Multifamily Preparedness Begins with an Incident Response Plan

Hurricanes, construction fires, cyber-attacks, catastrophic flooding, wildfires—just some of the many threats our industry faces on a daily basis. Given this unpredictable and volatile risk landscape, multifamily firms must be proactive in readying their communities to handle and navigate any and all crises that might come their way.

To manage risk effectively is to embed risk mitigation strategies across the enterprise and that begins with the C-Suite. Whether it's a cyber breach, impending wildfire or even a rare infectious disease outbreak, clear minded and orchestrated decision making is key. To ensure effective incident management, firms should start by creating a "Crisis Team" comprised of senior executives charged with developing the plan and carrying it out. This type of plan should be flexible and actionable regardless of whether the apartment firm is facing a potential outbreak like COVID-19 or staring down a catastrophic hurricane. Team members should include personnel from the corporate suite, risk management, human resources, legal, information technology, and operations. And team members should have decision-making and spending authority.

Write a Plan

Having a written plan in place will help organize and streamline the incident response process. The incident response players must have clarity on roles, responsibilities and authority during an incident. Without clear instructions and authorizations in place, personnel will respond inconsistently, which can be especially damaging to an organization's brand and can also create legal or regulatory risks. Similarly, without clearly identified procedures, organizations run the risk of departments duplicating efforts, wasting both time and resources. A written plan will help to provide structure, clarity and organization around the incident response process. The time to develop an incident response plan is not after your community is impacted directly.

Roles and Responsibilities

It is also imperative that the plan identify roles and responsibilities during the incident response process. The plan should clearly designate an Incident Commander, who is ultimately in charge of the response process and who has real-time decision-making authority. In particular, the plan should be clear about the scope of the Incident Commander's authority and whether any approvals are needed before certain actions can take place, especially with respect to actions affecting company systems. Similarly, the plan should identify key incident response team members (including designated back-ups) and clearly define their roles and responsibilities for the incident response process.

Communications

Perhaps one of the most important aspects of the incident response process—and one which frequently causes problems for organizations—is the communications process. It is critical that the incident response plan establish clear communications protocols, including triggers for cross-functional coordination and escalation. Key personnel are unable to carry out their responsibilities if they are unaware of incidents that require their attention.

A common communications error is neglecting to engage the appropriate parties early enough in the incident process, so clearly defined triggers for when certain departments and players need to be informed of and engaged in the response process must be established. In addition, clear protocols for when to escalate issues to senior management are also necessary. The plan should be clear as to who is responsible for re-porting to senior management and when such reporting should occur.

The issue of late engagement frequently surfaces with respect to communications with the legal department. For example, if legal is not engaged early enough in the process, the risk for non-compliance with state or federal laws (e.g., breach notification requirements) increases, which can result in or detrimentally affect government investigations or litigation. Legal is also needed for ensuring attorney-client privilege protection, which can be important in related litigation or investigations.

The plan should also include clear procedures for external communications, including who is authorized to speak on behalf of the company and what approvals are required. Because public health incidents can both be complex and have legal implications, early involvement by the legal department is also important for reviewing and approving external communications, especially public statements to the media and press.

Facts develop quickly, and many pieces of information are often unknown during the early stages of the incident response process. Apartment companies must develop a clear strategy for handling media inquiries at this early stage, such as cold calls from reporters. One way to manage this is by creating pre-developed templates or canned holding statements. Relatedly, companies will frequently experience an influx of questions from customers as well as employees outside of the incident response process during early stages of an incident.

Therefore, this process should be memorialized in the incident response plan, including: who is responsible for drafting communications for this audience; how the information will be communicated; and any associated approvals required for doing so. Finally, the plan should establish clear protocols for communications with third parties, such as: (i) law enforcement and first responders; (ii) public health officials; (iii); affected individuals and; (iv) insurance or other business contacts. Requirements or expected communications with public officials and affected individuals is often dictated by state law and can vary substantially across jurisdictions. Thus, legal counsel needs to maintain control and oversight of determining what, if anything, should be communicated and when such communication should occur to these parties.

Test Yourself & Your Incident Response Plan

A company can have a seemingly perfect plan on paper, but it can be rendered meaningless if the policies are not effective and internalized by key players in the process. Companies who test their incident response policies have a significant advantage—from both a practical as well as a liability standpoint—over those who first execute these procedures in response to a real-life crisis. Testing the incident response plan in a controlled environment allows the organization to identify and remediate gaps or deficiencies and to use the experience to prevent making similar mistakes in the future.

Implementing a clear process for documenting "lessons learned" after any type of crisis-type event—as well as ensuring this process is adequately communicated across the organization and accessible for review and consultation during events—will help reduce the veracity of any allegations that the company failed to learn from its past mistakes. Lessons learned meetings should be held regularly after live incidents as well as incident response exercises to review the effectiveness of the incident handling process and to identify necessary improvements to existing security controls and practices. The information accumulated from lessons learned meetings should be used to identify and correct any noted weaknesses and deficiencies in policies and procedures. Follow-up reports generated for each resolved incident can be helpful not only for evidentiary purposes but also for reference in handling future incidents and in training new team members. Multifamily firms should communicate these procedures and make these materials available to appropriate parties across the organization.