COVID-19 Highlights the Need for Smart Building Cybersecurity

The issue has evolved from an IT concern to a risk management issue where everybody plays a role, writes cybersecurity adviser Noelle Brisson.

MAY 08 2020

- By Noelle Brisson FRICS
- Commercial Property Executive. https://www.cpexecutive.com/post/covid-19-highlights-the-need-for-smart-building-cybersecurity/

Noelle Brisson FRICS

As firms across the globe strive to ensure business continuity and employee safety through remote working, they are increasingly relying on digital communications and conferencing technology to hold meetings and events. Similarly, companies are relying heavily on a variety of shared drives, programs and IoTs that enable remote workers to maintain workflow and project control.

In many cases, companies already have existing work-from-home and remote policies as an employee benefit, a collaboration empowerment tool or as an alternative to minimize the need for travel. These strategies are often part of larger sustainability frameworks, but whether a company is expanding on an existing set of remote policies or quickly adjusting to a new way of working, this rapidly increased reliance on remote access, communication and file-sharing is shining a light on an oft-overlooked aspect of these sustainability and health and well-being initiatives: cybersecurity.

This issue of cybersecurity is exacerbated by the rise of smart buildings. Smart buildings, to be sure, are overwhelmingly a positive trend for the commercial real estate industry and the public. These connected inter- and intra-building systems create efficiencies that reduce emissions, save on energy, streamline physical security, empower leasing strategy, prioritize elevator allocation and logistics, make maintenance and repairs more proactive and promote overall transparency and control over all aspects of these physical assets. These systems are hugely important for tenant health and well-being, urban and suburban sustainability and cost savings.

CYBER RISKS

However, smart buildings tend to focus on "green," at the expense of cyber risks. These smart buildings also bring with them new and unprecedented threats for owners, asset managers and tenants, creating new digital vulnerabilities that our post-COVID-19 connectivity is only making more apparent. Zoom, for instance, has been noted for its vulnerability to interlopers, while new applications also create concerns about what kind of data are being exposed and what's being done with the information. Buildings and companies need to think of their workplace and network as extending to wherever every member on their team is working.

ASSET MANAGEMENT

In the asset management world, every time you have a new tenant, the building's IT team needs to do a security sweep of the office space and assess what needs updating. They also need to make sure that the new tenant has security that is up to date and effective, not only for themselves but for all the other tenants in the building. Applying this logic, especially in this pandemic landscape, a "cyber sweep" of office or home space is critical. Information security isn't just about your Midtown Manhattan office server or even your building's internet connection, it's your CEO's home office in Scarsdale, your marketing intern's parents' home in Naperville, your consultant's office in London and your off-shore supplier's facilities. Any connected touchpoints are a potential vulnerability for your sensitive information.

Every owner and tenant needs to engage in an extensive audit of their policies and security protocol, as well as an accounting of who is using their systems and how they're accessing them. For instance, it's important, but not enough, to have VPNs, secure server access, robust and clear policies on email, file sharing and collaboration tools, like Outlook, Dropbox or Asana. Remember that information on the cloud is vulnerable not simply to hackers or malware but also to the companies that create this software and various domestic and foreign governments and agencies. Some companies are not aware as to where "their" cloud is located.

Training also becomes essential. Your teams need to be trained in data governance, and know the risks of working remotely. Now more than ever, they need to be prepared to make the right choices when it comes to obvious handling of email, files, and software, but also use connected objects around them cautiously. Many companies already have these measures in place, since working on public and home Wi-Fi networks is a normal practice now. People regularly work in airports and from bed. Revisit these policies on an ongoing basis and make sure your teams keep them top of mind. Also consider cybersecurity consulting help.

In a world where our buildings are connected for the greater good of the inhabitants, we need to remember the ways these efficiencies create risks. As we distance ourselves from co-workers and stay safe from home, we need to remember that the connectivity empowering public safety also opens up our businesses and our industries to threats. We shouldn't look at this as a reason not to stay connected—the benefits far outweigh the risks—but we should use this as an opportunity to make sure that we’re being smart, secure and current in our policies and practices.

Cybersecurity is no longer just an IT concern; it is a risk management issue where everybody plays a role.

Noelle Brisson FRICS is on the Americas Board for RICS and is a managing partner for SONRO Real Estate Services, where she conducts rating advisory services for the commercial real estate industry and advises on cybersecurity risks management. She also serves on the Board and is the president of the Audit Committee for Enda Tamweel, a Tunisian institution that promotes financial inclusion by providing microfinancing to those in need.