Risky Business: Why Cybersecurity Should be Top of Mind for CRE Professionals

Over the past year, it's sometimes felt like the number of factors that we, as commercial real estate (CRE) professionals, need to keep track of have grown exponentially. Especially in the face of challenging market conditions.

At the same time, there's an ever-increasing need to be conversant with new technology and tech tools that help boost productivity and add value for clients. The tools available span the spectrum from social media to drone technology, climate-savvy building tech, and even augmented or virtual reality software.

For brokers, building managers and developers incorporating these game-changing technologies, the possibilities are nearly endless.

There is, however, a flip side to this coin. Like many things tech-related, it's an area where CRE professionals have often been slow on the uptake: Implementing the right cybersecurity protocols.

A Growing Threat

Part of the problem is the idea that cybersecurity is something that's handled exclusively by a dedicated team, or automatically built into the software being used. While that's true to some extent, the fact remains that the tactics cyber criminals use, and the number of incidents each year, are continually growing.

Sophisticated "phishing" attacks, which aim to get staff to unwittingly compromise system security, and ransomware are the order of the day, and the real estate sector is far from exempt from these threats.

Given the amount of sensitive data passing through or stored by the CRE industry, the question we need to ask is: Are we truly prepared in the event of a breach?

New Risk Vectors

The first thing all CRE businesses should consider is whether all possible systems, and avenues of access to those systems, have been identified and are properly protected.

In an excellent recent interview on cyber threats in CRE, security consultant Coleman Wolf points out that many possible avenues of attack go unnoticed. These may be linked to building control systems (think temperature or lighting management) and other smart tech, or even to the specialized Internet-of-Things (IoT) systems being used in industrial operations.

Risky Business: Why Cybersecurity Should be Top of Mind for CRE Professionals

If these systems are connected to the internet, but not adequately protected, they may act as a springboard for access to other systems or data. Hackers may then be able to tap into sensitive information, including financial and personal data stored elsewhere. Alternately, simply taking control of building systems can be used as a tactic in ransomware attacks.

As the CRE industry begins to adopt new smart building technologies, and buildings are increasingly repurposed for niche markets, like the booming medical office sector, the potential for sensitive information to form part of breaches also grows exponentially.

Other trends, like the Bring-Your-Own-Device (BYOD) movement where employees use personal devices in the office, create additional avenues of attack if those devices aren't properly secured.

Best Principles

While all the above may make it sound like it's impossible to keep track of potential threats to a building or CRE enterprise, the good news is that there are certain essential principles that can be followed to mitigate the risk.

In a recent article on cybersecurity best practices in CRE, J.P. Morgan advises that:

- CRE companies should ensure all employees, beyond just the IT team, are aware of potential risks from phishing or ransomware and have been trained in how to minimize those risks.
- Companies ensure there's appropriate access control. For example, implementing multifactor authorization (MFA) and other safeguards.
- Employees are aware of the risks of oversharing on social media (e.g., detailed information on job responsibilities and the type of data they have access to, which could make them phishing targets).

Of course, these recommendations are only starting points, and the exact requirements and level of detail needed will vary based on each firm's unique context. There's certainly no "one-size-fits-all" solution for CRE cybersecurity.

An excellent resource to familiarize yourself with upcoming benchmarks and strategies for cyber-security can be found in PwC's "C-suite united on cyber-ready futures" guide.

Securing the Future

As we head into 2023 and beyond, some of the most exciting aspects of the CRE industry come in the form of new technology. There's an ever-expanding array of Proptech tools on hand to help us close deals. Smarter building technologies ensure we meet environmental and climate imperatives while also offering something new and different for tenants and investors alike.

As CRE professionals, we're right to be excited by these possibilities. But we also need to make sure we keep security top of mind as we begin to integrate these tools.

As PwC summarizes: "Digitization makes security everyone's business. The future promises more connected systems and exponentially more data — and more organized adversaries. With ever expanding cyber risks, business leaders have much more work to do."