Future of Cybersecurity: All Hands on Deck

With cybercrimes growing exponentially, commercial real estate experts weigh in on the future of cybersecurity. How do you stay one step ahead of a potential data breach?

- SEP052019
- By
- **IvyLee Rosario**
- https://www.cpexecutive.com/post/future-of-cybersecurity-all-hands-on-deck/

Image via Pixabay

The recent hacking of Capital One, in which an individual singlehandedly gained access to 100 million customer accounts and credit card applications, has jolted many real estate executives into scrutinizing how well they safeguard their data and the systems that run their buildings. With damages related to cybercrime estimated to reach trillions globally by 2021, the others need to catch up soon.

Automation of building functions and processes has accelerated the need for cybersecurity. From locks and HVAC systems to lighting controls and energy monitoring, the Internet of Things continues to take over and more information is being pushed to the cloud. But while artificial intelligence and machine learning tend to be more efficient and decrease the possibility for human error, they increase the potential for cyber threats. And with building technology changing every day, what is the future of cybersecurity?

"It goes beyond our phones and computers (and) spreads through the infrastructure that we rely on daily," said Cushman & Wakefield Director John Redeker.

Nevertheless, the commercial real estate industry has largely been focused on employees' interconnected devices while overlooking the security of the physical assets they operate out of, Redeker notes. Since cyber invasions on buildings haven't happened to an alarming point, most owner/operators choose not to spend money until it's too late and they are hacked.

"It's much easier for a hacker to shut down the electricity, open or lock certain doors or change the security systems in place," he said. *"By then the damage is done and it becomes a top priority when it's too late."*

Indeed. According to IBM's 2019 Cost of a Data Breach Report, the average time to identify and contain a breach is 279 days, with the lifecycle of a malicious attack from breach to containment being an average of 314 days.

Cyber threats are also becoming more sophisticated, with hackers going past just infiltrating machines and technology and moving onto people. This is evidenced by the growing number of phishing schemes against high level executives and dealmakers. A hypothetical example of this would be, after the closing of a transaction, a hacker might reach out to a buyer posing as a C-suite member and explain that they never received the funds for a transaction. Although at the end of the day an organization might not be liable for this loss, this still reflects poorly on the company and might make it more difficult to conduct future transactions.

According to **Deloitte's 2019 Commercial Real Estate Outlook**, respondents considered damage to reputation (41 percent), financial theft/fraud (37 percent) and theft of personally identifiable information (35 percent) as the top three impacts of cybersecurity breaches.

THE MISSING LINK

Investing in a proper cybersecurity program, experts say, is the only way to mitigate the risk of a cyberattack on your business or assets. While IBM estimates the average total cost of a data breach to be around $3.9 million, it finds that the formation of an incident response team and extensive use of encryption can reduce the cost of a major hack by an average of $360,000.

The key to a successful cybersecurity program is devising something that can be sustained in the long term that addresses the particular risks of the company, explains David Ross, principal & cybersecurity and privacy practices leader, Baker Tilly. *"These firms are in the business of real estate, not cybersecurity,"* Ross said. *"They have to sit down and determine 'where we are most at risk, where we need to spend our money, and what our limits are.'"*

Rapid IT changes and rising complexities (53 percent), lack of detailed response by management (38 percent) and ineffective security solutions due to functionality and interoperability issues (37 percent) were reported as the top three challenges in managing cybersecurity, according to the Deloitte survey. Even though prevention programs should be extensive, they don't have to be as difficult as it might seem. TEKsystems Director of Global Services Matthew Ehrlich explains that cybersecurity should be viewed as a timeline and not just a one-time incident.

"Traditional IT groups are assessing various industries at all times, but when it comes to (building) operational technology and the risk it creates, no one is talking about that," Ehrlich said.

In addition, owner/operators need to be more proactive rather than reactive in their cyber preparedness efforts. Therefore, cybersecurity measures need to be adaptive since the building technology around it is constantly evolving. This means involving leadership and board members, creating a close alignment with the company's business strategy, conducting scenario planning and cyber risk assessments and

making sure employees are fully aware of their responsibilities and how to stay vigilant, explains Surabhi Kejriwal, real estate research leader, Deloitte Center for Financial Services.

"The importance of cybersecurity will continue to increase as business and threat scenarios become more complex," said Kejriwal. *"Along with this, there will be an increase in regulatory oversight and actions, which may cut across geographies."*

FUTURE OF CYBERSECURITY

The most challenging question comes down to who is most responsible for your real estate company's cyber security? Some say protecting system data and the sensitive information landlords collect from tenants is a real estate problem and that the building management staff needs to be accountable for any foreseeable issues that might occur. Others would say it is an IT department issue to put a cybersecurity program in place along with the organization's IT infrastructure.

"This is why it is so important for owner/operators to become aware of the risks and realize that all departments and functions are involved in the prevention or mitigation of cyber-risks," noted SONRO Real Estate Services' Senior Advisor & Managing Partner Marie-Noelle Brisson, CRE, FRICS.

The answer lies somewhere in the middle. Owner/operators, experts say, should meet with their internal IT providers and outside vendors for each property to discuss what can be leveraged to protect the network and the physical asset. The solution will come when these two puzzle pieces can fit together, whether it be a technology system that can be integrated into real estate or vice versa.

"Good cyber hygiene starts with data governance," added Brisson. *"In a company, as in a building, cybersecurity is a risk mitigation issue—not an IT problem. It is everyone's job."*

Read the September 2019 issue of CPE.