NATIONAL
MULTIFAMILY
HOUSING
COUNCIL

Cybersecurity Strategies Checklist

As the cyber-threat landscape continues to evolve and expand, the apartment industry has prioritized cybersecurity and data privacy.

Maintaining a robust cybersecurity program is no easy feat, and it requires buy-in across the enterprise and ongoing evaluation and improvements. Having formal and standardized policies and processes is always the first step. The below checklist of data security strategies is by no means exhaustive but can serve as a jumping-off point for members interested in exploring cybersecurity best practices.

Incident Response

Develop a Written Incident Response Plan

An existing written plan will help organize the incident response process when a cyber incident occurs. This plan is often one of the first things regulators will request after an incident. An incident response plan outlines clear instructions and establishes a chain of command for responding to the event. Your incident response plan should:

- ✓ Be a preemptive exercise, not a reactive activity after a breach. Your firm should have a plan in place at all times.
- ✓ Engage your legal department as early on as possible in the response.
- ✓ Designate an Incident Commander who is in charge of the response process and has real-time decision-making authority.
- ✓ Identify roles and responsibilities and a key incident response team (including designated back-ups).
- ✓ Establish communications protocols, including triggers when certain departments need to be engaged in the response process.
- ✓ Include clear procedures for external communications and media inquiries.
- ✓ Establish protocols for communications with third parties, such as law enforcement, regulators, affected individuals and suppliers.
- ✓ Implement "Lessons Learned" reports after an incident or exercise has occurred.

Documenting Cyber-Related Incidents

Developing a robust cybersecurity program requires a database of all ongoing or previous security incidents. Doing so allows your firm to more easily comply with legal obligations, respond to regulatory inquiries, draft breach notification letters (which often have timelines for response) and learn from previous security incidents. When navigating an incident, the last thing a firm wants to do is dig through separate databases across various departments. When establishing a centralized database, your firm should:

- ✓ Ensure the database demonstrates steps taken and the chronology of facts during the incident response process.
- ✓ Designate an incident scribe (and appropriate backup) to outline all steps taken during the incident.
- ✓ Establish that the incident scribe is not also responsible for mitigating or responding to the security incident.
- ✓ Ensure the legal department reviews the scribe's documentation before distributing information to external parties.

Third-Party Relationships

Supplier Candidates

Increasingly, apartment firms rely on supplier partners for business operations. Those supplier partners also rely on suppliers for their operations. This chain often enables effective operations but can potentially be a significant source of cyber risk. If the supplier partner suffers a breach, an apartment firm may still be held accountable if something goes wrong. This is particularly true because suppliers may have access to an apartment firm's sensitive data and systems. Due diligence is necessary when vetting a potential supplier. Your firm should:

- ✓ Research the supplier to understand their business and data security and privacy practices.
- ✓ Understand what data they collect and how they use and protect it, particularly for data they have accessed from your systems.
- ✓ Vet suppliers' data security and privacy practices. This can be done in various ways, including through data security questionnaires, assessments or a formal RFP process that details their protocols.
- ✓ Check references from other clients.

Supplier Contracts

Any supplier your firm hires should have a robust security program. If/when a security incident occurs, supplier cooperation is necessary to assess what happened and the scope of the problem. Your supplier contract should include robust data privacy and security provisions, and:

- ✓ Require the supplier to immediately notify you of any suspected or confirmed data security incident involving your company's data.
- ✓ Mandate cooperation during a cybersecurity incident or investigations of your data.
- ✓ Hold suppliers liable for the incidents where they, their service providers or employees are culpable.

- Establish who holds financial responsibility in the event of legal or regulatory enforcement actions.
- Allow you the right to regularly audit the supplier to ensure they are upholding security standards.

Supplier Management Systems

A centralized supplier management system is an often-overlooked step in managing third-party risk by ensuring all supplier information is in one location. Cyber risk increases if your firm does not know the universe of its suppliers and what data and systems those suppliers can access. Your supplier management system should:

- Centrally manage a database of all suppliers, the function they serve and the data they can access.
- Be managed by one department, preferably your legal department.
- Include scheduled reevaluations of contracts to ensure the terms are still accurate and appropriate.
- Identify what access levels are essential for a supplier's services and assign rights accordingly.
- Limit access to sensitive data and provide access only as needed to carry out the supplier's job duties.

Oversight

Senior Leadership Oversight

As the cyber threat landscape expands, cybersecurity is an essential part of a firm's risk management strategy. Board members and senior executives should actively oversee this process and create a culture where cybersecurity is a top priority.

Many state data security and privacy laws already hold senior executives and/or the board responsible for data security. Further, Congress and Federal regulators are considering enacting federal requirements mandating board oversight, which will increase the stakes and underscore the importance of board- and executive-level involvement. Senior-level executives and board members are also often held financially and legally liable for lax data security or privacy breaches. As such, your firm's C-suite and board should:

- Institute a process of consistent formal reporting on cyber risks.
- Ensure technical and executive participants in the reporting process are "speaking the same language."
- Encourage technical personnel to report regularly in a manner accessible to a non-technical audience.
- Familiarize themselves with common industry terms and have a general understanding of well-known security threats.
- Be well versed in the risks and vulnerabilities so they can participate in making strategic decisions regarding the adequacy of their cybersecurity program, including whether appropriate organizational structure and resources are in place.
- Establish a process to conduct periodic assessments of the cybersecurity program.

Developing Relationships with Local Law Enforcement

Even before a cyber incident occurs, firms should build relationships with local law enforcement agencies. Identifying a specific law enforcement contact before an incident can streamline your response plan. Your firm can develop this relationship by:

- Joining your local InfraGard chapter, which serves as a public-private partnership between businesses and the Federal Bureau of Investigation. InfraGard is a no or low-cost organization to join.
- Actively engaging in the InfraGard information-sharing model on current trends and threats and establishing an ongoing relationship with the FBI.
- Once an InfraGard member, consider joining the Commercial Facilities Working Group (CCWG). CCWG is a partnership between the commercial facilities sector, InfraGard National Capital Region and the Real Estate Information Sharing and Analysis Center (RE-ISAC). CCWG encourages information sharing that is specifically relevant to the industry.

Training, Awareness and Enforcement

Testing Your Incident Response Plan

Once your firm has established a thorough incident response plan, key personnel must practice and internalize it. Testing the plan in a controlled environment will make all the difference when executing the steps in an actual incident. Proof of these test runs will be important when communicating with regulators. You can test your plan in one of two ways:

1. Tabletop Exercise: A facilitated analysis of your firm's response to a security incident in a conversational environment. Key personnel discuss simulated scenarios and assess incident response plans, policies and procedures but take no actions on live systems.
2. Operational Exercise: Simulate an actual incident (with or without a warning) with personnel seated in their usual work areas. This approach may identify tactical issues a tabletop would not reveal.

Enterprise-Wide Security Training

A strong security and awareness training program ensures your employees respond consistently to security threats. It also keeps security top of mind and—if emphasized by senior leadership—establishes a culture that prioritizes security. Your firm may have state-of-the-art technology, but without a well-trained team, your networks remain unsafe. Studies confirm that people are the weakest link in maintaining enterprise-wide cybersecurity. To develop a robust training program:

- Implement top-down messaging from senior leadership that promotes data security and privacy practices throughout the organization.
- Incorporate incident response and key cybersecurity policies into onboarding materials before new hires even have access to their computers.
- Host targeted security training for employees who will play key roles in incident response processes.

- ✓ Hold periodic refresher training to reinforce required policies and procedures and update staff on new threats.
- ✓ Establish staff accountability for data security obligations by enforcement of policies and disciplinary measures, where appropriate.

Cyber Insurance

Matching Your Risk Transfer Needs to Your Insurance Policy Selection

Cyber insurance policies are becoming common among private businesses as malicious actors become more creative. Understanding your firm's most pressing risks is essential to securing the best insurance coverage. Take stock of what your other insurance policies cover and determine any gaps a cyber policy may need to cover. Ensure your cybersecurity insurance policy allows you to:

- ✓ Use your experts and legal professionals to vet systems and procedures rather than require you to choose from your insurer's "panel list."
- ✓ Negotiate key terms in your policy based on your risk-transfer needs.
- ✓ Establish and negotiate your retroactive date. Many policies only cover cyber incidents occurring after the retroactive date, which may leave you uninsured if an incident was undetected before this date.
- ✓ Understand whether the policy is written on a "duty to defend" basis or a "non-duty to defend" basis and if there is a process for opting for a more robust level of coverage.

Additional Resources

NMHC Resources

Building out a thorough cybersecurity program may seem daunting, but fortunately, there are free resources to guide you on this journey. NMHC resources include:

- NMHC Cybersecurity Alerts System provides monthly and urgent information on industry-specific threats to NMHC members.
- 2022 NMHC Data Privacy and Protection White Paper explains recent U.S. data privacy and protection developments.
- 2019 NMHC Data Privacy and Protection White Paper offers strategies and practical considerations for firms.
- Multifamily and Cybersecurity: The Threat Landscape and Best Practices White Paper provides an in-depth analysis of the industry's data security challenges and strategies to mitigate threats.
- Smart Communities: The Internet of Things and the Apartment Industry White Paper covers well-established cybersecurity solutions and frameworks that can be used to navigate opportunities and challenges of IoT systems.