Cyber Incident Response Guide

For further information about the guide, please contact:

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

info@bomacanada.ca

BOMA Canada
www.bomacanada.ca

BOMA Canada

2022 Cyber Incident Response Guide

Continually evolving, cybersecurity incidents have become more aggressive and frequent.

This Guide is Sponsored by:

MNP FIRST CAPITAL QuadReal Canderel

Cyber Incident Response Guide

Introduction

Dear friends,

BOMA Canada is pleased to present the fourth guide in our knowledge 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 and residential buildings, this series is aimed at providing guidance 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 cybersecurity threats becoming more aggressive and sophisticated, it is likely that most organizations will be breached at some point despite planning and putting checks and balances in place. This fourth guide is aimed at helping you respond better if you face a breach.

How should this guide be used?

This guide is intended to introduce building managers and owners to the key elements of responding to cybersecurity incidents in ways that help reduce its negative impacts and expedite your recovery should you have a breach.

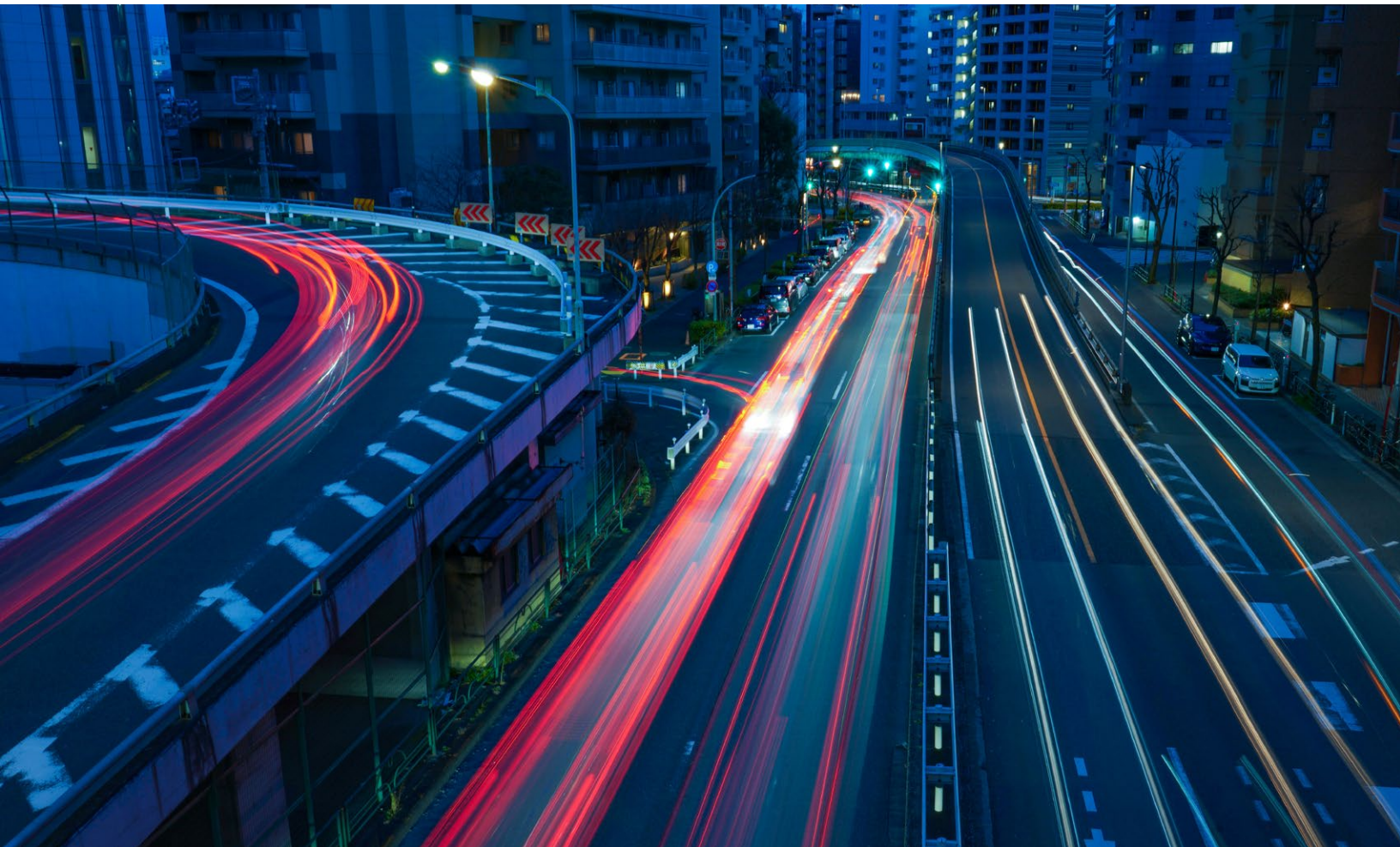
This guide is best used in conjunction with comprehensive cybersecurity planning, and follows our previous cybersecurity guides, so that readers can link dependent decisions about how they manage their response to a threat. While it is intended to help you respond better, it's not a complete strategy or standard on its own, and needs to be supplemented with further reading and adherence to specific standards, or the help of professionals, to respond effectively. Responding to a breach takes a coordinated and organization-wide collaborative effort including your leadership, your information technology (IT) department and resources, your team members and 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



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

Understanding the true impact of a cybersecurity breach

Cybersecurity threats have been continually evolving and becoming more aggressive and frequent. It is typically not a matter on whether an organization will be breached, it is more a matter of when the organization will be breached and how well prepared it is to deal with the incident.

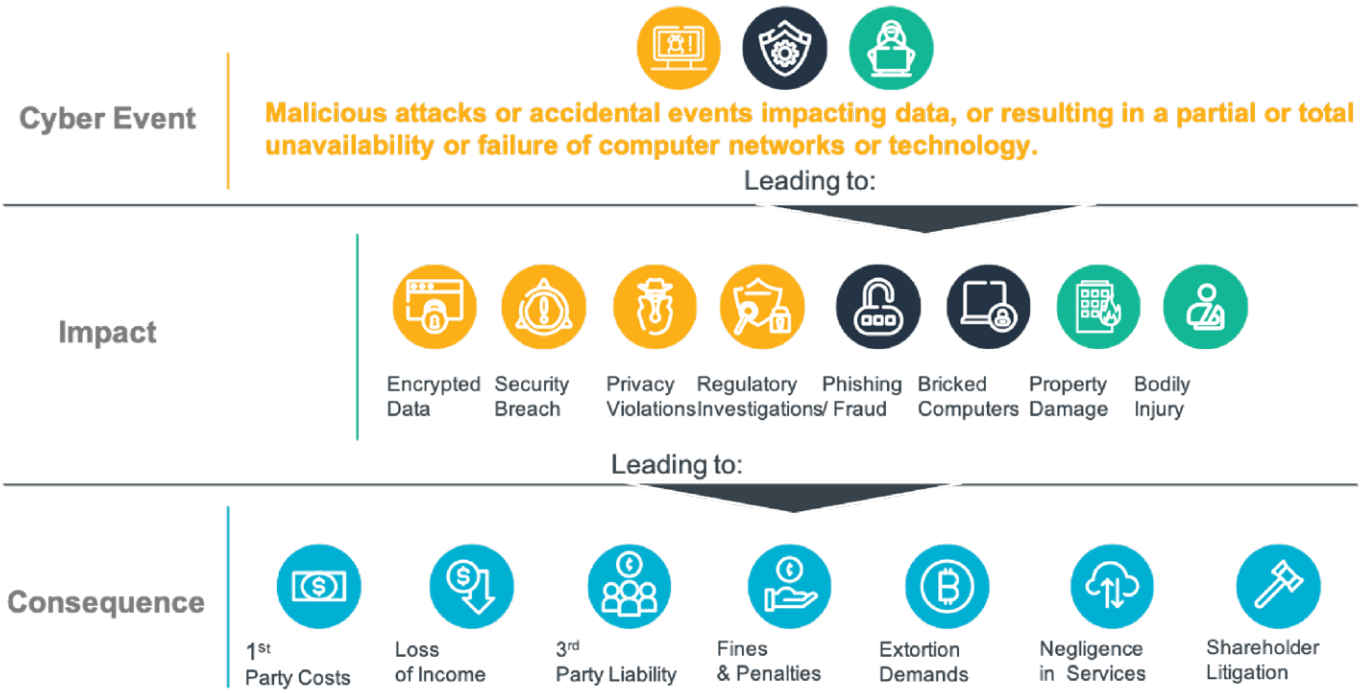
Attacks are reported to have increased even more during the COVID-19 pandemic. Ransomware incidents alone for example have increase 2.4 times year-over-year as of the third quarter of 2020 (Source: Marsh JLT).

In our previous guides, we explored strategies and tactics to plan and prepare to reduce the risk of cybersecurity incidents, and strengthen security posture to reduce the damage if an incident occurs. We also delved into managing one of the major sources of risk—weak links caused by third-party vendors embedded throughout an organization's value chain. The goal behind that preparation is to put safeguards in place to either prevent or make it as difficult as possible for hackers to gain access to your critical systems and data, avoiding or mitigating the impact of what can be a very severe and costly outcome for an organization.

The impact that a cybersecurity breach can have on an organization can be very significant, and recovering from the attack can take a lot of time, money and resources. Breach impacts can range from business interruption, loss of customer confidence, brand and reputational damage, actual hard costs to respond and recover, and most critically, the safety of people in a building. The combined impacts and costs of cybersecurity incidents can quickly add up.

IBM, in its Cost of a Data Breach Report 2020, has estimated that on average, a breach in the United States costs an organization US$3.86 million. Minimizing the impact to your organization and reducing the cost or loss of revenue is vital and is highly dependent upon the thoroughness of your response to the incident.

Consequences of a cyber incident



Having a plan: Your playbook for response and recovery

The cyber risk environment for commercial buildings can be high. Buildings typically store sensitive tenant information and are dependent on critical systems such as elevators, HVAC and building security that today are likely internet-connected. A breach could lead to safety issues or loss of vital tenant information, not to mention the possibility of compromising a building's own operational data and functional capabilities.

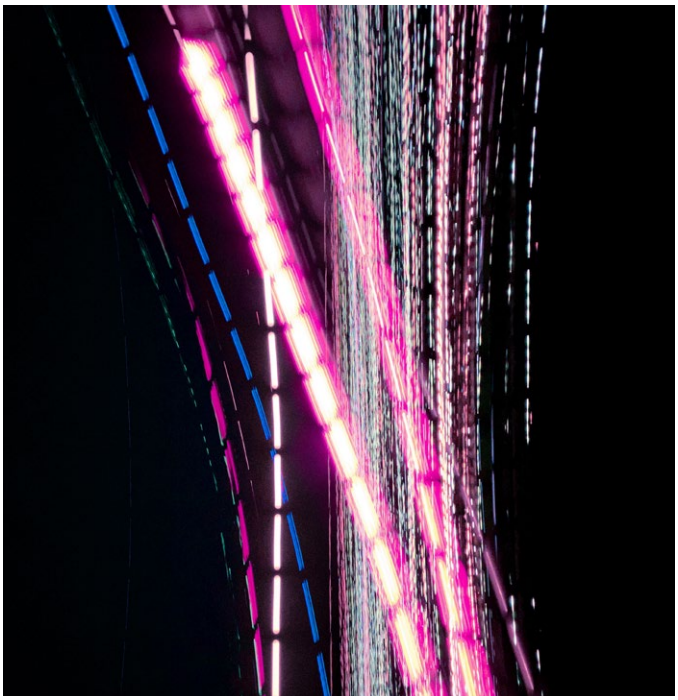
It is important to remember that the most difficult time to plan a response to an incident is when it is actually happening. Having a plan in advance which guides your actions when you are hit with a breach, will expedite dealing with the breach and mitigate its impact.

In our previous guides, we have discussed building a plan in detail, working with third-party vendors and securing your supply chain, all with the intent of reducing the likelihood of a cybersecurity incident, and being prepared to minimize damage if you are breached. While we recommend reading our other guides to be better prepared, some quick pointers from the previous guides are provided below:

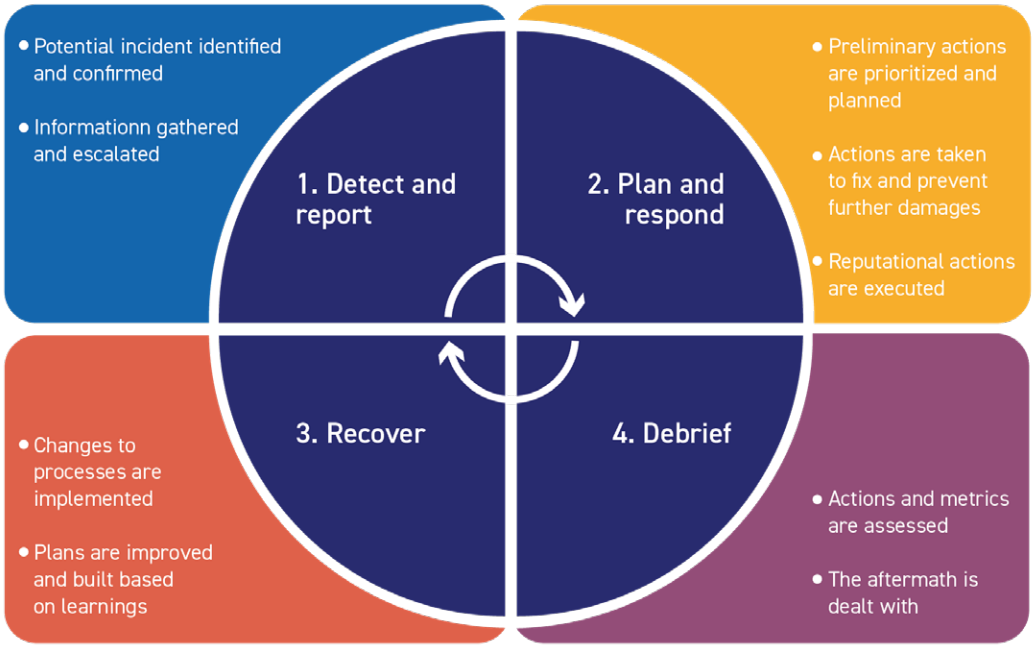
- Know which systems are connected to the Internet, who has access and how access is secured.
- Have protocols in place for procuring and onboarding new technology.
- Provide an ongoing cybersecurity training program to all levels across the organizatio At a minimum, standard cyber-hygiene training can be a critical factor in reducing breaches, and in identifying them quickly if one does occur.
- Identify third-party risk levels, and work with your vendors on cybersecurity practices, including building key elements into your contracts and procurement.
- Build a response team that includes both internal and external experts, including those that specialize in cybersecurity, who will come together to deal with a breach – this team should be ready to mobilize immediately, don't wait for an incident to assemble your response team
- Have an incident command structure with clear roles and responsibilities, including your leadership team or corporate office for key decision making and your onsite team for executing tactical, property level tasks.
- Consider getting the right cybersecurity insurance and fully understand what your insurance provider can contribute in the even of a breach.
- Test your plan through tabletop exercises, planning responses for different types of breaches and helping team members understand their roles.
- Keep your plan current as the threat landscape evolves.

You can read further on building your playbook in our previous guides:

1. *Addressing cyber risks in commercial real estate building operations*
2. *Embedding cybersecurity in procurement*
3. *The role of Supplier Relationship Management (SRM) in cybersecurity*



If you have been breached: Lifecycle of your response



1. Detect and report

Have you been breached?

There are some obvious signs of unauthorized breach of systems that building owners and managers can look out for.

Some more obvious signs include:

- Encrypted files appearing on corporate file shares
- Employees unable to access applications to perform daily tasks
- System operators being unable to access operational systems
- Ransomware notes being printed out on office printers or appearing on user screens
- Complete systems have been rendered inactive or not available such as access systems, lighting, escalators, or climate controls
- Reports of confidential information belonging to the organization made available on the Internet
- Reports from suppliers, customers, or partners not receiving their expected goods, payment, or services
- Defacement or takeover of corporate websites and other social media services such as Twitter or Facebook

Other indicators are more subtle and harder to detect immediately. Here is what they could look like:

- Seeing increasing delayed responses from normally respondent systems
- Usually reliable operational systems breaking down more often
- Increase in replacement of failed parts or systems for no apparent reason other than overuse
- Abnormal network activity and increased Internet traffic
- Sudden or inexplicable revenue loss on fee-based systems such as parking or facility usage meters

- The statistics from systems being inconsistent when compared with manual human sampling

Quite often the actual breach of systems happens long before some of the more obvious signs of the breach appear. If you observe any signs, obvious or subtle, it's important to act immediately to confirm the cybersecurity incident. Then, the response process and steps that are outlined in the next section can serve as a guide for you.

2. Plan and respond

Remain calm

Dealing with the situation demands a calm approach. You are not alone, and every organization has—or will—experience any number of cyber incidents. It is how the organization deals with each incident that will either safeguard or jeopardize its reputation with customers. With a level head and deliberate actions, first triage the situation. Quite often, you may not immediately know the full extent of the incident, so it's important to first mobilize your response team, involve your internal IT and operational technology (OT) resources, and engage an expert cybersecurity response advisor. If you do not have internal cyber response expertise, it is important to have an expert on standby rather than waiting for an incident to source this expertise.

Establish roles and responsibilities

Every single person as part of the organization has a key role to fulfill even if it is to remain calm, leave the premises, and not to communicate anything to anyone. Even if you have an IT and/or OT department, they will be instrumental in your response but all levels of the organization will play a part in your response.

Before an incident, everyone from the Owner/Operator, Board Chair and CEO/President, to the administrative staff should know their responsibilities and roles for any cyber incident. These can be developed and matured within a cybersecurity incident response plan. In the absence of a specific cyber incident response plan, you may not necessarily have to reinvent the wheel, by ensuring that your response aligns with an existing disaster recovery or business continuity plan, if you have one.

The key is to have a coordinated plan based on already established roles, and a plan that engages both appropriate internal resources and external expertise. These should ideally be people who understand your systems, have the expertise to address and respond to the various aspects of a cyber attack, and are ready to respond immediately as needed.

Workstreams to deal with a breach

There are several accepted frameworks when dealing with an incident, with each referring to the same overlapping workstreams. Regardless of the specific wording in different frameworks, each incident contains the following workstreams.

Visibility and Containment: This team works on getting as much visibility with each system and device to determine the extent of the incident, and once known, works to contain the issue through various means such as disabling access or the Internet, or moving the system offline.

Root Cause Investigation: This team focuses solely on investigating how the threat actor was able to breach the organization's system. This may include forensics.

Remediation: This team has the onerous and arduous actions of restoring the systems, ensuring that additional security protocols are in place, testing, and bringing each system back online.

Resilience: This is a growing but critically important workstream that must be built, given the number of legal cases and class action lawsuits brought forth today. This team builds the archives of all evidence, actions, and results, to ensure that it can be replayed to address any future claims.

Engage your cyber insurance provider

If your organization is covered by cyber insurance, refer to the policy for incident reporting requirements, and look to access assistance on cyber incident response, and cyber crisis communication.

Understanding incident reporting and approval requirement under your cyber insurance is an important step and should be understood prior to an incident. In order for the insurance policy to provide coverage, insurer consent and approval is required for all costs incurred in managing a cyber incident. For example, investigating an active threat or malware in your systems requires engaging external security forensic investigators. It is important to understand if the external firm has been approved by the insurer or what pre-approved external

firms are available to engage. Another example is that insurer consent is needed prior to payment of ransom demand or a breach coach (privacy lawyer).

In Appendix A, we have included some additional information on what cyber coverage typically includes, and what underwriters may be looking for.

Understand the nature and intent of the breach

In trying to understand where to look first, it's important to be aware of what the most common aspects to look for are, so you can start with a focused approach. As per IBM's Cost of a Data Breach Report 2020, there are typically three main causes of a breach for an organization: 23% can be attributed to human error, 25% is due to a system glitch, and with no surprise, deliberate, malicious cyberattacks are responsible for 52% of surveyed data breaches.

Of these malicious attacks, the most common methods include:

- Compromised credentials: Bad/weak passwords, or passwords already available from previous breaches – **19%**
- Cloud misconfiguration: Examples include weak Office365 or Amazon Web Services security control implementations – **19%**
- Vulnerable third-party software: Examples include the recent Solarwinds Orion software vulnerability – **16%**
- Phishing – **14%**
- Physical Security Compromise – **10%**
- Malicious or Disgruntled Insider – **7%**
- Social Engineering – **8%**

By far, the goal of threat actors is to first exfiltrate customers' personally identifiable information (PII) with the second goal being getting intellectual property (IP).

With any breach, a sophisticated threat actor or hacker will focus on the following goals:

- Obtain unauthorized access to as many systems as possible
- Increase their level of access to as many systems as possible, and gain administrative rights or privileges
- Remove the ability for any other users to access these same systems
- Install additional access methods to increase their ability to re-enter the systems as long as possible
- Exfiltrate as much sensitive data as possible
- Encrypt the data and any available backups
- Render critical infrastructure (CI), Operational Technology (OT), Industrial Control Systems (ICS) inoperable

Once some or all the above goals are met, the threat actors then focus on monetizing their gains by implementing the usual ransomware methods. Other threat actors may focus less on the ransomware aspect, but intentionally use social media to damage the reputation of the organization or to make political, religious, or environmental statements. Keep in mind that it is possible to have employees or vendors infiltrate systems deliberately, and you could be facing a breach orchestrated by a trusted individual who knows the systems.

It is important to try and understand the motives of the hacker and what they may be seeking, so you can prioritize where you look and how you block access. Isolating or moving systems offline may be required based on what you find.

Identify the severity of the breach

The building management, or your head office IT/OT if applicable, needs to have a risk-based approach in categorizing the level of the breach. One type of breach deemed critical to one organization is not always the same for another. It would depend on where the most critical information and safety of your building lie. However, commonly acceptable groupings include:

Critical: Where the safety of people is at risk, either through inaccessible elevators, building management systems, access card systems or others.

High Severity: Where sensitive data is deliberately exfiltrated, or access is granted to unauthorized systems.

Medium Severity: Where data may be encrypted and statistical data is available to unauthorized users.

Low Severity: Examples include web site defacement or parking access mechanisms that have been bypassed.

The severity may decide who you bring in and what actions you take first. For example, if life safety is at risk, you must act immediately to ensure the safety of your employees and tenants, and bring in the necessary professionals or public emergency services.

Engage external professionals

To contain the situation and minimize its impact on your building or organization, it is advisable to call in experts who deal with cybersecurity breaches on a regular basis. They typically know what to look for, how to prioritize and respond based on the type of breach and can apply the latest industry practices.

Professionals may include those in the fields of cybersecurity, legal, forensics, physical security in cases of life safety, and insurance and communications/ public relations. It is recommended that you have these individuals identified and have pre-negotiated service level agreements (SLAs) as part of your pre-developed cyber response plan.

Establish the 'war room'

There needs to be a central repository of actions and information exchange along with a platform for discussion and exchange of ideas and critical updates. During the COVID-19 pandemic, these have now typically become 24/7 virtual chat rooms where each reporting party gives their updates. It is important for an organization to ensure these are available at a moment's notice and not dependent on the existing corporate infrastructure in case it is compromised.

Establish communication protocols

What needs to be communicated, to whom, and when, are all critical aspects of dealing with a crisis such as this. Building this protocol based on your building or organization's situation is critical, as is ensuring that all the people and parties working on the response team understand the protocol too.

The important role of logs and backups in dealing with a breach

Often, when you ask a cybersecurity response expert what the one thing that an organization must do to deal with an incident is, they will say it is usually the logs and backups. While preparation and practice are obvious candidates, from a technical perspective, it is the logs and backups that can help save an organization's reputation.

Optimized logs from multiple systems can quickly facilitate the investigation and provide a critical record of what the threat actor's actions were to build the defensibility of the incident. The absence of logs forces the organization to accept the worst case scenario and therefore increases the effort and resources required to remediate.

Backups—especially clean, valid ones—have saved organizations a significant amount of money and work when it comes to dealing with cybersecurity incidents.

3. Recover

Once the immediate situation has been dealt with, it is time for the organization to focus on recovery.

Understand full extent of the attack

After dealing with the urgent aspects of the response, it is important to analyze and build a thorough inventory of all the systems and information that was affected. This will help in identifying improvement opportunities.

Build and implement a recovery plan

Once the inventory has been built, recovery and remediation should be ensured for each system and asset. It is best to check and double check that everything is now secure, backed up and fully recovered.

Improve security monitoring and controls

Whatever caused the breach, or allowed it to affect more systems, would have been identified during the response investigation. Review the monitoring and controls that allowed the lapse and fortify them if needed.

The human element

Through a crisis, there is always a human element that suffers. Often, the person or people who unwittingly were initially breached may need support. Whether there was a lapse, their account was hacked or their laptop stolen, the building management should have a plan to reassure the victim that today, the sophistication of these attacks fools the most knowledgeable of people. Some of the best handled incidents ensure that all staff and responders feel fully supported by the organization.

The IT/OT resources and response team typically work long and difficult hours during a crisis such as this. Any critical incident may take weeks to contain, months to remediate, and years to recover. Management typically communicates with stakeholders, regulators, and tenants to provide assurances. However, it's also important to ensure the wellbeing of employees who worked through the crisis, and remind them to rest, organize replacement shifts for them, provide food and transportation support, and bring in mental health support workers if needed.

Informing external authorities or agencies

In the aftermath of a cybersecurity incident, you face a decision on whether to inform external agencies or authorities. Often, there is hesitancy in informing the police of a cybercrime, unlike other crimes that have taken place, in part due to how cybersecurity breaches have come to be viewed. It is important to consult legal counsel and also verify whether there is any obligation or requirement to inform authorities in your jurisdiction.

There may not be an obligation to inform authorities, unless any external parties' information was accessed or there is any threat to physical security. Then the decision rests with the management and leadership of your organization, in consultation with cybersecurity experts and legal counsel. While it may not be necessary to inform or share information with the police or any external agency, there may be some value in sharing it with national cybersecurity agencies, giving only the information you are comfortable with, so that collectively, more knowledge is shared and gained. One such agency is the Canadian Cyber Threat Exchange (CCTX).

Keep in mind that there is always risk to your brand and reputation, and a potential of liability with any failure to communicate a cyberthreat that could reasonably have been foreseen to cause harm or damage to third parties, especially the public.

4. Debrief

Debriefing is a critical component in bolstering your building for the long term. It may be a matter of time before someone tries to breach your building or systems again. The learnings you embed and the gaps you bridge will help you come out on top of future attacks.

Understanding the root cause

Once the incident has been dealt with, it is important to get deeper into understanding the root cause. Earlier, you would have detected what systems were breached, and by now you would have recovered those systems. During the debrief phase, it is important to understand what systems and processes in your own organization may have reduced the risk of the incident. Was it inadequate

training, third-party risk management, password protocols, cybersecurity built into systems or something else entirely? It could be a combination of multiple things too. Identifying weak links will help you know what to strengthen.

Identify the true losses from the incident

The losses from the incident may not just be the immediate costs that you can identify. They may be more indirect, such as lack of trust or eventual move of a tenant. Identifying and understanding the deeper picture may be critical in helping you determine the true loss you incurred.

Develop and execute an investment plan

Based on what you uncover while analyzing the root cause, building or strengthening your investment plan for cybersecurity operations and awareness may be necessary. Identify the weaker areas, prioritize gaps based on criticality and then plan your investment in ways that will help you the most.

Revise and build your cybersecurity plan

If you didn't have a cybersecurity plan before you were breached, it is time to create one now based on your learnings. If you already had a plan, revising it and changing it based on your learnings is highly recommended. Cybersecurity threats are constantly evolving, and your plan must too.

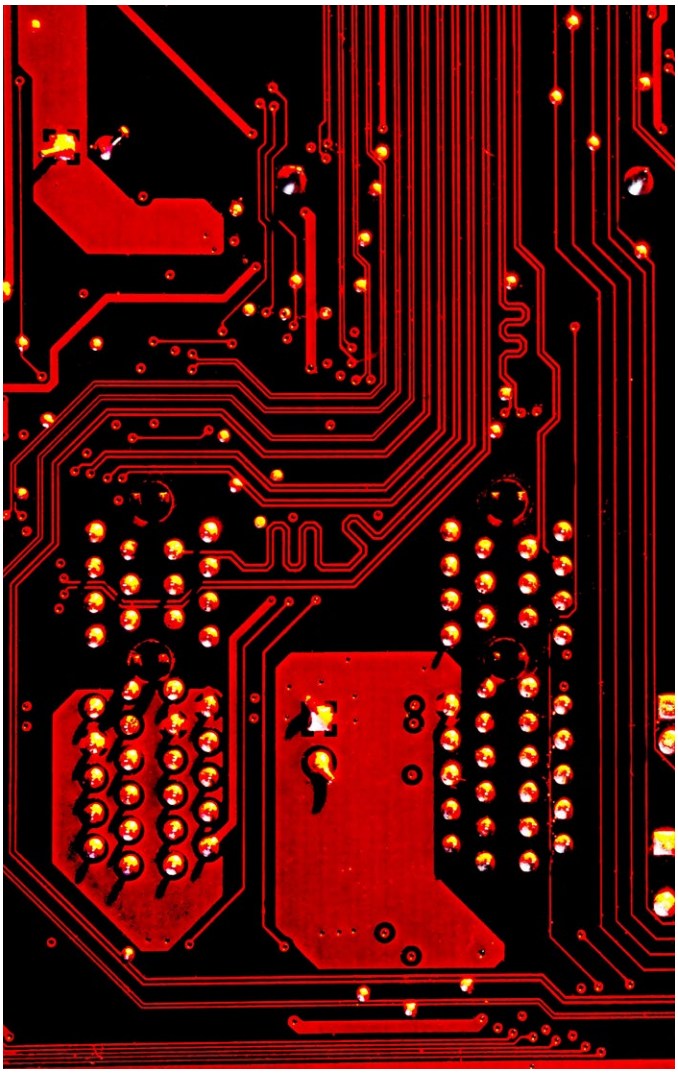
Establishing a culture of cybersecurity—from training to regular communication

Today, it's essential for an organization to live and breathe cybersecurity and make it common for staff to think of cybersecurity risks in all the work they undertake. That can bolster the building's defence and leave far less room for errors and oversight that lead to a breach or let it go unchecked. Regular training and communication is essential in building a culture that will protect you on a sustained basis.

Conclusion

Cybersecurity threats are evolving at a rapid pace and becoming more targeted and adept at finding gaps. Having a robust cybersecurity plan for your buildings is critical and must evolve with the threats. It is important to think of your cybersecurity approach as a marathon, that needs to keep moving and evolving, rather than a sprint that ends soon and is a one-time exercise.

Having a well-prepared team that you can bring together very quickly when needed is critical in controlling and managing your risks. If you have been breached, once you have dealt with the immediate response and started on a path of recovery, debriefing and strengthening your cybersecurity plans and systems is critical.



Appendix A: What underwriters are looking for – 12 key controls *(Courtesy: Marsh JLT Specialty)*

While these 12 controls are essentially what underwriters may be looking for, centralized risk management and insurance would also benefit from these controls. For real estate organizations where the operations may include property management or building management systems, a centralized risk management structure needs to be demonstrated.

It is typical to have multiple entities responsible for management of specific services or operations, however when it comes to data privacy or information security, one group or stakeholder needs to create a cohesive cybersecurity framework. A fragmented approach and not having a clear line of reporting is viewed negatively from an underwriting perspective.

1. MFA-controlled access
There are 15 billion stolen credentials on the dark web – a 300% increase since 2018*. Multi-factor Authentication (MFA) prevents attackers from effectively using them without this additional factor. Remote working has put MFA at the forefront to secure access to critical systems and sensitive data.

2. Secured and tested backups

Attackers are looking to delete backups prior to launching a ransomware attack launch so they can successfully cripple and extort their victims. It is essential to secure backups through encryption and isolation from the network (offline or MFA-controlled access), as well as regularly test backups and recovery plans.

3. Managed vulnerabilities

Regular vulnerability scans and annual penetration testing simulate cyber attacks on the network.
Such actions allow organization to uncover existing vulnerabilities and remediate before threat actors have a chance to exploit them.

4. Filtered emails and web content

Malicious links and files are still the primary way to insert ransomware, steal passwords, and eventually access critical systems. Today's first line of defense includes indispensable technologies to filter incoming emails, block malicious sites or downloads, and test suspicious content in a secure "sandbox" environment.

5. Patched systems and applications

Unpatched vulnerabilities remain a leading cause of intrusions into systems. Hundreds of vulnerabilities are revealed every month for multiple applications and systems. When technology environments are not patched in a timely fashion, attackers will seek to exploit their vulnerabilities.

6. Protected privileged accounts

Privileged accounts are the keys of a network. When attackers compromise these accounts, the likelihood of causing significant harm is extremely high. Limiting the number of privileged accounts, using strong password security practices/vaults, MFA, and monitoring these accounts is critical to network security.

7. Prepared and tested incident response plans

An up-to-date incident response plan with a trained team provides efficiency, speed, and quality in response to cyber incidents. When combined with backups and business continuity plans, it significantly helps to mitigate the impacts on operations and your organization's reputation, thereby limiting overall costs.

8. Protected network

All breached organizations used firewalls to protect their networks - but the technology is often underutilized or outdated. Now is the time to ensure efficient firewall and other technologies are in place with well defined rules; leverage network segmentation, intrusion detection and prevention systems, data leak prevention systems, etc.

9. Secured endpoints

Advanced anti-malware solutions on workstations, servers, and mobile devices detect malicious programs and contain their spread. Technology allows organizations to remotely respond to attacks and even prevent data leakage. The time when simple anti-virus was good enough is behind us.

10. Phishing-aware workforce

Recently, attackers took advantage of COVID-19 as a guise to spread ransomware. There will always be environmental factors that attackers can exploit to deceive people. Training and phishing campaigns help ensure people remain aware and vigilant.

11. Logged and monitored network

Logging and monitoring network activities allows organization to identify something possibly harmful might be happening. And attackers actions can be detected and contained at an early stage. Automated technology combined with operators monitoring is needed to watch network events or anomalous behavior of users.

12. Hardened device configuration

Attackers exploit default device settings or misconfigurations. Defining security baselines to harden devices, continuously managing secure configurations and change control processes is essential to preventing attackers from reaching their target.

Appendix B: Understanding cyber insurance

(Courtesy: Marsh JLT Specialty)

Cyber coverage parts

First-party coverages

First-party cover First-party insurance coverage: Direct loss and out of pocket expense incurred by insured	Description	Covered Costs
Business Income/Extra Expense	Interruption or suspension of computer systems due to a network security breach. Coverage may be added to include system failure and can extend to contingent businesses.	• Loss of Income • Costs in excess of normal operating expenses required to restore systems • Dependent business interruption • Forensic expenses
Data Asset Protection	Costs to restore, recreate, or recollect your data and other intangible assets that are corrupted or destroyed.	• Restoration of corrupted data • Vendor costs to recreate lost data
Event Management/ Breach Response	Costs resulting from a network security or privacy breach.	• Forensics • Notification • Credit Monitoring • Call Center • Public Relations
Cyber Extortion	Network or data compromised if ransom not paid.	• Forensics • Investigation • Negotiations and payments of ransoms demanded

Appendix B: Understanding cyber insurance

(Courtesy: Marsh JLT Specialty)

Cyber coverage parts

Third-party coverages

Third-party cover Third-party insurance coverage: Defense and liability incurred due to alleged harm caused to others by the insured.	**Description**	**Covered Costs**
Privacy Liability	Failure to prevent unauthorized access, disclosure or collection, or failure of others to whom you have entrusted such information, for not properly notifying of a privacy breach.	• Liability and defense • Bank lawsuits • Consumer lawsuits
Network Security Liability	Failure of system security to prevent or mitigate a computer attack. Failure of system security includes failure of written policies and procedures addressing technology use.	• Liability and defense
Privacy Regulatory Defense Costs & PCI Fines & Penalties	Privacy breach and related fines or penalties assessed by Regulators.	• Liability and defense • Investigation by a regulator • Prep costs to testify before regulators • PCI / PHI fines and penalties
Media Liability	Defense and liability for, including but not limited to, libel, slander, product disparagement, misappropriation of name or likeness, plagiarism, copyright infringement, etc.	• Liability and defense

Aknowledgements

We are grateful for the financial support of MNP LLP, First Capital Real Estate Investment Trust, QuadReal Property Group, Canderel Inc. and the expertise provided by MNP LLP.

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

Stephen Adams
General Manager
Cushman Wakefield Asset Service ULC

Maria Andonovsky
Director, Operational Excellence
BentallGreenOak

Trent Bester
Senior Vice President, Consulting and Public Sector
MNP

John Chung
Vice President, Portfolio Technology
Quadreal Property Group

Trevor Cleveland
Director, Operations Risk Management
Colliers International

Ken Cowan
Vice President, Risk and National Programs
Morguard Investments Limited

Nada Ebeid
Business Development Manager – Canada
Genetec

Sam Flis
Director, Property Technology
BentallGreenOak

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

Victor Lauer-Martin
Architecte, Sécurité de l'information, Technologies de l'information
Ivanhoe Cambridge

Kendall Peart
Managing Director, Real Estate
Marsh Canada Limited

Ruby Rai
Cyber Practice Leader
Marsh Canada Limited

Bob Riddell
President and Founding Advisor
Riddell Risk Management Inc

David Sulston
Director, Security
Oxford Properties Group

Nada Sutic
Director, Programs and Procurement
QuadReal Property Group

Martine Theriault
Vice-President of Property Management, Montreal & Ottawa
Canderel

Lee Thiessen
National Leader, Real Estate and Construction
MNP

Naveli Thomas
Director
Nyox

BOMA Canada team:

Benjamin Shinewald
President & CEO
BOMA Canada