BOMA Canada

2021 Cyber Wellness Guide

The role of Supplier Relationship Management (SRM) in cybersecurity

This Guide is Sponsored by:

FIRST CAPITAL Genetec MNP LLP QuadReal

We are proud to present this guide on the role of supplier relationship management (SRM) in cybersecurity, intended to help building owners and managers with their cybersecurity journey as it relates to their suppliers.

Dear friends,

BOMA Canada seeks to provide valuable education and tools to its members through its knowledge series. Over the last few years, cybersecurity has been a growing area of concern in commercial and residential buildings, and our cybersecurity guide series seeks to shine a light on this critical subject.

The BOMA Canada 2019 Cyber Wellness Guide—the first guide in the series—introduced cybersecurity threats and provided a starting point for buildings' cybersecurity journey. The following year, the BOMA Canada Cybersecurity Guide - Procurement delved deeper into embedding cybersecurity practices in procurement. With third-party suppliers often becoming the point of entry for perpetrators of cybersecurity incidents and breaches, there was a need to delve deeper into embedding cybersecurity in (SRM), which this guide seeks to do.

Sincerely,

Benjamin Shinewald
President & CEO,
BOMA Canada

How should this guide be used?

This guide is intended to introduce building managers and owners to building SRM programs that can help mitigate cybersecurity risks. It is best used in conjunction with overall cybersecurity planning, and follows our previous cybersecurity guides, so that readers can link dependent decisions about how they manage their supplier relations through a cybersecurity lens.

This guide, while intended to help you with your journey, 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 risk management and mitigation plans.

We hope you this guide is useful in your cybersecurity journey, and we welcome your suggestions on future guides.

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.

Why Suppliers Matter in Cybersecurity

Today, cybersecurity threats come from unexpected places, and attackers look for the weakest link in your supply chain. Their point of entry is often unwittingly a supplier, whose systems or processes may not be as robust as yours. The risk may also lie within their supply chain, where a hacker can breach via their suppliers to find an entry into your system.

Suppliers in commercial buildings can be varied and can include technology service providers, system integrators, contract workers who have access to your building or internet, visiting technicians and even sub-contracted maintenance staff, amongst others.

Typically, core suppliers, while essential to your organization, can increase your risks in various areas:

- financial
- location access
- business continuity
- recovery capability
- day-to-day operations

More recently, cybersecurity concerns have expanded these existing risks and opened up a number of new supplier-related risks. Some additional considerations for organizations in their risk assessment now include:

- the process suppliers follow to vet their own personnel that have access to your data, systems or facilities
- how your vendors vet the information security practices of their service and product providers to ensure that they do not pose potential risk
- the cyber safeguards that vendors embed in products and software that will be integrated into your systems
- safeguards against counterfeit hardware or hardware with embedded malware
- fourth-party data storage or data aggregator tools and practices

Managing your supplier relationships is more critical now than ever before to mitigate these risks and provide the services your customers and tenants seek in a safe environment.

Bringing the Risk to Life: A Case Study

How can more robust contracts and relationships with vendors help manage cybersecurity risks? Let's take a recent situation as an example.

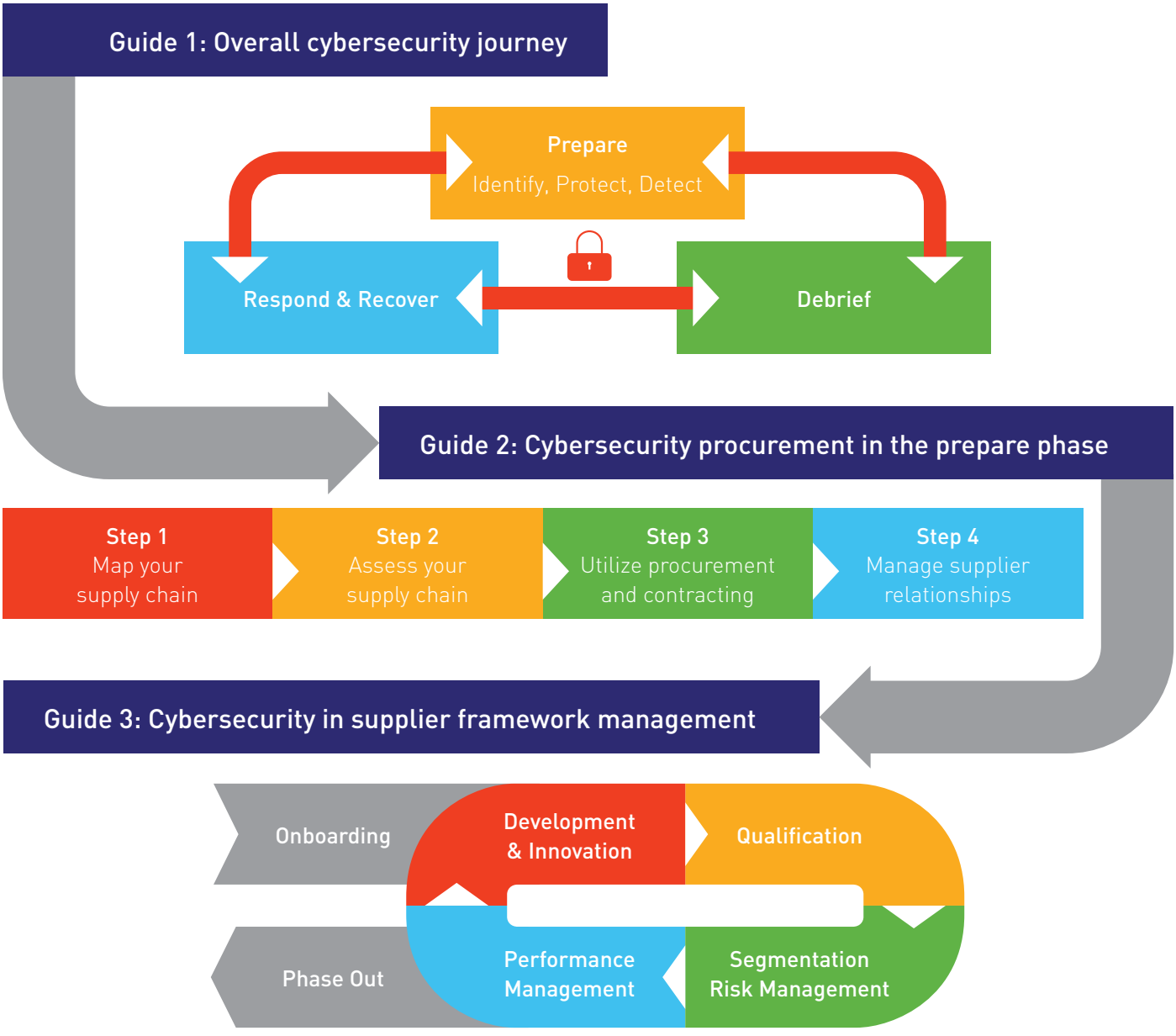
A property management company changed its electronic display vendor. When the contract ended, a new vendor was selected. Despite not having the contract any longer, the previous vendor was able to continue changing the visual displays. A deeper look revealed that the appropriate checks and balances had not been built into managing the vendor and the vendor contract, and the previous vendor still had administrative privileges to access the displays via unsecured wifi. Better management of the relationship, and a security assessment of how access is granted and disabled, would have helped mitigate this risk for the property management company.

What becomes obvious from this example is that a cybersecurity threat can emerge from anywhere, and while it can risk information, it can also risk any system within a building—whether large or small. Taking the right measures on multiple fronts, including SRM and cybersecurity, have become critical in mitigating and remediating risks irrespective of asset class and technology.

The Importance and Selection of this Topic

In our first guide, we presented an initial overview and checklist for building owners and managers to get started on their cybersecurity journey. The guide outlined the three key phases of cybersecurity planning: Prepare, Respond, Debrief. In our second guide, we delved deeper into the procurement aspects of the critical "Prepare" phase, since a key element of cybersecurity is reducing weaknesses throughout your supply chain. This guide focused on the procurement aspect of cybersecurity, including aspects such as contracting and creating better request for proposals (RFPs). As our conversation around cybersecurity for building owners and managers deepened, a key area of concern emerged—managing and building third-party supplier relationships to proactively enable better collaboration around cybersecurity. This guide delves deeper into this critical aspect of cybersecurity.

A visual representation of the subjects our three guides is below.



Understanding SRM

As a commercial building owner or manager, your operations rely on a multitude of suppliers and vendors. Managing relationships with your vendors is key for running operations smoothly, as they are often highly integrated and you require their cooperation. In an increasingly digital world, your suppliers are continually advancing their technology—and in turn their sub-vendors and suppliers are too. This drives the need to build strong relationships of collaboration to mitigate the associated cyber risk while driving greater benefit from advances in building technology. This is where SRM comes in.

Supplier relationship management, sometimes referred to as supplier or vendor management, is a comprehensive approach to managing an organization's interactions with vendors that supply products and services, in order to enhance cooperation, coordination and communication and manage risk. Just as organizations manage and improve relationships with clients through customer relationship management (CRM) programs, managing relationships with suppliers through SRM is critical.

Benefits of SRM

Strategic SRM is one of the most important means to drive innovation, and in the case of commercial building owners and managers, help them provide superior services to customers and tenants.

There are many advantages to SRM, and developing mutual, trust-based relationships with key strategic suppliers can help align efforts and produce significant benefits such as:

- greater access to supplier-led product innovation
- reduced supply risk with better cooperation
- coordinating towards a leaner supply chain
- reducing short, medium and long-term costs
- finding more efficient procure-to-pay processes
- increasing bottom line results and competitive advantage

Collaboration and building relationships of trust

The procurement function these days is looking to drive significant business value from their supplier relationships. What used to be more transaction-based relationships between suppliers and the organization have increasingly given way to more collaborative partnerships.

Organizations that get it wrong often start SRM programs with a short-term mindset, expecting immediate pay-offs, and then either abandon their efforts midway or have poor strategy and execution resulting in no significant benefits or gains. SRM programs should be seen as long-term commitments, with a cross-functional and coordinated approach, a robust governance structure, and innovative methods to track and measure value.

Here are some SRM best practices that building owners and managers can greatly benefit from:

Improving supplier segmentation

Often, suppliers are segmented based on their business impact or supply-market complexity. Based on these two parameters, suppliers are classified into strategic, bottleneck, leverage and routine suppliers. However, this segmentation often leads to errors in execution and poor returns. A critical third parameter is measuring long-term compatibility between the organization and supplier. This segmentation helps more in building an effective SRM program. **Cybersecurity adds another dimension to your segmentation, allowing you to separate vendors by level of access to critical data and systems.**

A clear model for key suppliers

After the suppliers have been segmented, a clear model should be established that helps organizations track a relationship from the beginning and throughout its lifecycle. This could include factors such as responsibility for managing the relationship regularly and when senior leadership needs to intervene. Of key importance is ensuring that both the organization and the supplier work towards performance that helps meet business goals. Suppliers of strategic importance require more oversight and monitoring than others.

A key component from a cyber perspective is ensuring there is a clear plan for both the prevention and response to cyber incidents. The plan should cascade from high level planning down to tracking and monitoring upgrades and patches to the technology your suppliers have embedded in your operations.

Effective communication

It is important to treat a supplier as a partner, and maintain strong levels of communication that can help build a mutually beneficial relationship for the long-term, and be strategic over the relationship's lifecycle.

Clear and transparent communication as well as feedback sessions are critical especially when dealing with cyber response plans and the execution of those plans in the case of an incident.

How well organizations manage supplier relationships can make the difference between suppliers that can help them succeed and those that do not cooperate when they need it. It is only when your organization is systematically invested in its relationship with key vendors, that you have cooperation and trust you can rely upon for cybersecurity and beyond.

Key features of leading SRM programs

SRM involves strategy, assessment, and action planning to continuously improve long-term strategic supplier relationships. There are diverse models, and each organization needs to evaluate what model, or combination is suitable for their specific situation.

Embedding cyber related elements into your SRM model does not come without cost to you and your supplier – therefore, a clear understanding of the mutual benefits of the relationship, trust in each other, fairness, and honest and open communication is critical.

Key factors to embed in your SRM program

Building a program that is right for you

Today, organizations with leading practices have a SRM program in place that is appropriate for their size and can be easily scaled for future growth. Similar to any other aspect of your business, strategies are required for a structured relationship with your key suppliers. Create a plan with clearly outlined SRM goals and timeframes, list the activities and processes to attain goals, establish roles and responsibilities, and for cybersecurity, identify high-risk systems and data that need to be addressed. Your plan should be measurable and achievable, and ensure fairness in what you expect from key suppliers.

Build relationships with strategic suppliers

It is important to value highly integrated suppliers over regular vendors, and not make requirements purely transactional or cost-based. These relationships of trust require time to build and are based on mutual benefit. The level of technological connectivity and data integration is a key cyber related requirement that should be assessed when identifying strategic suppliers.

Embed the right behaviours

It is the responsibility of both the supplier and the buyer to foster desired behaviours in order to ensure a mutually beneficial situation. Selecting sufficiently invested suppliers is key—purely opportunistic activities or a lack of a long-term vision may indicate that the supplier is not right for you. Your supplier proactively identifying potential cyber risks as part of their onboarding processes is a clear signal they have long-term and mutually beneficial interests in mind.

Create robust contracts

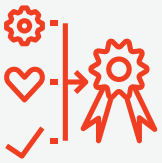
Create and agree on a clearly crafted contract, where terms, conditions and service level responsibilities are outlined. This will eliminate conflict or disagreement if any issues occur. Ensure that cybersecurity requirements and expectations are clearly outlined in your contracts.

Manage performance

An effective SRM program should include defined processes and metrics to manage performance. From a cyber perspective, this should include regularly scheduled meetings with senior people to discuss cybersecurity prevention and response plans, and with tactical operations people to ensure more technical aspects such as integration points, upgrades and patches are clearly understood and managed. Engagement with different management and operational levels will ensure that the program works day-to-day while continuing to meet the long-term goals of both parties.

Train adequately

Training is essential when instituting an SRM program, to educate your employees on benefits and their role to ensure a successful program. As an example, scenario-based training for front line staff to prepare them for cyber incidents should be a key element of the program.



Address roadblocks

Openly discussing and taking feedback on barriers from key suppliers is critical. Are there communication issues they have to deal with while working with your organization? Or incompatible software? Addressing roadblocks upfront is critical in overcoming issues with your key suppliers, and this will be particularly handy in case of a breach.

Invest in the right technology

Depending on the size of your organization and the scale of your SRM program, having the right SRM systems and processes in place will make it easy to view the status with your suppliers and analyze your risk factors. The technology can provide you with complete visibility on what is impacting your supply chain, making it easy to mitigate risks, including those that stem from cybersecurity.

Cybersecurity-related elements of SRM

An evolving element of SRM is working with vendors to not only ensure innovation, but do so securely with the appropriate cyber safeguards in place. Cooperation and strong, well-managed supplier relations become critical when risk needs to be managed or mitigated, and cybersecurity breach response is time sensitive.

While many models and frameworks have been created, the best approach is to understand what your organization needs based on your specific situation and scale, rather than follow a one-size-fits-all approach. In this section, we have attempted to illustrate how you can build cybersecurity elements into your SRM program.

Building cybersecurity elements into SRM processes

Some key practices help businesses manage their suppliers more effectively, bolstering their cybersecurity efforts in the process. We have provided a checklist that building owners and managers can use to institute SRM leading practices, best used in combination with our cybersecurity procurement guide:

Focus on what matters most

- ☐ Classify your organization's specific risks, and create priority levels based on your most valued and vulnerable assets—what you must protect most.
- ☐ Articulate and focus on your brand integrity—how customers perceive you—over brand protection. This view better supports lifecycle threat modeling, which in turns helps proactively identify and address critical vulnerabilities in your supply chain.

Engage your organization

- ☐ Develop procurement and sourcing processes jointly with input from IT, security, engineering, and operations personnel, so that sourcing decisions receive multi-stakeholder input and take different requirements into account.
- ☐ Assign senior-level ownership and formal responsibility for any exceptions that are made to cybersecurity guidelines and any resulting business impact.
- ☐ Jointly develop a responsibility matrix that clearly defines who is accountable and responsible (between you and your suppliers) for the management and monitoring of key system integration points and the security of critical data and systems.

Conduct comprehensive risk assessments

- ☐ If vendors have different levels of access and pose different levels of risk, design assessments to measure critical risks, and assign an appropriate level of risk to each vendor. For example, your assessments may reveal that a janitor has different risk level assigned to them than a technician with access to systems.
- ☐ Consider employing onsite verification and validation of risk assessments. Suppliers often offer self-evaluations, but these should be managed overall by cybersecurity and SRM personnel at your end.

- [ ] If required, cross train personnel so that they are more integrated with supplier activities. This will enable them to monitor security criteria as required.

Working with vendors on cybersecurity

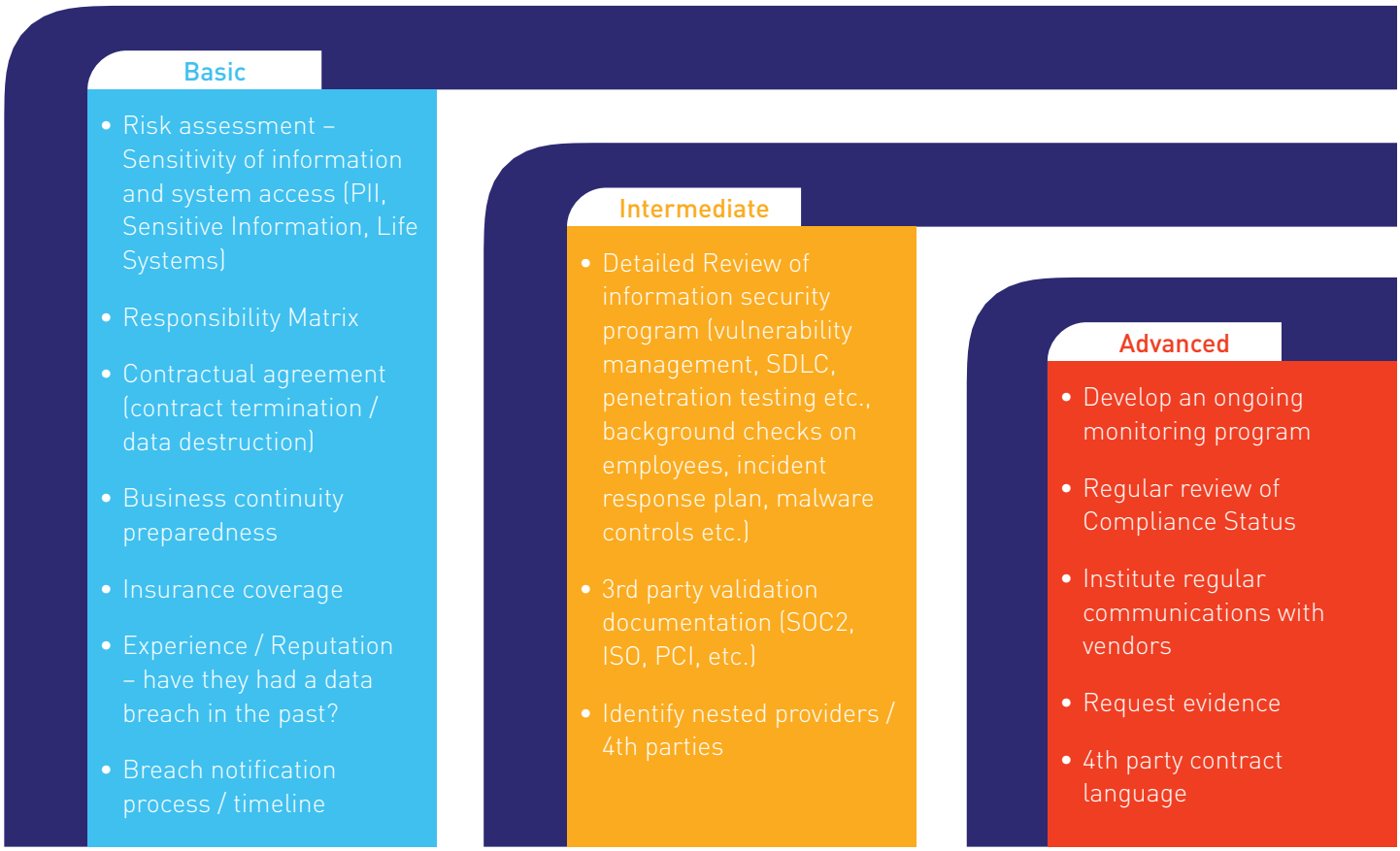
- [ ] Create approved vendor lists, which are established and complied with across your organization, with clear guidelines on the requirements and process for exceptions to be approved. Keep relationship compatibility in mind while doing so.
- [ ] Create standard security terms and conditions, which are included in all requests for proposals (RFPs) and contracts, tailored to the type of contract and business needs. Refer to our previous cybersecurity procurement guide for RFP and contracting recommendations
- [ ] For new suppliers, conduct a test and assessment period—to test the capabilities of the supplier and their compliance and compatibility with various requirements before they actively join the supply chain. In high risk areas, for example, a supplier might go through a series of carefully controlled pilots before they fully enter the supply chain.
- [ ] Require high risk level or key suppliers to hold their suppliers to the same standards.
- [ ] Conduct quarterly reviews of supplier performance and relationships with a stakeholder group with the appropriate knowledge and expertise.
- [ ] Conduct annual supplier meetings to ensure that suppliers understand your business needs, concerns and security priorities.
- [ ] Offer mentoring and training programs to suppliers, especially in difficult or key areas of concern related to cybersecurity.
- [ ] Create a Vendor due diligence package that requests key cyber-related information from potential new vendors or other third-party partners.
- [ ] Conduct ongoing and timely evaluation of vendor relationships from a cybersecurity perspective.

Certification of vendors—setting up criteria and a program, certifying existing and new vendors

Supplier relationship management from a cyber perspective is not a one-size-fits-all for the commercial and residential building industry. How an organization manages its cybersecurity risk is highly dependent on the portfolio of properties and the level of technology integrated into their operations. To address these specific needs, organizations have recently begun developing internal vendor certification programs designed to address the unique aspects of their supplier profile. The creation of the certification programs help with:

- Rapidly assessing and prioritizing the vendor portfolio for further review
- Obtaining analyses for previously unassessed vendors
- Alerting the organization whenever material change occurs for individual suppliers
- Tracking score changes over time to identify historical patterns, both positive and negative trends
- Triaging potential vendors during an RFP or selection process
- Continuous monitoring of medium- to high-risk suppliers
- Rapidly identifying specific issues for new suppliers to address in contract negotiations
- Enabling cybersecurity incident response processes when new vulnerabilities emerge

As with your SRM program, an embedded supplier certification program can evolve over time. The diagram below illustrates a guideline for starting your certification program and advancing it over time as required.



PII - Personally Identifiable Information

ISO - International Organization for Standardization

PCI - Payment Card Industry Data Security Standard

SDLC – Software Development Lifecycle

SOC2 - Service Organization Control 2, reports on various organizational controls related to security, availability, processing integrity, confidentiality or privacy

Centre of excellence

It is critical for all organizations to create a centralized source of information related to cybersecurity, which is accessible to others across the organization. This can be a person or department dedicated to this critical topic, or may be an outsourced third-party provider whose knowledge base you can tap into when required. Which option is best for you depends on the size of your operations and your specific cybersecurity journey.

Your centre of excellence should have some key responsibilities, outlined below.

Best practice repository: The centre of excellence should keep a central record of both cybersecurity best practices for your building(s), which are deployed and evolved as the threats evolve. The supplier management and relationship aspects should be coordinated with the people or team responsible for SRM.

Training: Cyber awareness training at scheduled intervals is critical for frontline property managers, operations teams and anyone with access to data or systems and responsibility for engaging with suppliers. This, based on your relationship with suppliers, may also include key suppliers.

Cybersecurity inventory: Collecting and monitoring the inventory of internet-connected devices and technology is an essential component of cybersecurity, and should be centralized to monitor risks.

Vendor lists and certifications: A list of vendors, along with their level of access to data, technology or systems,

should be centrally maintained. The cybersecurity standards, certifications or re-certifications your organization requires of your vendors as part of your cybersecurity protocol should be controlled and monitored centrally, and executed with the cooperation of the people or teams responsible for the supplier relationships.

New technology protocols: The protocols you require for cybersecurity need to be managed with consistency for the installation of new technology and for vendors that propose a beta or trial test of new technology. Installations, patches, updates and pilots should adhere to standards and clearance centrally, and the central person or team should work with others in the organization to ensure the suppliers comply.

Procurement requirements: In our last guide we delved into ensuring cybersecurity in procurement, including in contracts and request for proposals (RFPs) and request for information (RFIs). The centre of excellence should be a centralized resource for standardizing and monitoring these requirements.

Keeping a central and standardized source for cybersecurity excellence can help significantly in keeping track of and mitigating the many weak links that can exist in your supply chain. Combined with coordination and communication within the organization to ensure a robust SRM program, the centre of excellence can help mitigate risk throughout the organization.

Supplier Readiness and Collaboration

In the past, procurement was often seen as a transactional function—working on price and delivery terms, and creating and renewing contracts with suppliers. The focus was on cutting costs rather than seeking opportunities that generate value. Today, that has changed with the recognition of the value that SRM brings. Trust-based relationships with key strategic suppliers are resulting in significant strides in the area of supplier readiness and collaboration in the event of a breach. Proactively and strategically planning and managing critical interactions with key suppliers during and after a breach has occurred, helps gain significant advantage over cyber criminals and significantly reduces both the damages and the duration of down time.

Identification, communication and response

When an incident occurs, your vendor should have a plan in place to immediately inform you of the breach if it occurred at their end. They should work with you to address any breach-related issue in collaboration with your team.

You should understand and gain a high level of comfort with how they handle incident detection and response. As part of your SRM program, your organization can set itself up for a solid understanding of your supplier's ability to detect and respond by doing the following:

- ☐ Include a legal obligation in the contract to notify you in an event of an incident
- ☐ Review their Incident Management Plan (IMP) to ensure that it is comprehensive and includes intrusion protection tools, firewalls, anti-malware products, a patch management program and details for their incident response timeline and process
- ☐ Verify the vendor has cybersecurity insurance coverage as per your requirements
- ☐ Include strategic vendors (to the required extent) in scenario planning for breach response
- ☐ Conduct detailed debrief sessions to evaluate their performance in response to the breach and strive for continuous improvement

Conclusion

Technology often leads us into unchartered territory, with evolving opportunities and threats. As the threats evolve, so do cybersecurity trends—and SRM best practices need to keep up, with vendors playing a critical role in mitigating cyber risk. Effective SRM leads to major opportunities and savings for your organization, and can help you eliminate supply chain risk, improve supplier services and support and help improve customer and tenant experience.

It's important to not just start your SRM and cybersecurity journey, but ask yourself continuously how you are moving towards leading practices. While your strategy may be right for you today, it may not meet the needs of tomorrow, especially given the pace of technological change.

Acknowledgments

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

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

Scot Adams
National Services
Colliers International

Stephen Adams
General Manager
Cushman Wakefield Asset Service ULC

Trent Bester
Senior Vice President, Consulting and Public Sector
MNP

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

Nada Ebeid
Business Development Manager – Canada
Genetec

Sam Flis
Director, Property Technology
BentallGreenOak

Michael Di Grappa
Senior Vice-President, Property Management
Canderel

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

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

Victor Lauer-Martin
Information Security Architect
Ivanhoé Cambridge

Lachlan MacQuarrie
Vice President, National Programs
Oxford Properties Group

Kendall Peart
Managing Director, Real Estate
MARSH

David Sulston
Director, Security
Oxford Properties Group

Lee Thiessen
National Leader, Real Estate and Construction
MNP

Naveli Thomas
Director
Nyox

BOMA Canada team:

Benjamin Shinewald
President & CEO
BOMA Canada

Michael Parker & Natalie Rekai
Marketing and Communications Consultants
Citrus Creative

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

Ce rapport est disponible en français.

BOMA Canada
www.bomacanada.ca