NATIONAL MULTIFAMILY HOUSING COUNCIL

MULTIFAMILY AND CYBERSECURITY

The Threat Landscape and Best Practices

Presented By: Christopher G. Cwalina, Partner and Co-Chair, Cybersecurity and Privacy Team
Kaylee A. Cox, Associate, Cybersecurity and Privacy Team
Holland & Knight LLP

July 21, 2016

WEBINAR INFORMATION

- To ensure good sound quality, all attendees will be muted during the webinar.
- To ask a question: type your question in to the Question or Chat Box on your control panel. The moderator will review and present your question to the presenter at the end of the presentation as time allows.
- The NMHC/ NAA White Paper entitled “Multifamily and Cybersecurity: The Threat Landscape and Best Practices," is available for download on the NMHC and NAA websites.
- Today’s webinar is being recorded and will also be made available on the NMHC and NAA websites.

SPEAKERS

Kevin Donnelly (Moderator)

Vice President, Government Affairs
National Multifamily Housing Council (NMHC)
202-974-2344
kdonnelly@nmhc.org

Christopher Cwalina

Holland & Knight
(202) 469-5230
chris.cwalina@hklaw.com

Kaylee Cox

Holland & Knight
(202) 469-5185
kaylee.cox@hklaw.com

I. OVERVIEW

CYBERSECURITY WHITE PAPER

- 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, which can be valuable to data thieves
- NMHC/NAA takes seriously the importance of a robust cybersecurity program and the need to properly educate its members on these topics.
- NMHC/NAA tasked Holland & Knight with drafting a white paper to provide an overview of the existing cyber landscape, explain the associated risks, and offer suggested best practices that will assist NMHC/NAA members in navigating ever-changing and complex cybersecurity issues.
- This presentation is designed to provide an overview of the white paper.

II. THREAT LANDSCAPE

KEY STATISTICS

- In 93% of cases, it took attackers minutes or less to compromise systems, while 83% of victims did not realize they had been breached for weeks or more.
- On average, unauthorized intruders are in a company's network for more than 200 days prior to discovery.
- Social engineering and ransomware attacks continue to be very successful.
- The insider threat continues to cause havoc for companies…of all the incidents types, insider misuse cases are the most likely to take months or even *years* to discover.
- Any company, in any industry, is susceptible to a cyber-attack.

CYBERSECURITY AS ENTERPRISE RISK MANAGEMENT

- In the past, cybersecurity was often viewed as an “IT problem.”
- Today, it is increasingly viewed as an enterprise risk management process, requiring accountability and oversight at senior levels.
- These expectations are held by state and federal regulators, and several members of Congress have recently introduced federal legislation that would legally mandate board oversight for information security programs.
- A vast number of CEOs list cybersecurity as one of their top concerns.

APARTMENT INDUSTRY-SPECIFIC CONSIDERATIONS

- The cyber risk to the apartment industry is often erroneously overlooked and underestimated.
- Apartment companies and their suppliers collect, use, and maintain vast amounts of sensitive financial and personal data about residents, prospective residents, and employees.
- The apartment industry is also heavily reliant upon third-party suppliers, which can increase an organization's cyber risk significantly.
- The bad guys are patient, persistent, and adaptive, and they will often follow the path of least resistance.
- An industry that does not devote appropriate attention and focus on cybersecurity measures makes for a prime target, especially in an industry that maintains information about tens of millions of Americans.

III. DATA SECURITY LEGAL & REGULATORY FRAMEWORK

LEGAL FRAMEWORK OVERVIEW

- Currently, there is not a unified federal law that regulates data security generally.
- However, there are several avenues of regulation and enforcement both at the state and federal level as well as a well-developed body of voluntary standards.
- More and more regulators are asserting authority to regulate in the cybersecurity field.
- In the absence of a unified federal standard, regulatory enforcement actions and court decisions are, in effect, creating a standard of care with respect to "reasonable" cybersecurity practices.

FEDERAL TRADE COMMISSION

- The most active regulator for data security and privacy issues is currently the Federal Trade Commission ("FTC").
- While the FTC does not have explicit authority to regulate entities' cybersecurity practices, it has assumed this authority under its consumer protection power to enforce against unfair and deceptive trade practices ("section 5 authority").
- Over the years, the FTC has ramped up its cybersecurity focus and enforcement, and a recent court opinion is likely to embolden its enforcement efforts in the field.
- Companies subject to FTC data security investigations almost inevitably result in a twenty-year consent decree, which commonly mandate that the company implement and maintain a comprehensive, written information security program and conduct third-party risk assessments and/or audits. This process is both cumbersome and expensive.

OTHER ENFORCEMENT MECHANISMS

- The Securities and Exchange Commission ("SEC") and the Consumer Financial Protection Bureau ("CFPB") have also recently taken an interest in cybersecurity matters.
- Data security is also enforced by State Attorneys General through a patchwork of varying state laws across the U.S.
- Voluntary industry standards also play an important role and may create an unofficial standard of care (e.g., PCI DSS, NIST, ISO 27000/27001, COBIT, ITIL).
- International regulators are also increasing focus on data security and privacy (e.g., Privacy Shield, General Data Protection Regulation).

IV. KEY CYBER RISKS

VARIOUS TYPES OF ASSOCIATED RISKS

- Legal and Compliance
  - Federal or state investigations
  - Class action litigation and derivative suits
  - Congressional inquiries
- Third-Party Relationships
  - Contractual obligations and liabilities
- Brand and Reputation
  - Media inquiries and public statements
- Operational and Financial
- Cyber Insurance Liability

V. BEST PRACTICES

OVERVIEW

- Cybersecurity is not an overnight process, nor is it a “check-the-box” solution.
- Achieving and maintaining a robust cybersecurity program requires periodic and ongoing evaluation and improvements.
- A well-rounded program requires diverse perspectives and the collective attention and efforts from personnel across the enterprise, both at senior management and operational levels.
- While cybersecurity measures will differ across entities and should be tailored to your organization, we will discuss general best practices to help guide members toward achieving a reasonable level of cybersecurity maturity.

AREAS OF FOCUS

- We have organized these best practices into the following main topic areas:
  - Third-party relationships
  - Oversight
  - Incident response
  - Training, awareness, and enforcement
  - Insurance
  - Safeguards

THIRD-PARTY RELATIONSHIPS
WHY THIS MATTERS

- A company is only as secure as its weakest link, so even if it 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.
- If a supplier is breached—even if they are at fault—the company with whom 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.
- One of the main areas where organizations get into trouble with third-party providers is with their contracts, which are often drafted in favor of the supplier.
- Contract language is important because it will typically limit liabilities during an incident and outline any obligations that may apply during incident investigations.

THIRD-PARTY RELATIONSHIPS
RECOMMENDED BEST PRACTICES

- Establish a process to formally conduct due diligence on supplier candidates prior to engagement.
- Develop standard contracts that include robust data privacy and security provisions.
- Periodically conduct audits and re-evaluate supplier practices.
- Develop a supplier management system.
- Limit supplier access rights appropriate to job function.

OVERSIGHT
WHY THIS MATTERS

- As mentioned, cybersecurity is now widely viewed as a risk management process at the enterprise level, and regulators expect senior executives and board members to oversee this process.
- Board members may be held accountable through derivative suits alleging violations of fiduciary duties.
- Even without legal action, the negative press alone about failed cyber oversight can impact board members' roles within an organization.
- 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.

OVERSIGHT
RECOMMENDED BEST PRACTICES

- Ensure the Board and/or senior management maintains oversight regarding the company's cybersecurity program and associated risks.
  - ❑ Institute a process to provide formal reporting on cyber risks.
  - ❑ Ensure IT/IS personnel and executive leadership are "speaking the same language."
- Conduct periodic assessments of the company's cybersecurity program.
  - ❑ Assessments can be conducted both internally and externally.
  - ❑ When conducting a third-party assessment, it is critical to involve legal counsel.
  - ❑ Be sure to timely address and act upon any identified deficiencies or recommended improvements.

INCIDENT RESPONSE
WHY THIS MATTERS

- Many companies devote the vast majority of their resources and attention on incident prevention, but they neglect to focus enough on the incident response process.
- With today's landscape, a cyber incident is virtually inevitable, so it is important to devote adequate attention to how your organization would respond.
- When a cyber incident occurs, one of the first things regulators will ask to see is the organization's written incident response plan.
- One of the most important aspects of the incident response process—and one which frequently causes problems for organizations—is the communications process.
- Many companies have brought about far more damage through poorly-managed communications during an incident than damage from the incident itself.

INCIDENT RESPONSE
RECOMMENDED BEST PRACTICES

- Develop and maintain a written incident response plan, and ensure it is consistent with other company policies and procedures.
  - ❑ Ensure key terms are defined and consistent.
  - ❑ Clearly identify roles/responsibilities, including an Incident Commander.
  - ❑ Establish clear communication protocols, including procedures for cross-functional engagement and escalations.
  - ❑ Ensure the plan addresses clear protocols for external communications (e.g., law enforcement, regulators, affected individuals, suppliers).

INCIDENT RESPONSE
RECOMMENDED BEST PRACTICES (CONT'D)

- Establish playbooks for incident prioritization and conduct business risk assessments.
  - ❑ Ensure business lines are engaged early in the incident response.
  - ❑ Identify which actions are subject to senior leadership approvals or notifications.
- Designate an incident scribe, and create a centralized repository for incident information.
  - ❑ Ensure the legal department reviews the scribe's documentation prior to distributing information outside of the response team.
- Implement a "lessons learned" process.
  - ❑ The information accumulated from lessons learned meetings should be used to identify and correct any noted weaknesses and deficiencies in policies and procedures.

TRAINING, AWARENESS & ENFORCEMENT
WHY THIS MATTERS

- Although having a written incident response plan is critical, a plan alone is not enough.
- It is important that key players are trained on the incident response policy and that the plan is tested for consistency, effectiveness, and operability.
- Implementing a consistent security and awareness training program will help ensure security practices remain top of mind for personnel and will foster a culture that values such practices.
- Companies who test their incident response policies have a significant advantage over those who do so for the first time during a real life crisis.
- Testing the incident response plan in a controlled environment allows you to identify and remediate gaps or deficiencies and can help prevent making similar mistakes in the future.

TRAINING, AWARENESS & ENFORCEMENT
RECOMMENDED BEST PRACTICES

- Test your incident response plan.
  - ❑ Simulated cyber exercises are one of the best ways to test an incident response plan.
- Implement an enterprise-wide security and awareness training program.
  - ❑ Establish appropriate "tone at the top."
  - ❑ Incorporate incident response and cybersecurity policies into onboarding materials and new-hire trainings.
  - ❑ Institute periodic "refresher" information security training for all employees.
  - ❑ Hold employees accountable by enforcement of policies and disciplinary measures, where appropriate.
- Conduct targeted security training for employees with access to sensitive information or systems.

INSURANCE
WHY THIS MATTERS

- A strong cyber liability insurance policy may offer significant protection to companies and, in some cases, may even save a company from financial and reputational ruin.
- However, cyber insurance policies are new to the marketplace, very complicated, and rapidly changing.
- Understanding what risks are most important to the company is absolutely essential to the process of securing the best coverage possible.

INSURANCE
RECOMMENDED BEST PRACTICES

- Understand your risk, and match your risk transfer needs to your cyber liability policy.
- Ensure you are permitted to use preferred experts.
- Negotiate key definitions and the retroactive date.
- Request the right to control your defense.

SAFEGUARDS
WHY THIS MATTERS

- There is no one-size-fits-all solution to cybersecurity, and it is important that entities implement collective safeguards to help protect sensitive data.
- Although cyber criminals continue to adapt and improve their tactics, they still rely on traditional tactics (in part because these antics are still successful) and will often take the easiest route.
- Implementing baseline administrative, technical, and physical safeguards can help to prevent these sorts of attacks.

SAFEGUARDS
RECOMMENDED BEST PRACTICES

- The appropriate administrative, technical, and physical safeguards for a given company will depend on its size and complexity, the nature and scope of its activities, and the sensitivity of the personal information collected from or about consumers. The following is a non-exhaustive list of examples of best practices for implementing these safeguards, which have been derived from FTC guidance and consent decrees.
  - ❑ Start with security (do not collect personal or sensitive information you do not need, and do not use such information when it is not necessary).
  - ❑ Control access to data sensibly.
  - ❑ Require secure passwords and authentication.
  - ❑ Store sensitive personal information securely and protect it during transmission.
  - ❑ Segment your network and monitor activity.
  - ❑ Secure remote access to your network.
  - ❑ Incorporate security practices in the development of new products.
  - ❑ Establish procedures to keep security current and address vulnerabilities.
  - ❑ Secure paper, physical media, and devices.

CLOSING THOUGHTS

- While businesses are expected to take these matters seriously and devote resources to developing a reasonable cybersecurity program, regulators do recognize that there is no such thing as “perfect security” (i.e., breaches are going to happen).
- What is important is that companies take reasonable steps to help mitigate these risks and implement procedures to maintain a well-managed response process.
- Devoting time and resources to your cybersecurity program before you are required to do so (before an incident happens) will go a long way in helping to manage the costs and liabilities of an incident.
- Preventing an incident altogether is likely unattainable, but what you are doing now to prepare for the incident is within your control and will dictate the severity and impending aftermath when the time comes for a real-world response.

QUESTIONS?

Christopher G. Cwalina

Partner and Co-Chair,
Cybersecurity and Privacy Team

Holland & Knight LLP
800 17th Street N.W.
Suite 1100
Washington, D.C. 20006

(202) 469-5230
chris.cwalina@hklaw.com

Kaylee A. Cox

Associate, Cybersecurity and Privacy Team

Holland & Knight LLP
800 17th Street N.W.
Suite 1100
Washington, D.C. 20006

(202) 469-5185
kaylee.cox@hklaw.com

Holland & Knight