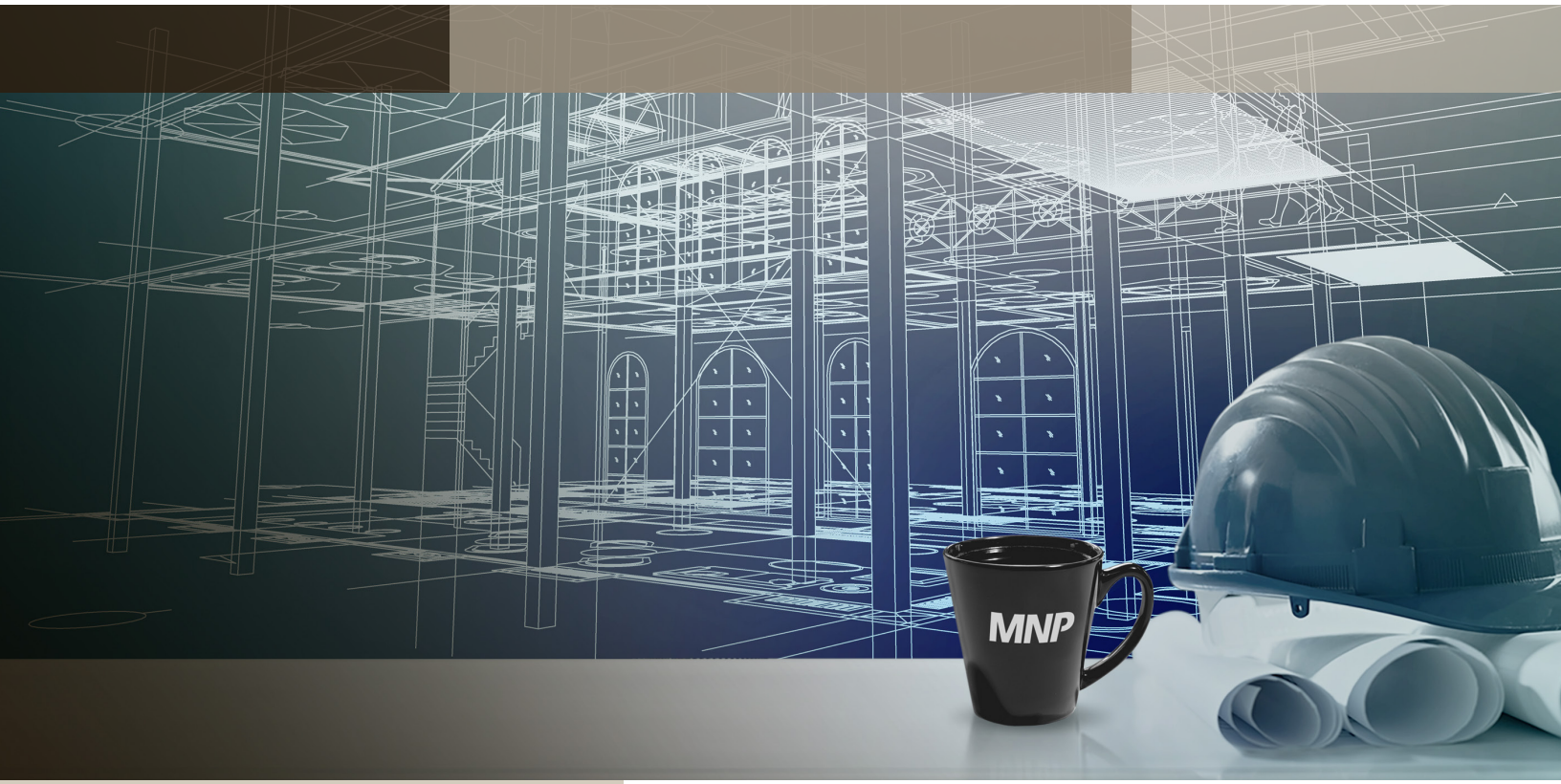

Cyber Security in Commercial Real Estate

Managing in an Expanded Risk Universe

Cyber security is recognized as a critical issue across industries, and most companies have some checks and balances in place to keep their data safe. Cyber risks have, however, grown at an unprecedented pace because of smart systems and the Industrial Internet of Things (IIoT) and that's especially true for the commercial real estate industry. Yet, cyber security planning within the industry hasn't caught up with today's reality.

The Industrial Internet of Things (IIoT) and Expansion of Risks

In a short span of time, smart systems and the (IIoT) have become the new reality for commercial real estate (CRE) organizations — from HVAC systems that can monitor occupancy trends and lower your utility bills, to elevator systems that run analytics to boost efficiency and reduce lineups. They've brought significant benefits, such as lower costs, improved efficiency and tenant satisfaction within CRE. But they don't come without risks.

Over the last few years, we've seen data and information-related cyber security breaches in the headlines and many CRE organizations have put checks in place. Now, the IIoT has opened up a whole new area of risks that are not just restricted to data and information, but also to physical systems and safety within every building.

These new Internet-connected systems are geared towards user-functionality but have minimal cyber security features built in, making them an easy target for attacks such as ransomware. Additionally, third-party vendors and building staff working on maintaining and managing these systems are often not trained in cyber security and further contribute to the risks. The massive 2013 breach at U.S. Target stores, for example, that impacted more than 70 million consumers, was caused by a third-party HVAC vendor's system.

Cyber security incidents and breaches aren't restricted to any particular size of organization either. Around 61 percent of the data breach victims listed in Verizon's benchmark 2017 Data Breach Investigations Report were businesses with fewer than 1,000 employees.

While CRE companies may have a certain level of cyber security planning at their corporate offices, the plans now need to evolve and account for these smart systems both at the corporate level and for their managed and owned buildings.

Expansion of Cyber Security Risks in Commercial Real Estate

What's at Risk

CRE companies have sensitive data that's related both to their own organization, and also to their tenants or customers. Cyber security for data has been a major concern and we've seen most CRE organizations recognize the threat it poses. As well, any malicious incident with a building system can be catastrophic. If elevator systems are altered in a building, door systems shut down, or even heating and cooling controls breached, people can be affected, and the results can have lasting damage. Smart systems can also provide an entryway into core data systems – the more connected the technology, the bigger the risk.

Brand, Reputation and Revenue

Incidents often make headlines and can have lasting impact on the image tenants and customers have of your company, whether the incidents come in the form of data breaches or building-system tampering that affects the comfort or safety of people. Any kind of cyber security incident usually has a longer-term impact on your revenue, too, as people are more cautious putting their trust and their money towards an organization that has been affected in the past.

Costs and Legal Risks

Most cyber security incidents affect the data or safety of tenants and customers and often come with legal risks attached. In CRE organizations especially, significant tenant financial information is stored on systems and physical tenant and customer safety is also at play, opening you up to legal ramifications if there is an incident.

Incidents and security breaches have an impact on your bottom line as well. First, there are costs associated with locating and stopping the source of the incident, purging the system of the malware, and strengthening the weak links. Then there are additional costs related to any repercussions that arise out of the incident, such as legal costs, payments to vendors, and even payouts to affected parties.

The Target breach cost the U.S.-based company US$18.5 million in settlements, not including other costs and damage the company incurred. Every incident isn't major like the Target one, but every incident does have an impact.

Taking Control

Each organization is at a different stage of maturity in its cyber security journey, but as cyber risks continue to evolve, so should your strategies. Before you start planning and creating a cyber security program, there are some critical steps you should consider taking.

Take it to the Top of the House

Cyber security no longer resides in a single department. It needs to be recognized as a top-of-the-house issue that has the attention of the C-suite, management and board. Then it needs to be filtered throughout the organization. While responsibility for the day-to-day strategy and execution may rest with a single department, the overall cyber security program needs to tie in with the firm's strategy and risk plan, and should lean towards protecting the most valuable parts of the business.

Increase the Cyber Security Scope

It's critical for CRE organizations to realize cyber security threats are no longer only restricted to information systems and enterprise resource planning (ERP) systems at the head office and corporate offices. They are also coming from anywhere in the managed buildings that have a smart system or are connected to the Internet. The people and departments responsible for managing cyber risks need to have a larger scope that extends to all the managed buildings and assets.

Include Third-Party Vendors

Most often, buildings have a network of third-party vendors to maintain or manage systems. With the systems themselves becoming smart and posing a new set of risks, the way vendors are selected, their capabilities, and the way they're integrated into your overall cyber security program needs to change too. Beginning with requirements built into request for proposals (RFPs) to overall cyber security responsibility matrices, these third party vendors need to be an integral part of your cyber security program.

Building Your Cyber Security Program

In response to the new reality, many industries have standards to create cyber security plans and checklists, such as the North American Electric Reliability Corporation (NERC) standards for the power generation and distribution industry. In the absence of such standards catered towards the CRE industry, it's critical to understand leading practices and then tailor them to your own organization and assets managed.

Your cyber security program can be divided into four parts: understand, prevent, detect and respond.

Understand Your Risks

Prioritize

The truth about creating a cyber security program is that funds and resources to put towards it are never unlimited. As a first step, it's critical to identify what your corporation's 'crown jewels' are because those are the most critical assets to protect. Second, it's important to understand the different types of assets you own or manage and categorize them: having a different detailed strategy for each asset is unrealistic, but you can create one for each asset type. And third, you need to outline the top priorities and goals for your program, which may include elements such as life safety deployment, fulfilling service commitments, and protecting tenant and corporate information, to name a few.

Assess

Assessing your organization's cyber security maturity and status is critical to analyzing the strengths and weaknesses of your program. This can be achieved through health checks and security posture reviews, especially for major assets. Often, your assets may be managed by third parties and you may not have a clear picture of their vulnerabilities. While assessing your assets to create a robust program however, you would need to delve deeper, both into physical systems and information. Your assessment may well reveal that based on your budget and resources, you need to focus on assets in stages, based on their level of importance.

Test

A critical component to test your business resiliency against a possible cyber attack, includes penetration testing and social engineering tests targeting your staff's vulnerability to cyber risks like phishing. While you might not be able to conduct testing on every building you own or manage, you could select a sample building from every category, prioritizing the important ones. Internal and external firewalls need to be tested for vulnerability, whether it's hacking from the outside or phishing emails that are clicked on from the inside. Testing usually reveals vulnerabilities organizations don't expect.

Prevent Incidents

Most organizations have some level of prevention in place but often have a lot of digital assets they haven't accounted for. In a commercial property, smart systems aren't always looked at from a security perspective and currently most smart devices and IIoT have only minimal security features built in. That increases the onus on CRE organizations to have a robust plan which builds in checks and balances for all types of systems throughout the network of buildings.

Setting standards and training both employees and external vendors at your corporate offices and buildings is critical in preventing incidents and breaches. Often, the organization is exposed to an attack through the actions of employees or vendors. Without training and demonstrating the results of actions to people, tests show as many as a third of employees click on phishing emails and a large number provide their confidential credentials.

Detect Breaches

Most companies have some detection systems and processes in place to guard against cyber breaches. However, they are usually manual processes, not 24 / 7 and don't extend beyond system logs or cyber security applications to get into the IIoT or other physical systems. Enough cannot be said about the value of artificial intelligence (AI) in overcoming these detection shortcomings.

AI systems can be deployed in your organization for cyber threat detection, based on your unique requirements. They run in the background continuously, detecting and understanding patterns. With the deployment of these systems, you can focus your resources on responding to threats, rather than on manual detection.

Respond to Threats

Once a threat is detected, you have very little time to respond if you want to minimize the repercussions. You need to have an incident response plan already in place for that particular situation, so you can start acting on it as soon as the incident is detected. Often, this is where many organizations fall behind and are forced to be reactive and inefficient in their response. Certain situations may require internal or external departments, such as forensics and legal, to get involved right away and with prior planning, the process is quicker with minimal errors. To truly be prepared, you should conduct tabletop exercises, which simulate incidents and your response to them.

Cyber risks exist across industries and commercial real estate is no different. What's changing is the pace of Internet-connected systems, leaving CRE companies with an expanded risk universe. It is imperative for companies to have a robust cyber security program that takes into account this rapidly changing reality — not only as a protective measure, but also as competitive advantage with tenants.

For a deeper discussion on cyber security in commercial real estate and how MNP can help, contact:

Lee Thiessen
National Leader, Real Estate and Construction
T: 403.537.7617
E : lee.thiessen@mnp.ca

Danny Timmins, CISSP
National Cyber Security Leader
T: 905.607.9777
E: danny.timmins@mnp.ca