BOMA Canada

Cyber Security Governance Guide

This Guide is Sponsored by:

MNP

Introduction

Dear friends,

BOMA Canada is pleased to present the fifth guide in our series on cybersecurity for building owners and managers. We seek to provide valuable education and tools to our members, and with cybersecurity becoming a growing area of concern in commercial real estate, this series is aimed at providing best practices 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 planning. The following year, the BOMA Canada Cybersecurity Guide – Procurement, delved into embedding cybersecurity practices and preventive measures into your procurement processes and procedures. The third guide took a deeper look into leveraging the role of supplier relationship management (SRM) in cybersecurity with the fourth guide aimed at helping you respond better if you face a breach. This fifth guide comes full circle by focusing on building a strong foundation through effective cyber security governance – from the management of your critical data through to clarity of the roles and responsibilities for effective cyber security.

How should this guide be used?

This guide is intended to introduce building managers and owners to the key elements and suggested steps for establishing effective cyber security governance. The guide is best used in conjunction with comprehensive cybersecurity planning, and follows our previous cybersecurity guides, so that readers can link dependent decisions about how they manage cyber security across their organizations. While it is intended to help you build a strong cyber security environment, it's not a complete strategy or standard on its own. This guide needs to be supplemented with further reading and adherence to specific standards or with the help of professionals. Establishing a governance framework that aligns with your organization's goals and objectives takes a coordinated and organization-wide collaborative effort including your leadership, your information technology (IT) department and resources, your team members and your external advisors.

We hope you find this guide useful and welcome your suggestions on future guides.

Sincerely,

Benjamin Shinewald
President & CEO,
BOMA Canada

Table of Contents

Acknowledgments

Stephen Adams	Cushman Wakefield
M Abdelsalam	Oxford Properties
Maria Aiello	Manulife
Trent Bester	MNP
Michael Chin	Triovest
John Chung	Quadreal Properties
Ron Cirillo	Oxford Properties
Trevor Cleveland	Colliers
Ben Cooper	BentallGreenOak
K Cowan	Morguard
Ken Dixon	
Obrey D'Souza	Morguard
Randal Froebelius	Equity ICI
Patrick Gilbert	Ivanhoe Cambridge
Heather Harms	MNP
Ryley Iverson	Colliers
Sue Klinner	First Capital
S Kurien	Morguard
Victor Lauer-Martin	Ivanhoe Cambridge
Kendall Peart	Marsh
Ruby Rai	Marsh
Bob Riddell	Riddell risk
David Sulston	Oxford Properties
Nada Sutic	Quadreal Properties
Martine Theriault	Canderel
Lee Thiessen	MNP
Bryan Borzykowski	ALLCAPS Content
Benjamin Shinewald	BOMA Canada
Krista Lachelt	BOMA Canada

Cyber Governance Landscape

In April 2021, one of the United States' largest property management firms sent off an email to hundreds of co-op and condominium boards containing the three words no building resident ever wants to read: "data security incident." That month, the firm noticed something suspicious with its IT systems – a subsequent investigation found that an unauthorized party somehow got access to its network, and potentially viewed, if not stole, tenant names, dates of birth, mailing addresses, social security numbers, driver's license numbers and more.

A few months earlier, a commercial real estate company was hit by a devastating ransomware attack – a type of cybersecurity breach where critical data is captured and then held until the subject of the attack pays a ransom for the data – with some people's personal information reportedly appearing on the dark web. While these two companies were hit with different types of attacks, both situations have at least one thing in common: neither had a data governance plan in place, a document that outlines everything from which employees can have access to personally identifiable information (PII) to what cybersecurity solutions should be put in place to how smart technology data is tracked and how that information gets stored.

Over the last few years, building owners and managers have gone from focusing on the spaces between their four walls to overseeing an ever-expanding amount of data, sophisticated cloud-based IT systems, smart building devices and more. Not surprisingly, as the real estate sector has become more connected, attacks on buildings have increased. According to Verizon, out of 29,207 cybersecurity incidents in the U.S. in 2021, 100 were in real estate (there's no comparable Canadian data), which may seem small, but it's a 170% increase in incidents over the year before. Those figures are only going to rise.

Combatting breaches takes a lot more than putting up firewalls and buying anti-virus software. It also requires owners and managers to think carefully about their business objectives, determine what data is most important to their operations, figure out who can have access to critical information, how often employees must change passwords and the list goes on. And it all needs to be codified in a governance document that employees, tenants and third-party vendors can access and understand.

Unfortunately, data governance hasn't been top of mind for most real estate operations. Many are still trying to figure out how to digitize their assets with Internet of Things sensors that collect the data they need to run more cost-effective, energy-efficient and operationally productive buildings. "Data governance has been an immature part of the real estate sector because a lot of these organizations have only recently started to outfit their facilities with sensors," says Eugene Ng, a cyber security partner with MNP. "But there's a lot more outsourcing of technology – you now have information flowing every which way to Sunday."

Too many companies think about governance too late – often after a breach or years after networks have been created and software has been installed. If your buildings have any network connectivity, which most do in some capacity today, there should be, at the very least, a short document that outlines the kinds of passwords that should be used to access company software and documentation around who can handle different types of data. If you're implementing new systems or thinking about digitizing assets, then those governance conversations should happen before or at least at the same time as your digital transformation. You need to ensure yours and your tenant's information is safeguarded and protected right from the start.

In this guide, we explore the concept of data and cybersecurity governance and explain how building owners and managers can create data and cyber governance plans of their own.

What is Governance?

Last January, Ben Cooper, a Vancouver-based smart technology expert, was hired by BentallGreenOak (BGO), to help them manage their growing property technology department. Soon after joining, Cooper noticed BGO didn't have a cybersecurity governance plan, which wasn't surprising because real estate hasn't historically been a tech-savvy sector where cyber is top of mind. "I had one conversation with a property manager who said why do we need cybersecurity? If someone breaks into our building, I'll just unplug the computer," he says. "This is typical – a lot of people who are in charge of these buildings aren't experienced in cyber." While it had some data governance documentation, if it wanted to add smart technology to its buildings, it needed a cybersecurity plan, too.

Governance is critical because it provides a roadmap for staff, third-party vendors and other stakeholders to follow around how data should be handled and protected and what cyber systems should be put in place. It should outline every process, procedure and risk and leave no room for interpretation. Cooper likens governance to a paved road – it's the smooth path a company must travel on if it wants to keep its systems safe from threats. Without a plan, you're essentially driving aimlessly on dirt roads that lead to nowhere.

Data and cybersecurity governance have always been important, but it's even more critical today with an increasing number of employees working from home and with more people changing jobs. "There's so much turnover at companies now and everyone wants to work hybrid," Cooper says. "So you need to have standardized processes that can keep a team on track, fill new people in and are ones that everyone can learn from and understand."

To Ng, governance "is really the management of your information security program," he says. The document, which accounts for every potential risk that could impact a company, puts guard rails in place to ensure these scenarios don't happen.

Without a governance guide, worst-case situations can – and do – happen. For example, in 2019, a large financial firm was subject to a massive data breach. For more than two years, an ill-intentioned employee stole social insurance numbers (SINs), email addresses, birthdates and full names of 2.9 million customers and reportedly sold that information to criminals. According to the Office of the Privacy Commissioner of Canada (OPC), the rogue staffer had limited access to this data, but other employees, in the course of their regular work, copied the information into a shared drive. "As a result, employees who would not usually have the required clearance or the need to access some of the confidential data were able to do so," wrote the OPC in a report. "While these practices violated the financial institution's policies, the technological measures in place to prevent these situations were lacking at the time of the breach."

Financial firms are the holy grail for hackers, given how much personal information they collect, but building owners and managers are responsible for an increasing amount of information, too. Many store bank account information and names, emails, and addresses of employees and customers. There are also contracts and pricing information they wouldn't want their competitors to get a hold of, while Internet-connected boilers, electrical systems and other mission-critical infrastructure could be controlled by nefarious individuals.

Building owners and operators don't just have to worry about their own data, either. With more smart tech in buildings, such as thermostats, lights, security cameras and even elevators, threat actors have more entry points to get into tenant networks and steal all kinds of customer information – data that has nothing to do with the building itself. "All of this underlying infrastructure requires some sort of connectivity and it's also giving people a lot more data to target," says Ng.

Get Your Governance Guide Started

How to go about creating cyber and data governance plans will be different for each business, but there's one thing everyone will do to start: open up a blank document, pull your chair up to your desk and start thinking about your business.

That's essentially what Cooper did when he began creating his company's cyber governance plan, which will serve an interim guide until a full smart tech governance strategy is developed. He opened a document on his computer, wrote the word cybersecurity in the middle and began writing down his thoughts. "I had a brainstorming session with myself," he says.

Cooper started with four words, which he says are the foundational elements of any cybersecurity plan: operations, vendor management, networks and standardization. Operations refers to the building itself, such as asset management, preventive maintenance and inventory. Vendor management is about third-party companies – ensuring they have incident response plans and there are regular audits of vendors, for instance. Networks involve securing the network itself, such as putting controls over who has remote access and what kinds of passwords people should create. Standardization is making sure everyone within the company is following the same processes across the entire organization, whether they're installing software, changing passwords or labelling wires. "You're making everything cookie cutter so if another property comes on board you can say, 'This is what we do,'" says Cooper.

While Cooper created this cybersecurity document together himself, a much broader group from BGO is starting to work on a larger governance guide that will encompass everything from data to vendor assessment, he says. Bringing in multiple people from across the organization to work together on governance is the

right approach, says Ruby Rai, Cyber Practice Leader, Canada at Marsh & McLennan Companies. It starts with the C-suite, she adds, which sets the tone for the whole organization and ensures accountability. A cross-functional team is also needed to ensure everyone is aligned on their priorities and individual roles. Include people from risk management, legal, human resources, finance and information security."You need multiple paths," she says. "It's not usually one person – it's a combination of roles."

Why so many people? Because everyone is responsible for a different aspect of the governance plan, she explains. Finance, for instance, will have to pay for new cybersecurity technology; risk may want to put insurance clauses into third-party contracts; HR will be responsible for ensuring employees follow governance policies; the CISO may be choosing new systems and so on.

Whoever's responsible, it's critical to have someone from both the business and IT sides at the table, explains Adriana Gliga-Belavic, a privacy and data governance partner with MNP. She's seen many situations where no one wants to take accountability for governance. The business side thinks it should fall under IT's purview, given they're the ones that have to protect systems, while the IT side says it's the business's responsibility to ensure the data it deems mission-critical remains safe.

Of course, though the responsibility falls on everyone, accountability must be clear. While IT will be the ones to put the many cybersecurity and data-collecting systems in place, it can't be up to them to know what information should be gathered or what data needs the most protection. The business side must tell IT what it wants to safeguard and then IT can help devise ways to keep data from falling into the wrong hands. "The business should be (accountable for) the data and they should be making the decisions on what to do with the data," says Gliga-Belavic. "IT knows how to manage IT systems, but they might not understand what data is important to the business. Do they care about pricing and the contracts? They cannot identify what data is important."

Key Steps to Creating a Governance Plan

As for the nitty-gritty of creating a plan, there are several steps you'll need to take and issues to consider as you get started.

1. Understand your business and your data

When it comes to data governance, it's impossible to safeguard every piece of information – nor do you need to. So what should you protect? Any business-critical information or PII that, if in the wrong hands, could negatively impact your business reputationally or financially. What exactly that will be will depend on your business objectives, which means the first place to start is to think carefully about the data you must protect and why you want to protect it.

Determining what to safeguard requires a clear understanding of your business objectives and how your company operates, says Gliga-Belavic – it's your goals and purpose that will guide you through this process. "I always say, start by understanding your business, the different lines of business and what information you're bringing into the organization," she says. "Then consider how data flows through your organization all the way to when that data is destroyed."

Once you have a handle on what you're collecting and what data's most important to the business, consider the risks of what could happen if information gets into the wrong hands. What happens if PII ends up on the dark web or if a contract gets stolen and sent to a competitor? Understanding the implications of a breach will impact how you protect your information, including what cyber technology and employee protections you put in place.

A lot of companies failed to think about these risks during the pandemic when staff started working from home, says Gliga-Belavic. "Many companies began interacting with customers and other staff through email rather than giving a piece of paper to a colleague, but nobody did an impact assessment to see what the risk would be for moving all that data into email," she says. "You need to understand all of your risks and what you could be exposing yourself to."

2. Classify your data

After you've mapped out all of the data you're collecting, you'll want to put each piece of information into one of three classifications, Gliga-Belavic explains. The first is public, which is usually the information on your website or in an annual report. "Anyone can go there and read it," she says. The second is confidential, which is data internal people can view. The third is restricted, which means only certain people within your organization can have access. This is the classification that human resource data, sensitive financial information or intellectual property typically fall into. These

classifications will help you determine what kinds of protections and controls to put in place. "Your restricted data will have the most controls in place," she says. "Then you'll need to define what are those controls and who has access?"

3. Assign ownership over data

A key part of this process is determining who's responsible for the data and making sure it's not only accurate but that governance policies are acted on. More companies, including real estate firms, are hiring chief data officers (CDOs) and making them accountable for information, which includes putting governance policies in place. Organizations that don't have CDOs often give the CIO this role, but different parts of a business, such as HR, legal and risk, will take ownership over various aspects of a data program, too. "Assign ownership over your data and understand your data environment," says Gliga-Belavic. "So, data maps, data flows and inventories – how are you going to keep all of that accurate going forward?"

4. Interview stakeholders

At some point, you'll need to start putting the document together. While a smaller governance group can do the work of identifying and classifying data, depending on the size of the business, you'll also want to interview various stakeholders to see how they're using, accessing, storing and managing information. The committee, or whoever is writing the document, will want to get a good handle on how people work, the ways in which they access information, the processes they take to save or ingest data into a system and the technology that's currently being used to both protect networks from a hack and software that collects data. In some cases, companies involve upwards of 100 people if not more in this process, says Ng.

5. Start writing

Once you've gathered enough information to create a cyber governance plan, you'll want to start writing. For Cooper, the process didn't take long – he spent a few days putting a nine-page document together, but for others it could take months of work resulting in hundreds of pages. "This is not typically short-term," says Ng. "It can take months if not years to design and then also implement certain controls."

6. Be aware of rules and regulations

As you're working on cyber governance plans, make sure you're well versed in the latest privacy-related rules and regulations, so you're incorporating any protections that may be required by law. While Canada doesn't yet have anything as robust as the European Union's General Data Protection Regulation, which outlines numerous rules around how people's personal information can be used and stored, it does have 28 federal, provincial and territorial statutes that govern the protection of PII.

Canada also has the Personal Information Protection and Electronic Documents Act (PIPEDA), which governs how organizations collect and use PII in the course of business. In mid-June the government introduced Bill C-27, which would give Canadians far more control over how companies use people's personal data. It's the first major privacy-related policy update in years and something all companies should have on their radars.

Buildings, however, come with different kinds of data, which don't easily fit into the current regulations. "Privacy protection is a real requirement right now and a lot of people are struggling with how to manage the information they're gathering from sources like automated billing systems and security solutions that can track movements within an environment, among other things," says Stephen Adams, a general manager with Cushman & Wakefield. "It goes back to who is responsible for managing and protecting data."

Understanding Roles and Responsibilities

While a governance committee itself should be made up of a cross-section of people within an organization, different people will have different roles to play when it comes to overseeing and implementing policies.

CEO	You'll never implement a governance plan if you don't get buy-in from the CEO. Indeed, their first responsibility is to greenlight the creation of a policy and get everyone else on board to support it. But they're also responsible for putting the right talent in place to carry policies out, says Rai, whether that's hiring a CISO, a CIO, cyber security experts or others who will be needed to keep their company safe, not only for existing threats but for an emerging and future threat landscape, too. The CEO, especially if they're running a public company, will have to report to the board and brief them on governance issues more broadly, but also keep them up to date on the progress of the plan itself, says Rai.
Corporate Board	As for the board, it's responsible for making sure the CEO, and the company, is performing in the best interests of its shareholders and other stakeholders. Because of that, board members need to be aware of the damage a breach could cause and give the CEO the support and resources they need to protect the organization from an attack. Bob Riddell, president and founder of Riddell Risk Management and the founding chair of BOMA Toronto's Security and Risk Management Advisory Council from 2012 until 2022, says that while some corporate boards may still have an unsophisticated approach to the governance of cybersecurity issues, commercial real estate sector boards are now far more aware of cyber risks. "They're finally seeing that this isn't something that happens to somebody else, but that it could potentially happen to them," he says. "That's when you start seeing investments being made." "They're finally seeing that this isn't something that happens to somebody else, but that it could potentially happen to them," he says. "That's when you start seeing investments being made."
CFO	The CFO, and the rest of the finance function, is responsible for assessing the financial risks associated with a breach and ensuring the company has the money it needs to invest in a cybersecurity plan. One of the CFO's first duties will be to help prioritize what data is most sensitive from a financial perspective – they can determine what losses might arise from stolen data and see how any reputational hits could impact earnings, for instance. Finance is also responsible for setting and approving new cybersecurity budgets and purchases.

Human Resources	People are often the first line of defence when it comes to cybersecurity, which means human resources leaders have an integral role to play in creating governance plans, says Rai. They can help review onboarding processes, workflows and how staffing requirements might evolve with additional governance needs. They can also help educate employees on how to follow policies. “Make sure cyber and data protection are part of an onboarding program,” says Gliga-Belavic. “You also need to train people who have the most restricted access on how to handle restricted data.
Risk and Legal	The risk and legal functions also have important roles to play. The former will need to be involved in any decision-making related to how best to protect your business from a risk event. They can also help identify risks that could arise and they may be the ones to suggest what kind of cyber insurance to purchase. Legal will want to review any third-party contracts and include language that aligns with governance policies. They'll also be involved in any discussions around the legal issues that could arise from an attack, says Rai.

Measure your Policy's Success

After a policy is created and disseminated – education is a key part of this process and can be done through workshops, annual training and regular tests, such as sending a fake email to staff to see if they click on a link – you'll want to measure its success. At Cushman & Wakefield, success relates to how many people were blocked from hacking into a system, says Adams. "That conversation would be based on how many people have attempted to probe our security systems," he says. "How many people were successful? No news would be good news."

Ng suggests looking at similar metrics, including how many people in an organization clicked on a malicious link and how many of those links were prevented from reaching staff. But there are other metrics to consider, too, such as how quickly vulnerabilities are remediated within the organization and how effective training has been in raising awareness of phishing and other scams.

Companies should create what Gliga-Belavic calls a measuring matrix to determine whether policies are working. It would include a host of KPIs and other metrics, such as whether someone sent an email to the wrong person, if breaches declined after implementing an education program, if people tried to view data they didn't have access to and so on. You'll also want to conduct audits to see if procedures and processes have changed over time and if third-party vendors are following and implementing your policies.

Cooper's cybersecurity policy has only recently been created, but he plans on measuring success through audits. He's created an Excel-based survey that will be distributed to various parts of the business to assess whether their system is at risk of an attack. The survey asks 18 questions, including whether there are firewalls in place, if cables are labelled and whether a building automation system connects to the internet. The person responsible will answer yes or no to each question and then

receive a score that indicates whether a system is at a major, moderate or minimal of a breach. Once the assessment is done, Copper will enter it into a report and offer recommendations for improvement. He then plans to check each site every quarter to see if his recommendations have been implemented. "It's not just cybersecurity incidents either," he says. "We want to make sure all sensors are in place, that people are changing their passwords, that serial numbers match up with what's been installed, that Windows has been updated."

While building owners and operators are only now starting to create governance policies – Adams says many industry players are relying on BOMA Canada's guidance when it comes to how governance plans should be created – companies are increasingly eager to put cyber and data protections in place. At the start of the pandemic, a lot of companies sent staff home and started sharing sensitive documents over email or allowing staff to access company files over their home network. While business continuity was important, many operations now realize they may have put their organization at risk. "Companies moved very quickly to adapt applications and systems," says Ng. "We're going to start to see people saying, 'We moved really fast, now we got to figure out where all this stuff is.'"

Add to that threat actors becoming ever more sophisticated and data becoming more integral to a company's operations, and now's the time for businesses to codify processes and procedures around how information is handled and gathered and what cybersecurity measures must be followed. "Whether it's increasing reliance on third-party cloud solutions or more data being generated from sensors, these risks are not going anywhere," he notes. "Commercial real estate companies need to take a hard look at what they're doing and how they're protecting themselves."

Cyber Security Governance Guide

For further information about the guide, please contact:

BOMA Canada
1 Dundas Street West, Toronto
Ontario, Canada M5G 1Z3

info@bomacanada.ca

September 2022

Ce rapport est disponible en français.

BOMA Canada
www.bomacanada.ca