only after the staff could no longer gain access.

Unfortunately, upon review, file and system image restoration was not possible due to lack of backups. A ransom screen appeared on all the workstations and servers and indicated that the entire organization had been compromised. The company panicked since they did not have an incident response plan, and reached out to a local cyber security firm for help. The organization would have to pay a six-figure ransom in order to get key systems back online so that their services would not grind to a halt. The cost and loss in business was severe, and now the company is developing better safeguards, creating an incident response plan and conducting user training on cyber security.

Scenario 2: Breach of information through an HVAC contractor

A major retailer faced a large-scale breach. When a third-party HVAC vendor plugged in his system at one of their retail locations to deal with routine maintenance work, hackers, who had gained access to his system, were then able to gain access to the retailer's systems.

Without adequate separation of network systems and information at the retailer, they were able to extend their access into the payment systems where card information of customers was stored. The retailer was not able to detect the breach and hence could not respond to it, until millions of people's credit cards and information were compromised.

Multiple levels of failures occurred, including the level of access allowed to individuals and vendors, lack of separation between the different systems and segregation of critical information, and an inability to adequately detect or escalate unusual patterns.

After facing lawsuits, it has been widely reported that the retailer paid settlements in excess of US$18 million. This excludes their costs for litigation, curtailing the damage and recovery, not to mention loss of reputation and trust, which is estimated to have cost the retailer in excess of a hundred million dollars.

> “
> a third-party HVAC vendor plugged in his system at one of their retail locations, hackers, who had gained access to his system, were then able to gain access to the retailer's systems.”

Scenario 3: Breach of Building Systems, Compromising Safety

A hacker discovered a vulnerability in a public facing web server, and used their tools to exploit the vulnerability. Once the attacker gained a foothold in the environment, they then discovered additional file servers, building operation systems and much more.

The hacker stumbled upon an industrial control system which was used to exhaust the parking garage. It had just been automated and the hacker was able to shut down the exhaust system. They then emailed the business to ask for an undisclosed sum of bitcoins to turn on the exhaust fans. Once notified of this ransom demand, the business tried to login into the system directly only to discover that they couldn't get in because the attackers had changed the passwords.

They called their exhaust system provider and cyber security firm, who had an offline backup to restore the system and address the denial of service that was caused. Once the immediate threat was neutralized, the next challenge was to figure out what other systems and backdoors this attacker had access to.

The cyber security firm performed an investigation and security scans to find additional weaknesses within the organization and found a few which were immediately remediated. Since the organization had prepared itself, it was able to control the access and remedy the situation without any significant damage. By being prepared, they were able to limit their exposure.

These are real life examples and can occur within and the real estate industry at any location. And because the problem isn't a malfunctioning of the system itself, but breached controls, your staff and even your vendors can find it hard to diagnose the issue and get systems back under control.

Evolving regulation around privacy

With growing public and shareholder concerns, boards of public companies are asking for more cyber reporting, as are insurance companies.

Regulatory requirements around privacy of personally identifiable information (PII) also exist and are developing here in Canada. These requirements will affect your buildings if you are storing information on your clients, tenants, staff etc. It is prudent to understand the risks around how a breach of privacy can affect your building.

Canada is soon implementing mandatory reporting of breaches under the Personal Information Protection and Electronic Documents Act (PIPEDA), with corresponding new record-keeping requirements. The European Union's General Data Protection Regulation (GDPR) has implications for organizations around the world, and it is likely that other countries will soon catch up with their own version of the requirements.

With increasing regulatory and privacy requirements, your property could be required to comply. By being prepared, you can mitigate cyber security risks and even get ahead of any requirements that come your way. Although beyond the scope of this document, we recommend staying abreast of all the regulatory changes and adjusting your cyber maintenance practices accordingly.

> “
> Canada is soon implementing mandatory reporting of breaches under the Personal Information Protection and Electronic Documents Act (PIPEDA), with corresponding new record-keeping requirements.”

Being prepared: A checklist

We understand that your specific building or group of buildings may be unique, and each property is managed differently. Instead of providing a prescriptive one-size-fits-all recommendation, we have created a checklist for you to work through in order to assess, and then address, the most common building-operations cyber vulnerabilities.

A general approach to dealing with any risk is to look at it in three phases: preparing, responding and debriefing. This checklist is also divided into these phases.

> “A cyber incident involving IoT is no longer ‘unforeseeable’. Although the industry can’t stop all cyber risks, what may be more defensible is your company’s planning and dedication to mitigate the various inherent risks in this area.“
>
> **– David Sulston, Director of Security, Oxford Properties Group**

1 Prepare › **2 Respond** › **3 Debrief**

1. Prepare

Attackers today look patiently for a weak link in your entire supply chain. Whether it is through your property operations network, or an extended vendor, they can find an entry point and cause damage. Making it difficult and expensive for them to do so requires effort and preparation, but acts as a major deterrent.

The preparation phase is for you to take proactive steps to avoid an incident, and also be ready to deal with any issue that still may come your way. This phase is the most time consuming, but it's critical to be thorough and get it right. A robust first phase will arm you with the right safeguards and plans. We have divided this phase into three levels—basic, foundational and organizational —so you can get through it systematically, and identify which level you are currently at.

> "With the emergence and deployment of data analytics, IoT, and AI creating benefits to industry and communities, new demands will be placed on the cyber protection capabilities of every organization. These new demands will require new proactive strategies to protect against malicious behavior both in day to day operations and long-term planning."
>
> **– Stephen Adams, General Manager,**
> **Cushman Wakefield Asset Services**

Basic

This level is about assessing and understanding responsibility and the particular risks in your building, and listing the potential sources of the risks.

- Who has responsibility for operational cyber security? Are they aware of the expanded threats through the IoT?
- If applicable, check at the corporate headquarters for any policies you need to be aware of.
- Take stock of all building systems, both major and minor. Identify which ones are connected to the internet and/or are collecting data of any type.
- Of the systems connected to the internet:
  - > Do the systems have cyber security measures such as end point security, firewalls, anti-viruses and anti-malware built in? Are they adequately protected?
  - > Are there available ways to further protect these systems or be able to segregate all network systems?
- If any data is being collected:
  - > What data is being collected— information and/or pictures?
  - > Classify the data and determine the critical and sensitive data.
  - > Identify where data is stored.

The high-level guidance for these three sub-levels has been adapted from the Center for Internet Security.

  - Who owns the data and who else has access to it? If there is no mention in contracts that have been signed, you may need to reach out to the parties involved to resolve the matter.
  - Understand and record the data destruction policy. How long is the data being stored for and how is it purged?
- Make a list of third-party vendors and even sub-contracted vendors, including maintenance staff, who have access to your network or systems connected to the internet. Identify all points of remote access.
- Conduct an internal assessment of your building staff, including their awareness of risks. This includes testing for employees' understanding that seemingly mundane occurrences such as blank screens or system reboots may be due to a cyber security incident.
- Are your systems and your hardware in a secured or access-controlled area?

> "You can't manage what you're not measuring."
>
> **- Ken J Cowan, Vice President National Programs, Morguard Investments Limited**

Cyber Security Tools

There are many different types of tools protecting network-connected systems from cyber threats. The most common types are explored below:

Endpoint security: Each remote device, including laptops and other wireless and mobile devices, with a remote connection to the network creates a potential entry point for security threats. Endpoint security is designed to secure each endpoint on the network created by these devices, and is installed on the devices themselves, and typically controlled centrally.

Firewalls: Network firewalls are frequently used to prevent unauthorized users from accessing private networks, especially intranets. Generally, the firewall has two network interfaces: one for the external side of the network, one for the internal side. Its purpose is to control what traffic is allowed to traverse from one side to the other. All messages entering or leaving pass through the firewall, which examines each message and blocks those that do not meet the specified security criteria. Firewalls can be implemented as both hardware and software, or a combination of both. They could, after threats are identified, turn on anti-virus, anti-malware/anti-bot etc for protection.

Anti-virus: An anti-virus is typically software that searches hard disks for viruses and removes any that are detected. They can be updated to account for new types of viruses.

Anti-malware: Anti-malware are software programs designed to identify and prevent malicious software (malware), from infecting computer systems or electronic devices. Anti-malware tools can also include malware removal capabilities.

Foundational

In this level, you start getting together the resources you need to create a robust plan and addressing some of the gaps you found at the Basic level of preparedness.

- If you find that you need more informed assistance to create a robust cyber security strategy and response plan, evaluate hiring a consultant and cyber security specialist, who can guide you.
- Do a thorough third-party vendor check including:
  - > Go over all third-party vendor contracts to understand if those contracts meet your cyber security policies for insurance, privacy, network, internet, patching etc.
  - > Work with the vendors to understand their safeguards, if any, and whether they are willing to work with you to ensure standards are met.
  - > Re-draw contracts or re-work future contracts with legal, operational and cyber experts within or outside your organization to require minimum standards and cyber security policies.
- Do you have a cyber security budget at the property level? Consider having budget allocated based on your property's specific risks and requirements, if possible.
- Read up on some common standards and frameworks such as ISO/IEC 27000 or those provided by National Institute of Standards and Technology (NIST) or Centre for Internet Security (CIS).
- Create a robust master list of all the possible cyber and data assets, both owned and third-party managed, basic information on each such as ownership, control and passwords, and store this in a highly secure manner to avoid hacking or theft.
- Map the level of impact all these systems can have if they are breached.
- Identify and install all software or tools you need to overcome identified vulnerabilities.
- Create an access hierarchy and establish password protocols.

> "All successful programs rely on team, practice and experience—particularly when they are shared. Many corporate cyber initiatives are well underway, and reaching out beyond the property industry to advance knowledge is a great starting point on the property cyber security journey."
>
> **- Giselle Gagnon, SVP Strategic Resources Group, Bentall Kennedy (Canada) LP**

- Create backups that are recent.
- Review the existing and upcoming privacy legislation regarding gathering information and disclosing breaches in case of an incident.
- How will you detect these breaches? Often, manual checks are not robust or 24/7, especially for system breaches. Are there existing artificial intelligence (AI) systems to help you detect incidents? Which one may be right for you?

Organizational

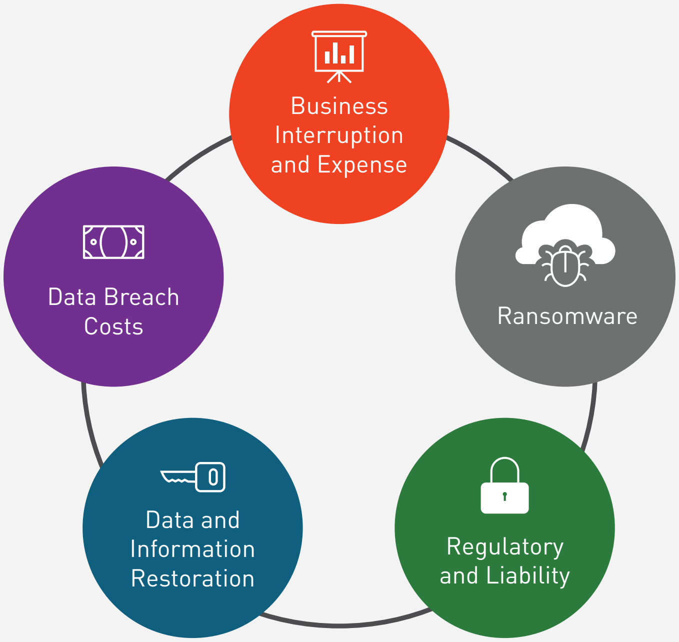
In this level, you create a robust plan and get ready to deal with any cyber security incidents that may occur.

- Conduct training to help staff understand and minimize cyber risks, and deal with breaches.
- You could explore whether your company has cyber insurance or is exploring a policy on having insurance in place for any breach that may occur, even at the building level.
- Finally, have a robust plan ready in case of an incident which may occur despite precautions. This plan should include:
  - > The different types of situations that may arise.
  - > A list of top priorities, such as life safety, tenant information, ransomware, system control etc., to be able to respond to a situation strategically and deal with the most critical issues first.
  - > Your response procedure based on the situation.
  - > The internal or external people who need to be informed and involved, which could include legal, communications, law enforcement and IT amongst others based on your specific situation.
  - > Escalation procedure.
  - > Internal and external communications plan including media responses if applicable.
  - > Recovery process.
- Conduct table top exercises and penetration testing to understand how robust your cyber security plan and response is. Penetration testing is a simulated attack to check how secure the system is. Address all identified gaps.

Artificial Intelligence in Detecting Breaches

Often, organizations deploy manual processes to detect cyber breaches. This method is restricted by the hours staff is working on detection, human error and also the resources available. Employees have to manually work through logs or cyber security applications to get into systems.

Cyber threat detection is an area in which artificial intelligence (AI) can have a significant impact. It reduces the level of detection shortcomings very significantly, and can be based on each individual building or organization's unique requirements. These AI systems run in the background continuously, detecting and understanding patterns, and evolving as they gather more information. AI to aid cyber breach detection is now available to companies, and with the deployment of these systems, you can focus your resources on responding to threats, rather than on manual detection.


Business Interruption and Expense
Ransomware
Regulatory and Liability
Data and Information Restoration
Data Breach Costs

Every company should have a comprehensive cyber risk management strategy, and cyber insurance may be a core component.

Understanding Cyber Insurance

What does Cyber Insurance Cover?

Cyber insurance should ideally be tailored to the unique cyber risk profile of an individual organization, which is shaped by: the firm's use of technology in its operations; interactions with vendors, suppliers, customers, and other third parties; and how it collects, handles, stores, and transmits confidential information.

Generally, however, most cyber policies will include a range of basic coverages and can be tailored to include additional coverages, such as physical damage or bodily injury resulting from a cyber event impacting operational systems.

In addition, policyholders can often access related services like technical advice and risk mitigation counsel; vulnerability detection tools; and cyber education and incident response planning.

2. Respond and recover

Despite your best efforts and mitigation, you still may face cyber security incidents. In such an event, you have to be ready to act immediately to minimize its impact. Any delays or inefficiencies can have significant repercussions. In this phase, you deal with the incident systematically. If you have Phase I worked out, Phase II (and Phase III) should become significantly faster and smoother.

- Identify what systems are affected and what other systems it could cascade to.
- Circle back to the plan you created in Phase I, and identify all priorities and the right response strategy.
- Inform all the people and teams that need to know.
- Have the right staff disconnect or isolate the system.
- Switch to operating manually if possible.
- Work towards life safety first if that is a concern.
- If there are any communications, legal and/or insurance teams—internal or external—that you need to liaise with based on the plan you created in the earlier phase, reach out to them as required.

3. Debrief and close gaps

After the immediate threat has been contained and recovery is in progress, it is now time to take stock of what went well, as well as what went wrong so it can be addressed in future plans.

- Gather the response team and evaluate why the breach occurred.
- If there were any gaps in your planning, address those and make your plan more robust to prevent any similar breaches.
- Assess any gaps and invest in those if necessary.
- Assess your response to the incident to see if you can improve upon it, in case of any future issues.
- Capture and communicate the lessons learned to all relevant parties.

Conclusion

While the process of creating a cyber security plan for your building may seem daunting, it is necessary to deal with today's reality and lower your risks.

Managing cyber security risks at the building level is increasingly important, and can affect your property's competitiveness in the marketplace. That's why, from having a robust plan to getting the right help, training and insurance, a lot of ground needs to be covered. The sooner you start, the more chance you have of mitigating these threats and being prepared.

This guide is meant to help you get started, think through the steps involved and serve as a checklist for your property. With the right diligence, approach and help, you can have more secure and resilient systems and an effective response plan.

Further reading

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

GDPR: https://www.eugdpr.org/

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

Canadian Cyber Threat Exchange (CCTX): https://cctx.ca/

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

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

Acknowledgements

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

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

Stephen Adams
General Manager
Cushman Wakefield Asset Services

Ken J. Cowan
Vice President National Programs
Morguard Investments Limited

Randal Froebelius
President & General Manager
Equity ICI Real Estate Services Inc.

Giselle Gagnon
SVP Strategic Resources Group
Bentall Kennedy (Canada) LP

Cheryl Gray
EVP, Enterprise Innovation
QuadReal Property Group

David Sulston
Director, Security
Oxford Properties Group

Sonny Thind
Vice President, Information Technology
QuadReal Property Group

Danny Timmins
National Leader, Cyber Security
MNP

Lee Thiessen
National Leader, Real Estate
MNP LLP

Lachlan MacQuarrie
VP National Programs
Oxford Properties Group

Terry Chowanec
VP National Security Operations
Cadillac Fairvview

Trevor Cleveland
Director, Operations
Colliers International

Gregory Eskins
National Security and Cyber Practice Leader
MARSH Real Estate

Sue Klinner
Vice President, Business Processes & Risk Management
First Capital Realty

Aaron Pais
CIO
Morguard Investments

Bob Riddell
Director, Security and Life Safety Security
Ivanhoe Cambridge

Jonathan Fleischer
EVP, Operations
Capreit

Senad Cehajic
Director, Business Continuity
Ivanhoe Cambridge

Gabriel Hebert
Director, IT
Ivanhoe Cambridge

Kristy Kent
Sr. Vice President
MARSH

Michael Chin
VP, Information Technology
Triovest

Kendall Peart
Managing Director
MARSH Real Estate

Scot Adams
VP National Services
Colliers International

Brian Claman
Director of National Security and Life Safety Services
GWLRA

Michele Walkau
SVP of Corporate Services and Building Excellence
GWLRA

Naveli Thomas
Director
Nyox

Michael di Grappa
SVP, Property Management
Canderel

Robert Gordon
Executive Director
Canadian Cyber Threat Exchange

BOMA Canada team:

Benjamin Shinewald
President & CEO
BOMA Canada

Michael Parker
Marketing and Communications Consultant
BOMA Canada

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

Ce rapport est disponible en français.

BOMA Canada
www.bomacanada.ca