BOMA Canada

2020 Cyber Wellness Guide

Embedding cybersecurity in procurement

This Guide is Sponsored by:

MNP LLP QuadReal Genetec Morguard

We are proud to present this procurement cybersecurity guide, intended to help building owners and managers with their cybersecurity journey as it relates to third-party vendors.

Dear friends,

BOMA Canada has been focused on providing ongoing education and valuable tools to its members through its knowledge series. With Internet-connected and smart systems within commercial and residential buildings causing a corresponding increase in cybersecurity risks, one of the key areas of focus for us is cybersecurity.

Our BOMA Canada 2019 Cyber Wellness Guide introduced cybersecurity threats and provided a starting point for buildings' overall cybersecurity journey. Since a large proportion of incidents and breaches originate from third-party vendors, in this guide we delve deeper specifically into managing cybersecurity risks through procurement and contracting practices.

How should this guide be used?

This guide is intended to introduce building managers and owners to embedding cybersecurity practices with their third-party vendors, and provides a checklist as guidance. It is best used in conjunction with overall cybersecurity planning, and follows the structure of our Cyber Wellness Guide so that readers can link dependent decisions about how they perceive, identify, strategize and buy cybersecurity solutions.

While specific stages of the cybersecurity journey in this guide may be differently named or grouped, the overall stages covered largely follow the structure of commonly used standards. However, this guide 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.

An executive summary is included for quick and easy reference. We hope you find this guide useful, and we welcome your suggestions on how we can further provide cybersecurity guidance for your buildings.

Sincerely,

Benjamin Shinewald
President & CEO,
BOMA Canada

BOMA Canada

Copyright

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 cybersecurity 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 cybersecurity 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.

Executive Summary

Adoption of smart systems and the Internet of Things (IoT) in buildings have increased cybersecurity risks, and breaches often originate from third-party vendors and sub-vendors, who have access to your internet or data. Embedding cybersecurity in your supply chain is critical as part of your overall cybersecurity journey.

Cybersecurity through Procurement

I. Prepare: Identify, Protect and Detect

This is the most time consuming stage, but critical to get right in order to reduce your cybersecurity risks. It has four critical components:

1. **Map your supply chain**

- Create an inventory of all buildings systems, vendors and sub-vendors, and identify all points of direct, indirect, onsite and remote access to your network, internet or data. Identify how each login and access is being logged.
- Categorize and assign priority to vendors based on their connectivity to sensitive systems and data.
- If any data is being collected by vendors, identify ownership of the data, where it is stored, how it is purged and who has access.

2. **Assess your Supply Chain**

- Establish an evaluation framework to assess current and new vendors, which should include level of risk, contractual terms, insurances and ability to log activities and create backups.
- Conduct thorough third-party vendor checks covering contracts, safeguards, cooperation levels and cybersecurity policies.
- Create a robust master list of all the possible cyber and data assets, and create secure storage.
- Map the level of consequences in case of breaches, and communication channels between you and third-party vendors in such an event.
- Create a work plan to address critical gaps and a longer-term plan to implement continuous improvement across your supply chain.

3. **Utilize procurement and contracting**

- Assess cyber protection in your procurement activities, including your staff's knowledge.
- Identify what cyber insurance you and your vendors have.
- Review or update RFPs and contracts you use with vendors, based on the risk level the vendor poses from the data and systems they have access to. These should at least cover breach notification, cooperation, access for investigations and indemnifying you.

4. **Manage Supplier Relationships**

- Establish and manage collaborative relationships with your vendors, from orientation to connectivity, and ensure a rigorous cybersecurity assessment and feedback process.
- Implement a process to manage contract terms and conditions, and ensure compliance to all cyber-related accountabilities.

II. Respond and Recover

- If you face cybersecurity incidents through vendors or their smart systems, respond jointly with the concerned vendor based on the plan created in Step 1, and identify all priority areas and a collaborative response plan in the event of a breach.

III. Debrief

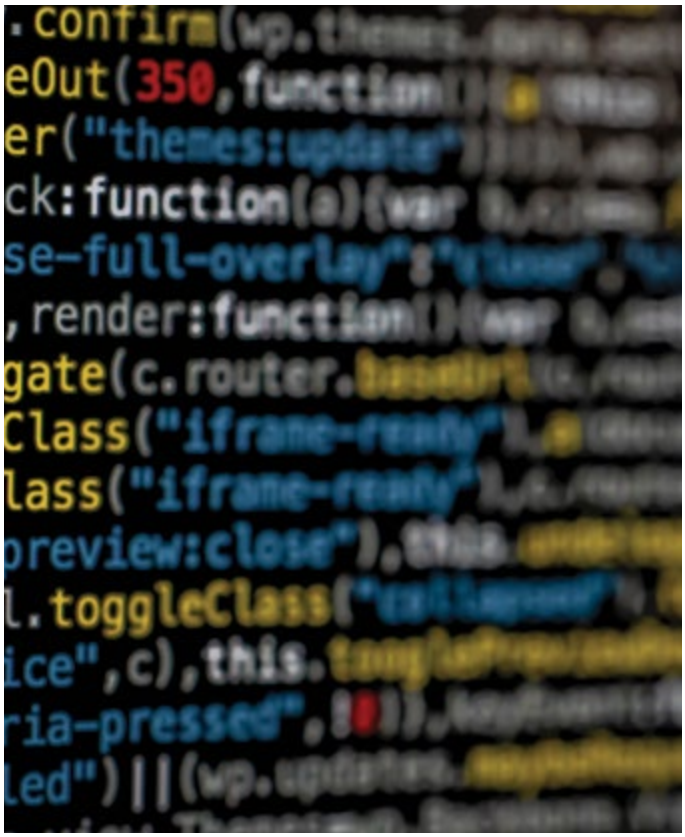
- After the immediate threat has been contained, debrief with the response team, including vendors, on what went well, and identify what went wrong so it can be addressed in future plans.

Introduction

Cybersecurity concerns within commercial and residential buildings have grown with the adoption of Internet-connected or smart systems. While these new technologies add functionality and improve customer satisfaction, managing the cyber risks associated with these systems—as with any Internet-connected systems—is critical.

From HVAC, lighting and elevator systems to sensors that collect data in the background, commercial buildings' adoption and reliance on smart systems or Internet of Things (IoT) is growing at a rapid pace. These systems are built for user functionality and convenience, and not necessarily with cybersecurity in mind. With the expansion and adoption of such systems and devices, new vendors often get added unvetted, or existing vendors have inadequate support for newer operating systems. As cyberattackers become more persistent and patient in trying to take control of your systems or access valuable data, they explore every channel to find your weak links—which are often through third-party vendors or their systems. The increase in smart systems provides a lucrative avenue for cyberattacks across your supply chain, and can leave you increasingly vulnerable as unauthorized parties can gain access to your systems or data through your vendors, or even their suppliers.

Throughout this guide, the reference to supply chain also includes your value chain, where systems or activities may be interdependent, or may be independent of others. A supply chain or value chain attack occurs when an unauthorized party gains access, or infiltrates your systems or your tenants' systems, through one of your outside partners or suppliers who have access to your systems or data.



> "Building cybersecurity requires deep and trusting partnerships with the entire value chain. Setting clear cyber procurement guidelines and processes is one of the best proactive measures a real estate manager can undertake."
>
> – **Scot Adams,** Vice President of National Services, Colliers International

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

There is substantial evidence that organizations have not fully addressed cybersecurity risks posed by third-party vendors.

56%

56% of organizations have had a breach caused by one of their vendors

35%

Only 35% of companies had a list of all third parties they were sharing sensitive data with

18%

Only 18% of companies say they knew if their vendors were sharing that information with other suppliers

Is this for you?

Whether you are fully aware of it or not the following conditions likely exist across your network of properties:

- You have multiple third-party service providers or vendors—from janitorial services to engineering—with physical or virtual access to your information technology (IT) systems, operational technology (OT) systems, software codes, or internet (wired or Wi-Fi).
- There are various access points to your systems/data that affect the physical security at your property.
- There is likelihood of poor information and systems security practices by lower-tier suppliers.
- A real possibility exists that compromised software or hardware from suppliers is resident in your buildings.
- Multiple third-parties are connected to your systems, and are collecting, aggregating or storing data from your building.
- Your staff members that manage or interact with third-party vendors may not be adequately trained to manage cybersecurity risks.

The impact on your organization

In our Cyber Wellness Guide, we listed the impact breaches can have on your properties, from minor to disastrous. As a quick recap, some of the risks cybersecurity incidents pose are:

- 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

Scenarios: Bringing the risks to life

In our Cyber Wellness Guide, we detailed three scenarios drawn from real-world incidents. Two of those were caused by third-party vendors. In this guide, we further explore some examples, which can apply to any building.

Scenario 1: Compromised smart device

A casino in North America had a smart thermometer installed inside a fish tank, that could monitor and transmit data related to the water in the aquarium. The small smart device was hacked by cyber criminals, who were able to utilize it to further penetrate the network.

The hackers were able to gain access to the sensitive high-roller database from the casino and pull that data through the thermostat, and finally upload it to the cloud.

While the device was innovative and made managing and maintaining the aquarium easier, it is likely that many smart devices being manufactured and installed by vendors do not always have adequate levels of cybersecurity built in.

Scenario 2: Compromised building parking system

In 2016, the parking management system of Aviv Tower in Israel was breached in an internet-based hack that exploited a gap in its license plate recognition system. The cyber criminals gained complete control over the parking system, which was operated by the property manager, Hightower Consulting and Management Ltd. As a result, the parking system was inoperable, and the building had no way to manage the payment parking system. There were three immediate concerns:

1. The breach could significantly affect operations causing actual physical damage or an emergency.
2. The potential of loss of reputation and lawsuits.
3. The risk that other systems, especially vital ones, could also be compromised.

Hightower's immediate response was to shut down the parking systems and immediately allow free parking, which resulted in a financial loss but helped avoid chaos and protect both its own and Aviv Tower's reputation. Solid data backups helped mitigate the damage, as did proactive communication with tenants and with the client's leadership. This reassured all stakeholders that the situation was under control and that the inconvenience would be limited.

The hackers asked for a ransom of $8,000 to be paid in bitcoins to restore and return control of the breached system. The property management took the principled decision not to give in to the ransom demand. However, since the backups were not fully comprehensive, the system had to be restored in a process that took an entire week and cost NIS 50,000 (about $18,000 CAD).

Since then, the property manager has conducted an in-depth analysis of their risks to understand where vulnerabilities could exist, and has begun ongoing meetings between its own cybersecurity experts and those of its third-party vendors. As a result, Hightower and Aviv have developed the following action plans which include:

- separation between the different network systems
- segregation of critical information
- routine backups of complete data and systems
- identification of all points of remote access and limiting such access to authorized privileged accounts, as well as the use of one-time passwords/two-step authentication
- regular checkups of all systems and firewalls

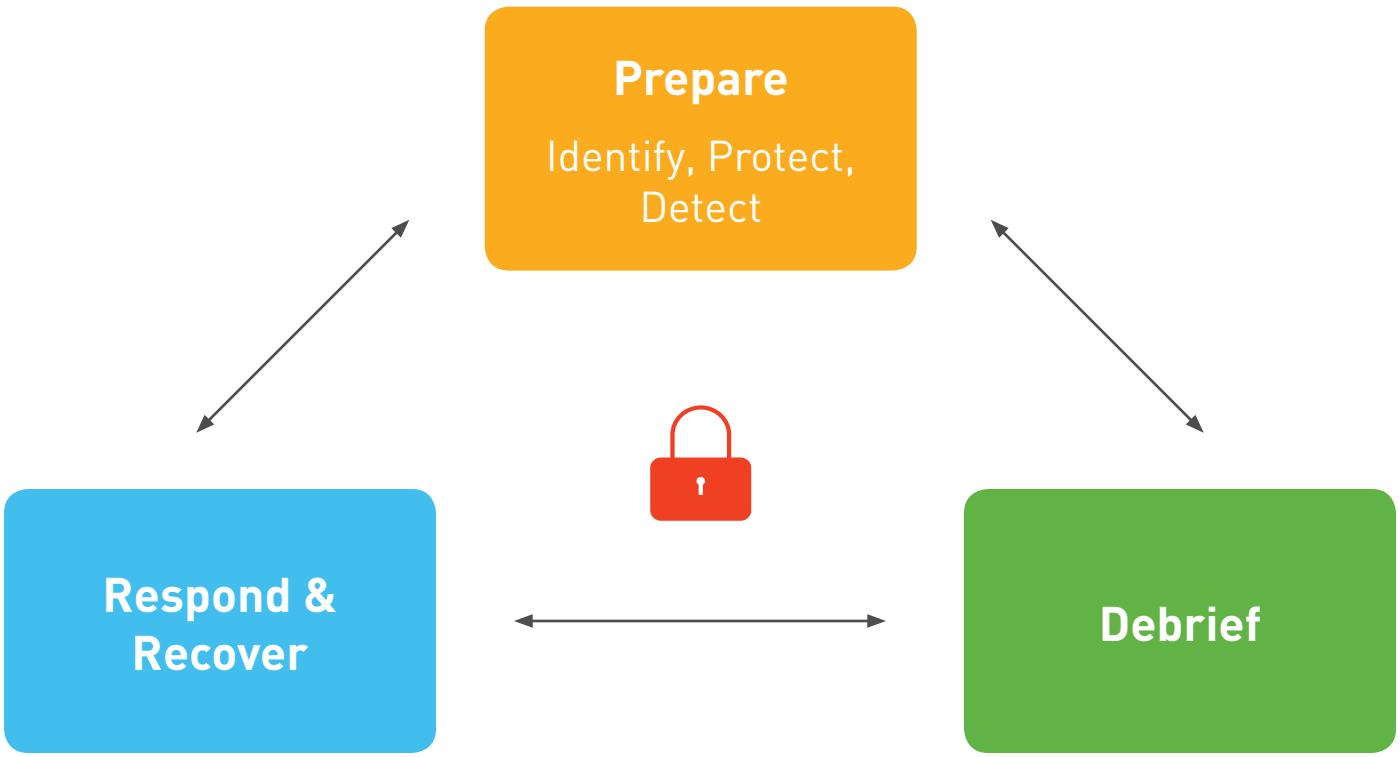
The building is now constantly working towards improving and strengthening their systems and their ability to immediately deal with any incident that could occur. As a result of managing this challenge successfully, its reputation has actually grown stronger.

Incidents, both minor and major can have a significant impact on your buildings, and a large proportion of incidents may occur due to third-party vendors or their systems. With this in mind we have delved deeper into what you can do to guard against and mitigate cybersecurity risks through your procurement practices, with a step-by-step approach.

Cybersecurity through Procurement

> "With the buildings getting more interconnected, everyone shares the responsibility of securing cyberspace."
>
> **- Harsha Vachher,** Manager of Smart Building Solutions, BentallGreenOak

Recognizing that each building or group of buildings may be unique, and each property is managed differently, we have created a series of steps you can work through in order to assess, and then address, the most common cyber vulnerabilities throughout your supply chain. In our Cyber Wellness Guide we covered three high level phases for cyber wellness: preparing, responding and debriefing. This deeper dive into cybersecurity in procurement provides a step-by-step approach to leveraging procurement across these phases.

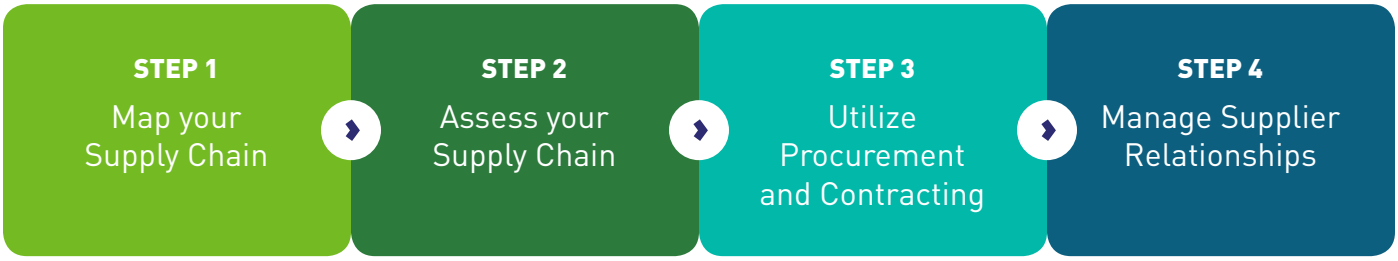


I. Prepare: Identify, Protect and Detect

> "We cannot overemphasize the importance of having a well-defined and documented process inclusive of vetting, continuous monitoring, and an integrated business continuity plan specific to third-party vendors connecting to your environment."
>
> **- Gregory Eskins,** Canada Cyber Leader, Marsh JLT Specialty

The 'Prepare' phase is the most time consuming, but it is critical to get this phase right, as it arms you with the right analysis and mitigation plans. To mitigate your risks, the most effort should go into this phase, and as a result, a large part of this guide is dedicated to helping you with the Prepare phase.

Rather than provide a prescriptive one-size-fits-all recommendation, we have laid out a series of steps or guidelines to leveraging procurement across your supply chain. You can follow these steps to address the most common cyber vulnerabilities throughout your supply chain.



1. Map your Supply Chain

Vendors are often the weak link that attackers are looking for in your supply chain. By building safeguards in your procurement practices, you can make it difficult for attackers to gain access. In this first step, you are building the foundation for a secure supply chain by "taking stock" and understanding the state of your current supplier base and the level and extent of their connectivity into sensitive systems and data within your buildings.

Earlier in this guide, we provided statistics indicating that there is a general lack of awareness of the extent to which vendors and their suppliers have access to—and share—what could be your most sensitive systems and data. While mapping this level of connectivity can be time consuming, it's critical to get right, as it arms you with a clear picture and a starting point for assessing your exposure.

Critical Steps for Mapping your Supply Chain

It is essential to understand and take a detailed inventory of your supplier base and mapping vendors' access to your sensitive systems and data. This should preferably be done simultaneously with creating a complete systems inventory as part of an overall cybersecurity exercise. Through this exercise you need to look beyond your vendors to their supply base. Once you have a clear picture of your supply chain, you will be well positioned to categorize your vendors by risk tier (high, medium, and low risk) and prioritize them by data and system sensitivity. As you map the network of vendors throughout your buildings, you will gain focus, allowing you to address your most vulnerable and high-risk areas.

This step prepares you to assess your current state and vulnerabilities, and then design your procurement practices to proactively identify and mitigate specific vendor risks in your buildings. The following are detailed activities to be undertaken in this phase:

- List all building systems, both major and minor. Identify which ones are connected to the internet and whether they are collecting data of any type.
- Create an inventory of all vendors that have access, directly or indirectly, to these systems, and indicate how the vendors interact with the systems and whether they are accessing or collecting data from the property.
- Determine who installed, and who is servicing these systems, and what level of access they have. It's critical to know the access history, both past and present. Make a thorough 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 authorized users and their level of privileged access to the systems and people who may have left vendor companies but still have access.
- Identify all points of remote access and how each login and access is being logged.
- Categorize and assign priority to vendors based on their connectivity to your most sensitive systems and data.
- Identify how vendor staff that leave the company are currently off-boarded.
- If any data is being collected by vendors:
  - What data is being collected—personally identifiable information or financial data?
  - Classify the data and determine the critical and sensitive data.
  - Identify all data centres and where backups reside. Request information on security protocols for each location.
  - Determine who owns the data and who else has access to it.
  - Identify the mechanism of user authentication to access the data, both onsite and offsite.
  - Review contracts that have been signed with vendors for data ownership and rights clauses.
  - Understand and record the data destruction policy. How long is the data being stored for and how is it purged?

Leading Practices

The following practices should be considered throughout the mapping of your cyber-supply chain:

- The mapping exercise should look beyond the immediate vendor to their supply base.
- The size or scale of the extended supply base should not be a consideration when mapping the supply chain.
- The mapping exercise should not only identify areas of connectivity, but should also identify the ownership and usage of systems and data.
- Verify that you are assessing and applying similar standards to vendors for similar systems, and also different vendors for the same system.

2. Assess your Supply Chain

Framework for Assessment

In this stage, you will assess the supply/value chain within your buildings. Once you have mapped your supply chain, the next step involves conducting a thorough assessment that provides an understanding of your exposure to risks, the strength of your protection to mitigate risks and where to focus your attention for mitigation strategies that can be deployed through your procurement and contracting activities. The following steps will help assess your supply/value chain:

- Establish an evaluation framework to assess your current suppliers. This framework will also be useful for onboarding new vendors. The framework should include the following criteria:
  - Access to systems and data, including user authentication
  - Maturity level of vendor cybersecurity
  - Level of vulnerability
  - Potential for loss
  - System criticality
  - Tenant exposure
  - Contract rigor
  - Insurances
  - Sub-vendor access
  - Degree of influence with vendor
  - Data collection and usage
  - Ability to log activities and allow audits
  - Backups of both data and systems
- If you find that you need more informed assistance to create a robust assessment framework that scales to your business and portfolio, consider hiring an external advisor, who can guide you.
- Utilizing the evaluation framework, assess each vendor (large and small) against the criteria. Apply the same evaluation framework to your vendors' supply base too.
- Conduct thorough third-party vendor check including:
  - Going over all third-party vendor contracts to understand if those contracts meet your cybersecurity policies for insurance, privacy, network, internet, patching etc.
  - Working with the vendors to determine their safeguards, if any, and whether they are willing to work with you to ensure standards are met.
  - Reviewing contracts for potential updates in collaboration with legal, operational and procurement experts within or outside your organization, to require minimum standards and cybersecurity policies.

Leading Practices

The long-term objective is to create a sustainable evaluation and monitoring framework in collaboration with your supply base.

- Establish an evaluation framework that becomes a living document evolving with changes to IT and OT systems and the level of vendor connectivity.
- The cybersecurity profile of third-parties/vendors with access to networks, systems, and data can change frequently. Implement a cost-effective means of continuous monitoring, which allows corrective and proactive action to be taken as risks/threats present themselves.
- Involve your supply base in both the outcomes of the assessment as well as the evolution of the assessment framework.
- Refer to available standards such as NIST and ISO 27001 amongst others.

- Create a robust master list of all the possible cyber and data assets that involve vendors, and get 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 and consequences that all these systems can have if they are breached, and what communication channels exist between you and third-party vendors in such an event. Ensure that any overall incident response plan you have in case of a cyberattack takes into account these communication channels.
- Identify a path to conducting ongoing assessments.
- Conduct an assessment of your vendors and the building staff who deal with them, including their awareness of risks. This includes testing for their understanding that seemingly mundane occurrences such as blank screens or system reboots may be due to a cybersecurity incident.
- Create a work plan to address the most critical gaps and a longer-term plan to implement continuous improvement across your supply chain, including where to focus your mitigation strategies.

3. Utilize Procurement and Contracting

Once you have mapped your supply chain, assessed your level of exposure and conducted a robust evaluation of your strengths, weakness and key exposure areas, you are now ready to deploy specific procurement and contracting activities to help mitigate the risks of infiltration via your supply base.

In this step, you ensure that your procurement and contracting activities have a keen cyber focus. Doing so will position your procurement as a key line of defense that provides expedited and coordinated response with your vendors should an attack occur. To accomplish this, you will be taking a look at your current procurement practices, and realigning them to create a robust environment for cyber protection and response. Site-level contract awards should adhere to the cyber framework and process, so that vendors cannot be awarded without adequate security assessments, and contractual obligations.

> "Procurement has historically been viewed as a transactional function, but should be positioned strategically to strengthen cybersecurity and protect you from infiltration of your systems and data through your supplier base."
>
> **- Trent Bester,** Senior Vice President – Consulting and Public Sector, MNP LLP

Procurement

The following are key procurement elements to consider:

- Look at your how your procurement is organized. Is there a single point of contact for assessing how cyber protection is embedded in procurement activities?
- Do your procurement people or teams have the required training in cyber procurement concepts?
- If necessary and possible, conduct joint cyber awareness training for both your vendors and your staff enabling them to understand and minimize cyber risks, and deal with breaches seamlessly. Caution should however be exercised in sharing any sensitive information or vulnerabilities.
- While selecting vendors, analyze the risk-reward balance that innovative new products and start-ups may offer from a cybersecurity perspective, and make choices accordingly.
- Explore whether your company has cyber insurance, and what insurance your vendors have. This insurance can be very critical if a breach occurs. Refer to the 'Key Insurance Considerations – Cyber Procurement' section on page 15.
- Review any requests for proposals (RFPs) and contracts that you are currently using, and identify whether the appropriate cybersecurity requirements are built in or assessed during selection.
- While reviewing your vendors, both old and new, it is important to classify exactly what data and systems they have, or will have, access to, and classify it as: (i) highly sensitive; (ii) somewhat sensitive; or (iii) not sensitive and update the inventory created in Step 1.

Cybersecurity in RFP Questionnaires

During RFPs, or if possible even with existing vendors, have a detailed questionnaire that they have to fill out. This should include questions on:

Technical safeguards

Do they have any technical cybersecurity standards that they adhere to or certifications such as NIST, ISO 27001, CIS etc? If not, what technical checks do they have in place?

Administrative or governance safeguards

Often, companies are found to falter on administrative or governance-related safeguards. Do the vendors you are evaluating have the following?

- an incident response plan
- a data policy
- formal employee training and testing, and if yes, what kind
- background checks while hiring employees or contractors
- access monitoring, onboarding and offboarding practices for subcontractors
- cyber insurance (Refer to the 'Key Insurance Considerations – Cyber Procurement' section on page 16)

Physical safeguards

What physical protection do they have onsite, including access cards or fobs, and physical restriction from systems?

Contracting

It is critical to review the existing contracts you have from a cybersecurity perspective, and also when you onboard new vendors to ensure you have clear insight into your cybersecurity risks and checks.

- In your contracts, safeguard yourself based on the risk level the vendor poses from the data and systems they have access to. Also include safeguards based on their responses to your questionnaire (refer to earlier section on procurement).
- Review or update the contracts you use with vendors to include cybersecurity requirements. Consider hiring a legal expert with up-to-date cybersecurity expertise to help you. Some common considerations in your third-party vendor contracts include:
  - Their obligation to notify you if they detect any breaches.
  - Cooperation requirements if any incident is detected by them or you. This includes information or systems they would have to allow access to for an investigation.
  - How they indemnify you—that is, protect you financially—or compensate you from financial repercussions related to an incident. Vendors often attempt to limit their exposure, but crafting broad indemnity agreements, ideally backstopped via an insurance placement, may be possible. Consideration of the level of access and sensitivity of data should guide the agreements.
  - If a vendor has access to highly critical information or systems which could result in significant loss of safety, money or your reputation, you may consider adding a clause to audit your vendor for cybersecurity practices. This clause is typically added only in high-risk situations, and also depends on the vendor's willingness.

Leading Practices

Companies across industry sectors have adopted a variety of practices that help them manage cybersecurity risks in their supply chain. Embedding these practices can add significant value to your cybersecurity program:

- Cybersecurity requirements and questionnaires are included in every RFP to assess a vendor's cybersecurity maturity level.
- Cybersecurity requirements are included in every contract and component purchases are tightly controlled.
- Notification requirements from your vendor if they detect a breach within a certain time limit—usually no longer than 24 hours.
- Programs and training for all internal and external servicing personnel in the life cycle are established, and access is limited to trained personnel.
- 'Zero-tolerance' policies with respect to vendor products that are found to be counterfeit or do not match the specification as per your contract.
- Indemnity and insurance provisions adequately protect both the vendor and the building/data owner in the event of a breach.
- The vendor must identify all data centers where the data or data backups will reside.
- Refer to the NIST standards as a source for additional leading practices.

Key Insurance Considerations – Cyber Procurement

Requiring a vendor to carry insurance coverage for their business risks is routine. These insurance requirements include such standard business insurance as Auto, Property, and General Liability. In professional or technology service contracts Professional Liability (E&O) is also standard, and increasingly so is cyber coverage.

It is important to remember the reason for requiring your vendor to carry coverage—to help ensure they have the financial wherewithal to support their indemnity obligations.

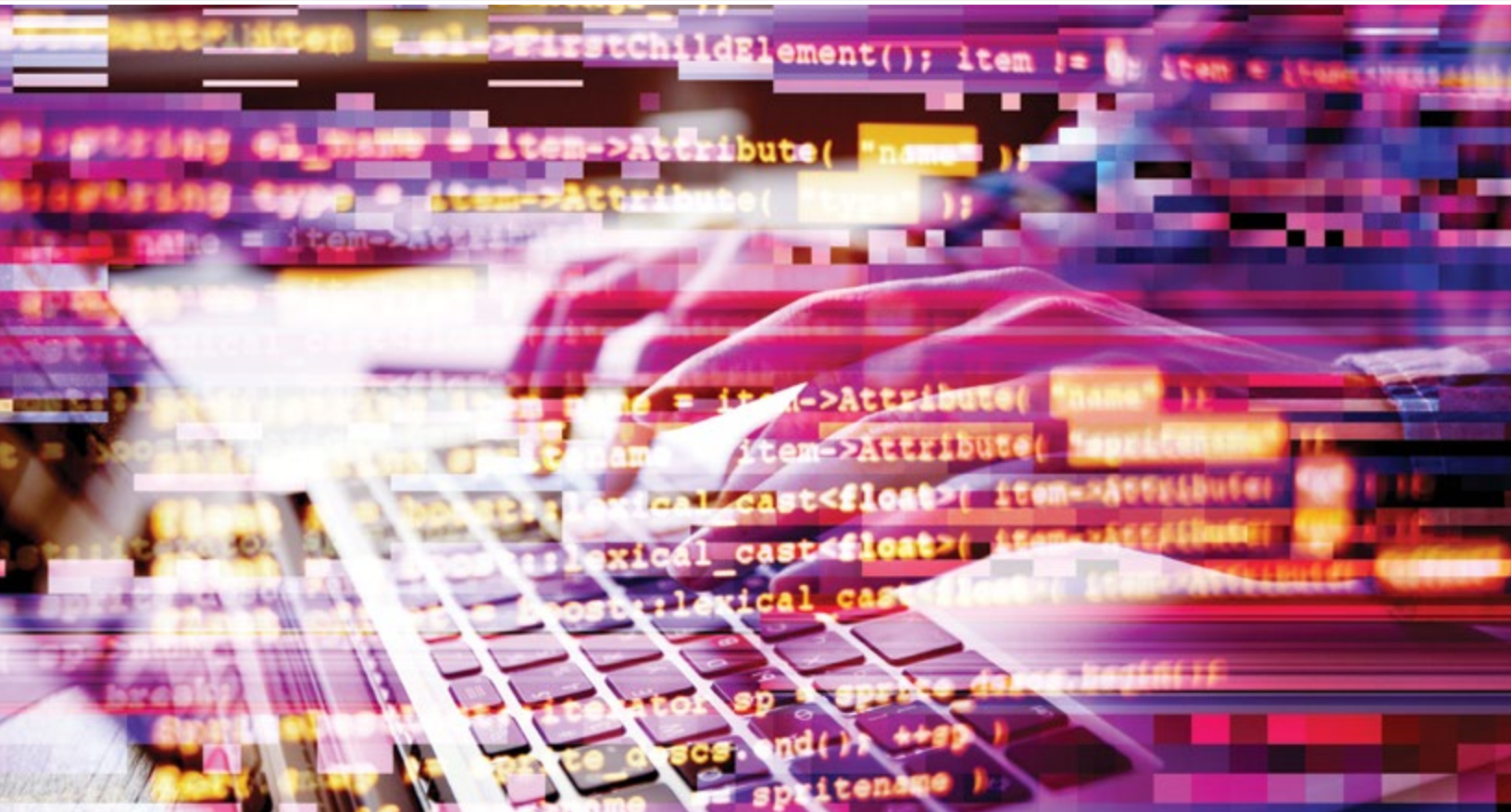
With respect to cyber insurance, the reason may also be to ensure that the vendor has been through the cyber insurance due diligence process, meaning that underwriters have evaluated their risk management maturity and risk.

Should I request that my vendor carry E&O or cyber, or both?

Typically, E&O insurance provides the vendor with coverage for a failure of their services, while cyber coverage addresses cybersecurity issues with the vendor's network or disclosure of private information, however caused.

E&O should be required if the vendor is providing a service and the policy must cover negligence more generally. Most companies who need to purchase E&O insurance will bundle the liability elements of cyber coverage into their E&O policy, so one policy may satisfy both requirements.

If the concern is a data breach due to a vendor handling your data, then either E&O or cyber may be sufficient, depending upon policy language. In an abundance of caution, in this emerging field of risk, it may make sense to require both (and many tech services companies buy these coverages together). Your insurance broker should be able to assist in drafting insurance specifications for your vendor contracts.



4. Manage Supplier Relationships

The most effective defence against cyberattack via your supply base is to establish and manage collaborative relationships with your vendors.

Supplier Relation Management is the discipline of strategically planning for, and managing, all interactions with third party organizations that supply goods and/or services to an organization in order to maximize the value of those interactions.

Managing your supplier relationships, while asking for better cybersecurity practices from them, can be a difficult balancing act. On the one hand, you want to retain your best vendors and get new and innovative systems, but on the other hand you have to seek more robust cybersecurity practices and greater compliance from them to mitigate your risks. In exploring what balance may be right for you, consider the following:

- Onboard your vendors, and include cybersecurity discussions, right from orientation to connectivity.
- Implement a process to manage contract terms and conditions, and ensure compliance to all cyber related accountabilities.
- Create an environment of open communications on issues and areas of improvement.
- Implement a rigorous and ongoing evaluation and feedback process for critical vendors.
- Create a transparent and clear testing and audit process.
- Work collaboratively to mitigate risks for both parties.
- Include vendors in your process discussions and planning for monitoring, review and patch installation.
- Agree and work with vendors on breach reporting and response protocols. This does not mean however that you should include third-party vendors in tabletop exercises, since sensitive company information should only be shared with select parties such as your lawyer or consultant.
- Work out how to seamlessly terminate protocols and delink systems in case of a breach.
- Conduct an assessment and monitor vendors' cybersecurity performance on a regular basis.
- Jointly establish and monitor off-boarding ensuring that requirements are adhered to.

Often, if the vendor is a large company, it may be harder to influence. Coming together with other buildings' managers through an association may be an option to consider.

On the other hand, if the vendor is a small company or a start-up, asking them to significantly change their products or buy more insurance may not be financially feasible for them. Work on a case-specific basis to see what the size of the risk is, and what can be done to mitigate the risk, while not putting undue pressure on either you or them. Remember, your first priority is to protect your organization and your tenants. If your vendor is not able to support that goal, you should extend your search to others.

Leading Practices

Building the following practices into a robust supplier relationship program will assist with mitigating cyber related incidents:

- Create a formal supplier relationship program that oversees vendor activities from selection and onboarding to offboarding and decommissioning of their connected systems.
- Once a vendor is accepted in the formal supply chain, a security staff member or team works with them onsite to address any vulnerabilities and security gaps.
- Personnel in charge of supply chain cyber-security should partner with every team that touches any part of the product during its development lifecycle. This ensures that cybersecurity is part of the suppliers' and developers' processes and tools.
- Refer to the NIST standards to incorporate some key practices.

Incidence Response Plan: Include Third-Party Vendor Considerations

Despite mitigation efforts, a cybersecurity incident may occur. An incident response plan should be created as part of your overall cybersecurity planning. Your third-party vendor risk management program should align with your security operations and incident response capabilities. From a third-party vendor standpoint, it is important that your incident response plan include:

- The different types of situations that may arise due to third-party systems and vendors.
- 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 jointly with vendors, based on the situation.
- Escalation procedures.
- Joint internal and external communications plan including media responses if applicable.
- Joint debriefing and post-mortem analysis.
- Recovery process.

II. Respond and Recover

Despite your best efforts and mitigation, you still may face cybersecurity incidents through vendors or their smart systems. In such an event, you have to be ready to act immediately, systematically, and jointly with them, to minimize its impact. Any delays or inefficiencies can have significant repercussions. Preparations in earlier phases should have you and the concerned vendor(s) ready for any breach that may occur.

- Circle back to the incident response plan you created in Phase 1, and identify all priority areas and a collaborative response plan in the event of a breach:
  - Identify what systems are affected and what other systems it could cascade to.
  - Inform all the people and teams that need to know, both within your organization and the concerned vendor's organization and supplier base.
  - Have the right staff and vendor disconnect or isolate the system, and switch to operating manually if possible.
  - Work towards life safety first if that is a concern.
  - If required, include your vendor in 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.

III. Debrief

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

- Gather the response team, along with the vendors concerned and evaluate why the breach occurred.
- If there were any gaps from the vendor, work with them on how to prevent any similar breaches and build in any necessary improvements into your RFP/vendor selection process.
- Assess whether any additional policies relating to the vendor could have prevented the incident.
- Assess the response to the incident from the vendor's perspective to see if you can improve upon it in case of any future issues, or whether you need to change your vendor.
- Analyze whether all parties were informed and communicated with in a timely manner.
- Work on and communicate the changes needed to prevent another incident, including any further patching, system lock downs, passwords changes, anti-virus updates, email policies etc.
- Capture and communicate the lessons learned to all relevant parties.

Conclusion

Today, cybersecurity planning is critical for commercial and residential buildings as smart systems increasingly make inroads. While the breaches and incidents can often originate from third-party vendors, the risks and ensuing losses can greatly affect you.

To manage these risks better, it is critical to apply the cybersecurity lens to your third-party vendors , whether it is in how you select them, or in how you work with them. Understanding your supply chain and areas of exposure will assist you in planning to mitigate risk and formulate a robust plan in case an incident should occur —one that includes your third-party vendors.

It is critical to get started, and work diligently towards cybersecurity planning. We hope this guide, along with the BOMA Canada 2019 Cyber Wellness Guide, can help you with your cybersecurity journey towards becoming more resilient.

> "We are in the midst of a rapid acceleration in the digitization of the built environment. A critical part of this evolution is ensuring that as an industry, cybersecurity is top of mind and rooted in everything we do."
>
> – **John Chung,** Vice President, Portfolio Technology, Digital Innovation, QuadReal Property Group

Further reading

BOMA Canada 2019 Cyber Wellness Guide: http://bomacanada.ca/resources/cyber-wellness-guide/

National Institute of Standards and Technology (NIST): https://www.nist.gov/cyberframework

Incident Response Plan (IRP) by NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-61r2.pdf

Acknowledgments

We are grateful for the financial support of MNP LLP, QuadReal and Morguard, and for the expertise provided by MNP LLP, Marsh and Blakes.

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

Scot Adams, Vice President, National Services Colliers International

Stephen Adams, General Manager, Urban Portfolio Toronto, Cushman Wakefield

Imran Ahmad, Partner, Blake, Cassels & Graydon LLP

Trent Bester, Senior Vice President, Consulting and Public Sector, MNP

John Chung, Vice President, Portfolio Technology, Digital Innovation, QuadReal Property Group

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

Gregory Eskins, Managing Director, Canada FINPRO and Cyber Leader, Marsh JLT Specialty

Patrick Gilbert, Senior Manager, IT Security, Ivanhoé Cambridge

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

Kendall Peart, Managing Director, Real Estate, MARSH

Bob Riddell, Director, Security and Life Safety Security Ivanhoé Cambridge

Lee Thiessen, National Leader, Real Estate and Construction, MNP

Naveli Thomas, Director, Nyox

Harsha Vachher, Manager, Smart Building Solutions BentallGreenOak

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