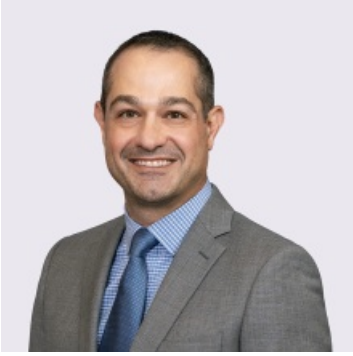
Legal Update Article

Is the Real Estate Industry a Target for Cyberattacks?

By Jason C. Gavejian

January 20, 2021

Meet the Authors



Jason C. Gavejian
Office Managing Principal
908-795-5139
Jason.Gavejian@jacksonlewis.com

Related Services

Privacy, Data and Cybersecurity
Real Estate

No industry is immune to privacy and cybersecurity risks, and the real estate industry is no exception. Those in the real estate industry can protect against cyberattack by understanding the risks and vulnerabilities and developing a plan.

The industry appeals to cyberattackers in many ways. Real estate transactions contain *significant* amounts of personal information, including, but not limited to, financial data, Social Security numbers, driver's license numbers, passports numbers, insurance information, and passwords. Moreover, organizations increasingly are storing this information in the cloud, which may make it more accessible to hackers than ever before. In addition, real estate companies work with a variety of vendors, and each transaction may involve several parties, providing ample opportunity for an internal or external bad actor to wreak havoc. Finally, many real estate organizations are not yet prioritizing data privacy and security. A survey of the real estate industry by KPMG found that 30 percent of organizations had experienced a cybersecurity event in the last two years, and only 50 percent of organizations said they were prepared adequately to prevent or mitigate a cyberattack.

The cyber threats plaguing the real estate industry are real, and organizations should address the significant risk to their businesses. Strong IT safeguards are just one part of the solution. Administrative and physical safeguards also are necessary when developing a comprehensive data security program or plan. Such safeguards include, but are not limited to, access management policies, awareness training, equipment inventory, and vendor assessment and management programs. Even the best safeguards cannot prevent all cybersecurity breaches. Thus, companies should be prepared to respond to the inevitable: that they will experience a data incident or breach of some kind.

Understand Risks and Vulnerabilities

Not all real estate-related organizations are faced with an equal amount of inherent business risk of a cyber breach. That would depend on factors such as the type of business, the jurisdictions in which business is conducted, and the amount and nature of the personal information involved in the business (*e.g.,* payment card data, Social Security numbers, and insurance information).

In addition, the level of risk can depend on how well an organization is prepared for the challenge. For example, members of the organization's IT staff may be adept at systems management, but are they up to the challenge when it comes to the latest cybersecurity tools and attack methodologies to provide competent leadership and execution?

Develop and Practice an "Incident Response Plan"

Organizations can develop and practice an incident response plan before a breach occurs. Steps include the following:

- Identify the internal team (*e.g.,* leadership, IT, in-house counsel, and HR). These are the persons in the business who will direct the response to any data incident. They will make quick, informed, and prudent decisions that likely will be critical to the success of the response process and, possibly, the future of the business.
- Identify the external team (*e.g.,* outside legal counsel, forensic investigators, notification vendors, and public relations). Having external members of the team identified ahead of time and any applicable contracts negotiated and agreed upon can be vital to the success of any preparedness plan. When a breach happens, valuable time can be lost trying to identify, evaluate, negotiate with, and engage third-party service providers necessary for the response.
- Consult with insurance brokers or cyber-insurance carriers to confirm applicable coverage or to discuss coverage options for cyberattacks. If coverage exists, notifying the insurance carrier should be one of the organization's first steps in response to an incident.
- Take into account all legal and contractual obligations that may affect the response process.
- Clarify the roles and responsibilities of the team members at key points in the response process: discovering the incident, investigation, coordination with law enforcement, remediation, notification, third-party inquiries, compliance, and reevaluation. This should include a well-defined decision-making process to facilitate good choices and avoid delays.
- Practice, practice, practice. It is likely that members added to the response team do not have first-hand experience with helping to coordinate a data breach response. Unfortunately, even a well-drafted plan does not give persons charged with implementing the plan proficiency in executing it. Once the organization creates its plan, it should gather its internal and external breach response team members to simulate a breach in action to help members gain valuable experience navigating the issues in a breach response, as well as working with each other. Just like a fire drill, practicing the data breach response process will help ensure any data incident is addressed in an efficient and orderly fashion.

Create Awareness Throughout the Organization

It is important that organizations create awareness of the risk of cyberattacks and of cybersecurity risks. This can include the following:

- Educate employees on how to recognize attacks and other forms of data breach.
- Instruct employees on what to do immediately if they believe an attack has occurred (*e.g.,* who to notify IT and how to disconnect from the network).
- Instruct employees on what *not* to do (*e.g.,* delete system files and attempt to restore the system to an earlier date).

Preparedness can make all the difference in the success of a real estate organization's ability to handle a cyberattack. An incident prevention and response plan is only as strong as employee awareness. Employees must understand the risks involved in maintaining sensitive data (especially in an industry where the collection and storage of such data is necessary to complete transactions) and the basic steps they can take to prevent or mitigate a cyberattack.

For additional guidance, please contact a Jackson Lewis attorney.

Focused on employment and labor law since 1958, Jackson Lewis P.C.'s 1,000+ attorneys located in major cities nationwide consistently identify and respond to new ways workplace law intersects business. We help employers develop proactive strategies, strong policies and business-oriented solutions to cultivate high-functioning workforces that are engaged and stable, and share our clients' goals to emphasize belonging and respect for the contributions of every employee. For more information, visit https://www.jacksonlewis.com.