RYCOM

Cyber impact to Real-Estate

Casey Witkowicz
President & CEO, RYCOM

RYCOM
Smart Tech. Smarter.

CYBER SECURITY

CYBER SECURITY

RYCOM

Cyber impact to Real-Estate

Introduction

Many groups such as the World Economic Forum, ISACA and Center for Strategic International Studies (CSIS) are all sounding alarm bells on the economic impact and disruptive nature of cyber crime; currently representing “nearly 1% of global GDP” [1]. The sophistication and ubiquitous nature of cyber attacks leaves little room for second guessing if you’re a target. In fact many would agree that we have reached the point of mathematical certainty that we already have or will experience a breach.

The tremendous advancements in technology over the last couple of decades have created new sets of building blocks for businesses to leverage in their day-to-day operations. Investors and C-suite stakeholders are beginning to leverage these technological innovations in the development, growth and management of their business strategies to meet the ever-changing market demands and maintain competitiveness. This is especially true today in CRE.

The **Real-Estate industry is in the midst of a Digital transformation** where we are developing strategies and deploying underpinning operational digital tech in every facet of building operation. This is leading to a transformation of the existing built environment/inventory and new development towards smart Real-Estate; building the foundation for autonomous buildings and smart cities.

As Real-Estate absorbs more digital technology, we are expanding the attack surface for cyber criminals. The technological innovations of our time serve everyone good and bad. Isaac Asimov said, “***The saddest aspect of life right now is that science gathers knowledge faster than society gathers wisdom”***. We face the challenge of increasing our wisdom to mitigate the risk of tech misuse. We can ask ourselves, can we put the (digital) genie back in the bottle, or more importantly do we want to - I am afraid the answer is NO, no more than you can give up your smartphone, PC, elevators, car or air travel. Technology is here to stay, influences our lives, makes us more informed, and allows us to reach further than we have before. So, for all of us, technology will continue to embed itself further in our personal and business lives, dragging in with it the unwanted, namely cybercrimes.

This creates a back drop, where “Cybercrime seems relentless, undiminished, and unlikely to stop. It is just too easy and too rewarding, and the chances of being caught and punished are perceived as being too low” [2], this requires the industry to build a dynamic and responsive cyber defence strategy (Asimov, “wisdom”). This strategy is not purely technology based but encompasses people, processes and tech in the right proportions to be effective. This is especially true in the Real-Estate industry.

[1] Economic Impact of Cybercrime – CSIS – February 2018 - https://www.csis.org/analysis/economic-impact-cybercrime

[2] Economic Impact of Cybercrime – CSIS – February 2018 - https://www.csis.org/analysis/economic-impact-cybercrime

With everyone in your company digitally enabled the CIO no longer can carry the sole burden of keeping your enterprise safe. As the Real-Estate industry absorbs more and more digital technology into their assets, existing and new stakeholders like Operational Technology team members must play a material role in cyber crime defence. This is especially important in the Real-Estate industry. Traditional IT methods and technologies must be adapted to work in the property space since this arena utilizes much more diverse technology products and solutions. Not only that, but each property has unique characteristics, blends of technologies, and different operational methodologies. Understanding the threat landscape is complex and requires context when creating Cyber strategies.

The Stakes are High with Cybercrime

"The economic impact of cyber crime is material, however the brand and safety damage last far beyond a calendar year".

The economic impact of cyber crime on a global scale is hovering around $2 Trillion [3] in 2019 climbing to a 2021 forecast of $6 Trillion. CSIS reported globally on a daily basis, some 80 Billion malicious scans are done, 300K new malware introduced and some 800k records compromised and that's only representative of about 13% [4] enterprises reporting breaches. As we move forward, it becomes more and more important about not how much we spend on Cybersecurity but how we spend it. Real-Estate is a key economic driver throughout all the major centers in the world. Not only does Real-Estate contribute greatly to every country's GDP, Real-Estate houses all the industries currently on the planet. Real-Estate must meet the ever-changing requirements of their tenant populations and position themselves as the foundation for smart cities, all the while maintaining their competitiveness. Further adding to this, Real-Estate houses, entertains, and hosts millions of people/tenants each day. This creates a multi-dimensional environment to protect against Cybercrime when creating and implementing digital and smart Real-Estate strategies. The impact of cyber breaches mimics the effects of property related safety issues. To address the latter the Real-Estate industry invested in physical security technology such as cameras, access control, and security guards to provide premise safety and security to tenants, shoppers and residents. These are visible security measures. Cybercrime is the unseen threat making the defense and governance of spaces and properties even more challenging however, the consequences no less severe than property safety.

[3] https://businessmirror.com.ph/2019/03/26/cybercrime-worldwide-to-cost-6-trillion-in-two-years/

[4] Economic Impact of Cybercrime – CSIS – February 2018 - https://www.csis.org/analysis/economic-impact-cybercrime

In any risk management process the key step is to understand the impact of a breach and then formulate the response. In the situation of known cyber attack cases the impact and defence are understood; someone else was first to suffer so we can all benefit. The more complex almost hidden scenario is when your firm is under attack and the traditional existing safety measures are not enough.

If cyber crime history has taught us anything it's that cyber criminals are first movers, smart and bleeding edge users of the next generation innovation. This warrants a proportional, measured response from the industry to defend their business interests, reputation and brand.

Board and management principal responsibilities

"A well-structured assessment and quick response plan are key in avoiding or minimizing a cyber attack crisis".

One basic function of a modern corporate board is to oversee risk management and along with that comes the need to understand the impact of Cyber. Consequences of cybercrime could be regulatory investigations, loss of intellectual property, risk from fraud, and potentially Brand risk in the eyes of customers and investors. At a high level, the board must ensure that the company has cyber risk management policies and procedures consistent with its business strategy, risk appetite and prevailing laws.

Further, the board must ensure that these policies and procedures are functioning, tested, and constantly improving. With that, boards should review things like annual budgets commensurate with risk, for privacy and security, review efficacy of assigned roles and responsibilities, and get regular briefings on preparedness, cyber issues, and risk mitigation efforts.

To that end the National Association of Corporate Directors (NACD) in its handbook for cyber oversight lists the following principles to uphold:

Principle 1:
Directors need to understand and approach cybersecurity as an enterprise wide risk management issue, not just an IT issue.

Principle 2:
Directors should understand the legal implications of cyber risks as they relate to their company's specific circumstances and prioritize their most valuable assets and their associated risks.

Principle 3:
Boards should have adequate access to cybersecurity expertise. Cyber risk management should be given regular and adequate time on board meeting agendas.

Principle 4:
Directors should set the expectation that management will establish an enterprise-wide cyber risk management framework with adequate staffing and budget.

Principle 5:
Board-management discussions about cyber risk should include identification of which risks are avoided, which to accept, and which to mitigate or transfer through insurance, as well as specific plans associated with each approach.

These principles are rooted in cyber risk mitigation strategies and operations protecting business, personal and brand interests. In addition, these principals build the foundation for day-to-day business operation.

For the Real-Estate industry much like industry in general, one additional principle should be in respect to third parties that are directly involved with the operation, implementation and development within properties. They must have controls and policies in place that are aligned with corporate expectations. These third parties must also adhere to at least, the intent of the 5 principles.

Cyber defence is a holistic strategy from employee one, third party providers, to the board. Boards must always remain informed to ensure that their company is prepared to respond, confirming preventative and detective controls are in place.

Having a Cyber governance models to fit Your business

“Getting tactical and dynamic in your Cyber defence strategy preserves the continuity of your enterprise”.

There are many evolving approaches to defending your Real-Estate & company against cyber crime. A report issued by MITRE Corporation put forward several working governance models that allow your cyber advisors to adopt the best model or models to suit your business. Cybercrime tactics and tools are always changing, so each model must be adapted to a particular risk requirement. With the digital transformation that is occurring in the Real-Estate industry, hybrid models will need to be implemented depending on the site maturity. This doesn’t preclude establishing a standard by which portfolios can be measured but does assist in the Cyber Maturity journey. The models are directional in nature:

A

Pervasive Agility. The organization maintains operations on a continuing basis and adapts to current and future coordinated, successful attacks, regardless of their origins. The organization employs a highly agile, adaptive and flexible structure that permeates all aspects of the organization (including planning, supply chains, collaboration, architecture, governance, and resources), allowing the organization to continually and dynamically reshape all aspects of its technology and operations in face of changing, successful attacks.

B

Architectural Resilience. The organization shapes its business or mission processes and systems architecture to provide attack tolerance, designing and operating systems with the concepts of resilience and protection through multiple distinct enclaves, so that organization can limit exfiltration of critical information, contain adversaries, and operate through (even in degraded mode) and recover from a successful attack.

C

Responsive Awareness. The organization deploys capabilities to detect and respond to indications of attempts to gain a foothold within the organization's information infrastructure, complementing these capabilities with procedures to better understand the methods of the adversary.

D

Critical Information Protection. The organization identifies and protects critical data regardless of its location, using encryption, enhanced identification & authentication and access control methods.

E

Perimeter Defence. The organization establishes and defends the information system perimeter; protects against the introduction of known malicious cod/malware and discourages unauthorized internal access; and uses commercial security products and professionally manages perimeter and desktop systems.

When creating a cyber strategy that best matches your business needs, it is necessary to understand that it will require continuous re-evaluation and optimization as your spaces and businesses continue to digitally transform. The digital landscape is continuously evolving, bringing new technologies and with them new cyber challenges – cybersecurity activities never end – rinse and repeat.

Should cyber be part of your due diligence in a M&A?

"Would you buy impaired assets with broken windows, no heating or utilities? Perhaps at a deep discount, however knowing target asset's cyber past, current defence and current cyber contamination status needs to be part of your decision to purchase, before you put your brand on it".

Real-Estate owners and investors are investing globally. According to Global Investment Atlas 2019-2020 Real-Estate investment transaction volumes in 2018 reached US$1.75 trillion [5]. Real-Estate changes hands on a regular basis so understanding the properties full digital information profile and history will be key. This digital profile needs to include property Business Continuity plans, technology systems in place, Cybersecurity measures in terms of policies and procedures, and site risk profile, as well as tenant and property breach history (to name a few). Understanding if there have been any cyber events and the actions taken to either circumvent, prevent, or respond to these events will provide insight into sites cyber readiness. With the impact that ransomware [6] has had through North America, ensuring that the systems in your newly acquired properties are not compromised and waiting to be activated is important.

Over the last decade, the Real-Estate industry has moved more towards converged operational networks for base building systems. These digital platforms provide controlled access and focused command and control integrations. Ensuring that technology implementations have been carefully designed with Cybersecurity embedded in the architecture must be part of the due diligence process. Technology no longer can be ignored in asset evaluations.

However, legacy type operations are not an antidote to cyber attacks. In fact, legacy operations can lengthen the duration of the attack, recovery and identification of the issues resulting in longer system outage and frantic restoration activities. Legacy access and control of building systems are typically under the care of the building systems vendor and as such are subject to their (3rd party) cyber security policy. This results in a fragmented and vulnerable property security strategy, increasing the risk profile to the acquirer and operator. Remember risk is not just associated with data breaches; it could impact Brand or reputation, system functionality, and even have an impact to life and safety.

[5] http://www.cushmanwakefield.com/en/research-and-insight/2019/global-investment-atlas-2019-2020

[6] https://www.allot.com/blog/10-ransomware-attacks-2019/

Having a Cyber strategy and platform within your assets improves the speed of your defence when under attack and/or recovery from an attack. With digital platforms like Base Building Networks the ability to converge, control, and share data from all vital building systems, enhances the buildings security defence posture. Having an established digital platform like a BBN, ensures that the digital surface and device inventory is known providing your trusted cyber security operations centers (CSOC) a known geography to defend, investigate and support.

During the due diligence prior to site acquisition, a cyber and security evaluation of the building operating systems and the cybersecurity measures that are in place must be added to the process. Although traditionally asset evaluation is generally around system age, functionality, and lifespan to determine cost to maintain, cyber must be added to determine cost to brand, system functionality and business continuity.

Why is cyber security so difficult?

"For the most part safety and security strategies are against adversaries that we see, cyber criminal is invisible but just as dangerous if not more".

"Technology alone is not a cyber defence, constantly evaluating risk disposition is just as important as understanding your business viability".

After a few decades of investments, innovation, and invention of some the worlds best technology we still see Cyber crime as a runaway train wreck, seemingly causing harm at will. In-building technologies are drastically changing. Money is being spent to create new technologies which will drive access to new data for business and operational intelligence. IoT isn't just the smart watch you are wearing. In the property world, processing power is being moved to the edge devices for edge computing. This is also allowing for analytic activities to be done on these devices with more powerful analytics occurring on the management systems – fog computing. We are starting to see Software Defined based IoT (SDIoT), where they are creating their own mesh networks circumventing traditional cyber management.

These IoT systems and devices are going to increase in importance as we move towards smart-cities where real-time decision analytics will be done “on the fly”. There isn’t a silver bullet to deal with the complexities that this environment brings for Cybersecurity. Not only that but we have now increased the “threat landscape” with all of these additional smart devices and increased the complexity of how the data flows. This is going to make it easier for the Cyber Criminals and more difficult for Cyber Security. However, particularly in the Real-Estate industry, understanding what you have, what the risk is, and how to mitigate that risk is really the starting point. We have to look at traditional processes but take untraditional approaches to securing digital assets.

If we start to think about the following things, we can get better situated to deal with the new and upcoming digital landscapes. Here’s a few to consider.

- We need to be smarter & better than the Cyber criminals, knowledge and experience are invaluable, invest in experience (people),
- Work with our partner ecosystem to ensure that we are aligned on our cyber practices,
- Start with policies and procedures that are “doable” and then build from there,
- First mover advantage, we believe it to be an advantage in business but very few practice it in cyber, we wait for the patch to solve our problem,
- Build a 24/7 cyber defence strategy, support and governance (board level to employee), Cyber crime is a 24/7 operation,
- This is not solely a tech problem, the attack shows up in tech, but the attack strategy seldom starts there,
- Cyber laws and policy are not fully developed globally, we have laws that are local to a country however cyber lawlessness is global,
- Your cyber strategy and investments should be closely guarded information no different than your IP or any other privileged information,
- Build a dynamic defence and response environment and if your enterprise is not big enough to go it alone hire experience trusted cyber security operations center (CSOC) companies to partner with you.

It is becoming abundantly clear in industry that to truly build a sustainable defence against cyber crime your defence strategies need to engage all the stakeholders in the mix; people, processes, supply chain and tech.

What is the future of Cyber crime?

"Unfortunately, the future of Cyber is bright for now unless we do something about it".

One favorite group that's constantly under attack are financial institutions many of which are key or anchor tenants. According to the American Bankers Association, bank robberies have dropped by 83% compared to 1991 levels, while ATM skimming, and cyber heists are steadily on the rise. Other digital crimes like keyless entry break-ins into cars and hotel rooms are demonstrating that Cyber is not just a hack on your computer.

As we apply sensors to virtually anything and anyone, the opportunity to exploit these devices increases. Here are some areas of current and future cyber crime that could affect us:

- Cyber Ransomware – extorting payment from the victims to return the use of their PC, use of data,
- Brick Attacks – attacking computers and rendering them useless so any key data or purpose of the device is just dead weight "Brick". One of the first brick attacks was Saudi Armco in 2012 destroying 30,000 computers and in 2013 NSA foiled an attempt to brick computers across the US the impact here would be severe,
- Going forward the amount of data records that will be compromised are in the 100's of billion, according to Juniper research 146B over a five-year window.

The list of potential and possible attack targets is many. Identifying them would not add anymore context to the serious nature of cyber crime and the importance of a sound cyber defence strategy. The point is that if you can think it, it likely can be done.

Conclusion

As you can see there are many aspects to developing and understanding the complexity of a Cybersecurity strategy. There are also many stakeholders that are involved and have a component of responsibility in order to have a robust Cybersecurity program. Adding to the mix, technology adoption in Real-Estate is increasing, and the technology is getting smarter. We have more attack vectors than we had before, and this isn't decreasing.

In order to establish a good Cyber practice, context of environment is important. Generally, you can take the same way you evaluate physical security risk if it's comprehensive, and leverage some of those best practices. However, it's easy to "jump the shark" and implement traditional technologies to combat or reduce the risk gap. Understanding the complexity of the environment, the associated risks, and establishing a roadmap will ensure that you are de-risking what's important to your business. Too often we see Threat assessments done, without any remediation. A commitment to Cyber Security is a top down strategy with a bottom up execution. Any Cybersecurity strategy must have pragmatism at heart to ensure that it is adopted in the areas where there is the most risk.

Although we are always moving towards Cyber legislation and programs to fight Cybercrime and ensure more transparency, as companies we must also ensure that we protect our assets. As mentioned, a breach is inevitable if it hasn't already happened…however you may not know, so there are several things that have been outlined.

- **Understand** what your risks are, where they are, and what is important to your business,
- Don't be a **roadblock** to business operations – any Cyber Strategy must be aligned with business objectives and priorities as well as ensuring that operations can do their job,
- **Resilience** – how do you respond when there is a breach or a Cyber Event that impacts business continuity,
- **Be Creative** – understand that innovation can be used as a proactive defense since the "bad guys" are always innovating,
- **Everyone** has a contribution to the success of any Cybersecurity program and can also be the reason for failure. The partner and employee ecosystem.

The move is yours!

rycom.com
rycom
linkedin.com/company/rycom

Casey Witkowicz
casey.witkowicz@rycom.com