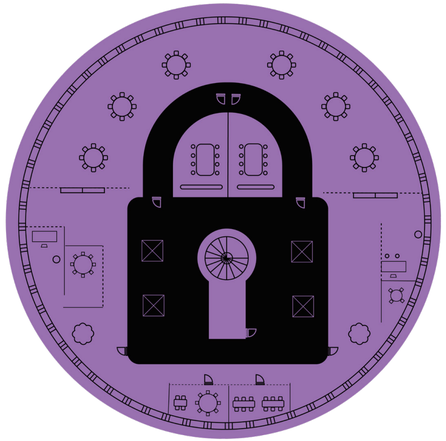
Deloitte.



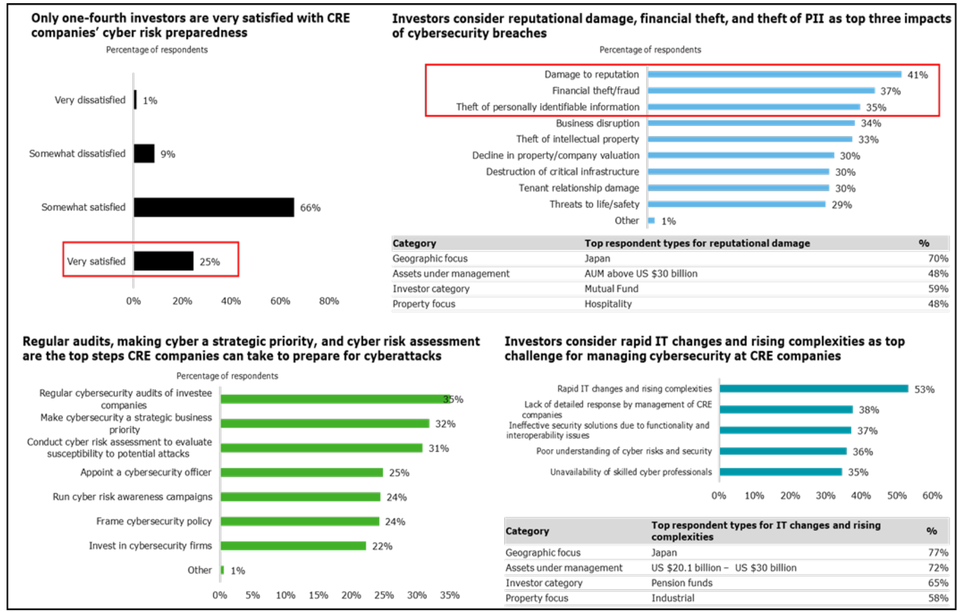
Securing the enterprise: Assessing cyber risk in commercial real estate

Evolving technologies, business models, and risks

As extensive technology advancements reshape the traditional commercial real estate (CRE) business model, owners and operators must contend with new forms of risk, including cyberattacks information security, and data privacy. For example, the growing use of IoT technologies such as sensor-enabled building management systems could broaden the attack surface for CRE firms, increasing access to sensitive data that can cause financial and reputational damage to owners/operators and tenants. The question is, then, are CRE companies ready to handle cyber risks?

To better answer this, Deloitte conducted a global survey in 2018 of 500 institutional investors. The survey revealed that only 25 percent of respondents are very satisfied with CRE companies' cyber risk preparedness, though the rates do vary by geography (see figure 1). Given this assessment, CRE companies should probably consider how to better balance their investments in technology with their ability to manage growing cyber risks.

Figure 1: The investor pulse: Cyber risk management



Category	Top respondent types for reputational damage	%
Geographic focus	Japan	70%
Assets under management	AUM above US $30 billion	48%
Investor category	Mutual Fund	59%
Property focus	Hospitality	48%

Category	Top respondent types for IT changes and rising complexities	%
Geographic focus	Japan	77%
Assets under management	US $20.1 billion – US $30 billion	72%
Investor category	Pension funds	65%
Property focus	Industrial	58%

Note: The categories highlighted in the graphic tables suggest the following about the survey respondents:
Property focus: Property specialization of investors;
Geographic focus: Home country of the investor;
Assets under management: Investor size

Source: Deloitte Center for Financial Services Analysis

Navigating cyber risks

With the heightened threat from cyber risks, surveyed investors expect investee companies to make cyber security a leadership-driven business priority, perform regular cyber risk assessments, and conduct awareness campaigns to evaluate susceptibility to potential attacks. It is imperative that CRE companies take a proactive approach to determine appropriate responses to cyber risks and be more secure, vigilant, and resilient.

Make cybersecurity a leadership-driven business priority

Involvement and engagement of senior management and the board is crucial to making cybersecurity a strategic business priority and maintaining it. The SEC's updated cybersecurity disclosure guidelines emphasize that the board of directors take ownership and responsibility for developing and supervising cyber risk mitigation controls and procedures.[1] As such, CRE senior management and boards should be deeply involved in developing policies; framing the cybersecurity policy, roles, and responsibilities; assigning budgets; and tracking overall progress to establish and maintain accountability. The board and senior management should strongly consider appointing a cybersecurity officer—who should be an accountable cyber risk strategist and advisor along with senior management—to design, execute, and align their cyber risk strategy with a central mandate. To do this, the CRE board and senior management must work together rather than in silos.

[1] "Commission Statement and Guidance on Public Company Cybersecurity Disclosures", Securities and Exchange Commission, February 26, 2018.

Perform regular cyber risk assessments

A detailed scenario planning and cyber risk assessment would allow companies to evaluate susceptibility to cyberattacks and identify appropriate responses. Companies should develop a cyber risk assessment framework that offers guidelines to evaluate the threat landscape and align appropriate resources to manage the risk[2]. Bearing in mind that it is not possible to eliminate risk, CRE companies should deploy advanced detection technologies such as artificial intelligence to sense potential threats and use analytics to devise appropriate response management tactics.[3] It is important to not treat cyber risk assessment as a singular activity but rather a regular and ongoing part of the company's cybersecurity policy and framework.

Conduct awareness campaigns

CRE companies should evaluate employees for their exposure to cyber risks. They should conduct trainings to help employees understand the potential threat and implications of various types of risks, especially cybercrimes, to themselves and to the company. CRE companies may also need to train or hire appropriate cyber risk talent in their organization. Finally, companies should drive behavioral change to instill the responsibility and mutual accountability for risk management among all employees.

[2] "3 types of cybersecurity assessments," threatsketch.com, May 16, 2018.
[3] Carlos Molina, "Next-generation cyber attacks call for next-generation solutions," CUNA Mutual Group, accessed on September 3, 2018.

The bottom line: Change the mindset

Clearly, CRE boards and senior managements need to reassess their current risk prioritization. Some of the key questions they should consider are:

- Are you broadening the risk management agenda to include newer ones such as cyber risk?
- Is the CRE board and senior management ready to assume responsibility and accountability for managing these new risks?
- Are you considering a centralized or decentralized approach to risk management?

To learn more about other factors that are likely to influence institutional investors' CRE investment decisions over the next 18 months, see the Deloitte report, 2019 Commercial Real Estate Outlook: Agility is key to winning in the digital era.

Written by:

Surabhi Kejriwal
Lauren Hampton
(US)

"CRE companies should evaluate employees for their exposure to cyber risks".