EXECUTIVE SUMMARY | JUNE 2016

Multifamily and Cybersecurity: The Threat Landscape and Best Practices

By CHRISTOPHER G. CWALINA, ESQ., KAYLEE A. COX, ESQ. and THOMAS H. BENTZ, JR., ESQ.
HOLLAND & KNIGHT

Overview

Cyber policy is critical to the multifamily industry because apartment companies often collect, use and maintain vast amounts of highly sensitive, personal data about residents, prospective residents and employees. The information collected is valuable to data thieves, and NMHC takes seriously the importance of a robust cybersecurity program and the need to properly educate its members on these topics.

NMHC has tasked Holland & Knight with drafting a white paper to provide an overview of the existing cyber landscape, explain the associated risks and offer best practices that will assist NMHC members in navigating ever-changing and complex cybersecurity issues.

NMHC will be releasing the complete white paper to its membership in the near future. It will be a comprehensive report that provides an in-depth analysis of the challenges facing the multifamily industry and, most importantly, provide a clear roadmap on how to implement best practices. These recommendations will aim to help organizations navigate the complexities of the cyber landscape and help ensure they have a reasonable information security program in place.

The information discussed in this document is general in nature and is not intended to be legal advice. It is intended to assist owners and managers in understanding this issue area, but it may not apply to the fact circumstances or business situations of all owners and managers. For specific legal advice, consult your attorney.

NMHC/NAA Joint Legislative Program
1850 M Street, NW, Suite 540 | Washington, DC 20036 | 202 974 2300 WeAreApartments.org

Executive Summary

The cyber risk to the apartment industry is often erroneously overlooked and underestimated. Underscoring this point is a large apartment firm suffering a well-publicized breach in 2014, causing one reporter to state, "It's time for the multifamily industry to stop ignoring the onslaught of data breach warnings. It's here. It's happening." [i]

While companies in the retail and healthcare sectors often consume the media's attention for cyber incidents, the apartment industry is no less vulnerable to these risks and is rich with valuable information that bad actors want. Cyber criminals will often follow the path of least resistance, and an industry that fails to devote the attention and focus needed on cybersecurity measures makes for a prime target, especially in an industry that maintains information about tens of millions of Americans. Apartment companies and their third-party service providers often collect, use and maintain vast amounts of sensitive financial and personal data about residents, prospective residents and employees, which can be of great value on the "dark web."

The risk to the apartment industry is elevated since apartment firms' information security programs may be relatively less developed compared to other, more heavily regulated sectors, such as banking or retail. Moreover, a risk factor that cannot be ignored is the apartment industry's reliance upon third-party providers to process and maintain sensitive information, which can open up another potential access point to cyber criminals.

Enterprise Risk Management

While multifamily firms often mitigate their direct exposure of a breach by outsourcing data collection and retention to third-party service providers, the potential damage to their brand and reputation remains at high risk. Consumers rarely differentiate between first- and third-party responsibility and hold the organization with whom they have their primary relationship—in this case, their apartment owner—responsible. For this very reason, multifamily executives must be conscious of how their contracts with third parties are drafted. In these often overlooked documents, the responsibilities, limitations and liabilities are often determined and dictate which party is financially and legally liable for breach notification, fines, identity protection services and credit monitoring, as well as other legal fees. In the past, cybersecurity was often viewed as being the sole responsibility of the Information Technology ("IT") department. Today, however, this area is increasingly viewed as an enterprise risk management process, requiring accountability and oversight at executive levels, including boards of directors. These expectations are held by federal and state regulators, and several members of Congress have recently introduced federal legislation that would legally mandate board oversight for information security programs.

Legal and Compliance

The legal framework surrounding data security and breach notification is complex and nuanced, and there currently is not a unified federal standard that governs businesses' cybersecurity practices. Instead, apartment firms face a framework composed of several sector-specific federal laws, state-by-state requirements, self-regulatory regimes and industry standards. Further, numerous federal and state agencies have begun to assert authority to take

enforcement actions in the data security space despite the absence of unified requirements. The existing patchwork of laws and regulations can be difficult to navigate, and there is no one-size-fits-all approach for multifamily firms. However, it is clear that organizations should prioritize cybersecurity risk management programs—and should do so *before* a cyber-attack comes to fruition.

Failure to prepare for cyber threats can be detrimental to a company's prosperity, and a cyber-attack can result in damage far beyond the costs to mitigate the incident. In addition to regulatory investigations and class-action lawsuits, cyber intrusions can lead to long lasting residual effects, such as impact to business operations, brand image issues and diminished consumer trust and business relationships.

Best Practices

It is essential to recognize that cybersecurity is a process and not readily achieved overnight. Preparedness is key, and it is equally vital to devote resources to incident response as it is prevention. Likewise, it will always be necessary for organizations to periodically reassess applicable cyber risks and their security posture in order to adapt to and address the evolving threat landscape and to meet legal and regulatory expectations and obligations. Development and improvement of cybersecurity programs is an iterative and ongoing process.

In the near future, NMHC will be releasing a comprehensive cybersecurity white paper that will provide in-depth analysis of the challenges facing the multifamily industry and, most importantly, provide a clear roadmap on how to implement best practices. These recommendations will be aimed at helping organizations navigate the complexities of the cyber landscape and help ensure they have a reasonable information security program in place. These selected best practices will be organized in the following categories: incident response; third-party relationships; oversight; training, awareness and enforcement; insurance; and safeguards. Below is a brief overview of why each of these categories is critical to a comprehensive data security program.

Incident Response

When a cyber incident occurs, one of the first things regulators will ask to see is the organization's written incident response plan. Having a written plan in place will help to organize and streamline the incident response process. Importantly, the time to develop an incident response plan is not after your first cyber intrusion occurs.

Perhaps one of the most central aspects of the incident response process—and one which frequently causes problems for organizations—is effective communications. The incident response plan must establish clear communications protocols, including triggers for cross-functional coordination and escalation. In addition, clear protocols for when to escalate issues to senior management are likewise crucial. The issue of late engagement frequently surfaces with respect to communications with the legal department. For example, if legal is not engaged early enough, the risk for non-compliance with federal or state laws (e.g., breach notification requirements) increases, which can result in or detrimentally affect government investigations or litigation.

Failure to adequately track incident response procedures can also create obstacles for complying with legal obligations, such as regulatory inquiries or breach notification requirements. Incident response activities will be scrutinized in the event of regulatory investigations and/or litigation, so it is imperative that the organization is able to quickly ascertain the chronology of facts known and steps taken during the incident. To ensure this ability, companies must be able to demonstrate all steps taken during the incident response process.

Third-Party Relationships

Third-party service providers often have access to a multifamily firm's sensitive data or systems. It is also important to note that service providers and suppliers typically have third-party providers of their own. If a service provider is breached—even if the service provider is at fault—the company with which the service provider is contracted is generally held responsible, at least in the public's eye and is at risk for monetary, brand or reputational damage. An organization is only as secure as its weakest link, so even if a company robustly secures its own system, if it fails to ensure that its third-party providers are doing the same, the risks for a cyber incident are much higher.

Both parties often rely on boilerplate style contracts that fail to consider necessary liability protections in the event of a cyber incident. A contract should be drafted so that the responsible party retains liability for incidents where they are culpable. It is especially important that companies establish an internal review process to ensure that these protections are included in all provider contracts that have the potential to deal with sensitive information.

Oversight

Cybersecurity is now widely viewed as a risk-management process at the enterprise level, which regulators expect senior executives and board members to directly oversee. Board members and executive management cannot effectively oversee their cybersecurity program if they are not adequately informed of the organization's risks and processes. Board members and senior management should have an active role with respect to the program and need to be versed enough to actively participate in making strategic decisions. They should also ensure they are capable of making judgments as to the adequacy of the cybersecurity program, including whether appropriate organizational structure and resources are in place. A successful cybersecurity program is largely driven by cultural expectations, and board members and executive management are in the best position to create this environment.

Cybersecurity is a continual process, which requires ongoing attention and improvements. Organizations must continually evaluate their procedures relative to the cyber threats with which they are confronted and adapt measures accordingly.

Training, Awareness and Enforcement

Having a cybersecurity policy or plan alone is insufficient. While one of the first things a regulator will request during an investigation is a copy of the organization's written incident response plan, the next thing they will ask is whether that plan was followed. Thus, key players must be trained on the incident response policy and the plan should be tested for consistency, effectiveness and operability.

Companies that test their incident response policies have a significant advantage—from both a practical as well as a liability standpoint—over those which 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. In addition, regulators expect companies to routinely test their data security programs, and doing so will help inform prosecutorial discretion should a real incident arise.

Insurance

Cyber liability insurance is complex, new to the marketplace and evolving, and with it comes a learning curve. Understanding what cyber risks are most relevant to the company is absolutely essential to the process of securing the best coverage possible. It is likewise crucial to understand your existing coverage, if it exists at all. Failure to negotiate coverage amounts, exclusions, specific dates of coverage and legal recourse options upon a cyber incident may leave the company financially vulnerable. Once you have an understanding of your cyber risk transfer needs, it is important to find a liability policy that most closely aligns with those needs and protects your company from financial and operational harm.

---

[i] Kayla Devon, *Data Breach at Essex Property Trust*, MULTIFAMILY EXECUTIVE (Sept. 30, 2014), available at http://www.multifamilyexecutive.com/technology/data-breach-at-essex-property-trust_o.