Cybersecurity & Technology Risk Management

Community associations, management companies, and third-party vendors increasingly rely on technology to support daily operations, communicate with residents, and manage financial and administrative responsibilities. Online portals, electronic payment platforms, cloud-based records, smart building systems, and digital access controls have become standard tools for modern associations. While these technologies can significantly improve efficiency, transparency, and accessibility, they also introduce new and evolving risks that boards and management teams must be prepared to address.

As associations continue to adopt and expand their use of technology, cybersecurity is no longer a purely technical concern; it is a governance, financial, and risk-management issue. Data breaches, fraud, ransomware attacks, and unauthorized system access can result in substantial financial losses, operational disruption, safety concerns, and legal exposure. Understanding how these systems function and recognizing common vulnerabilities is a critical first step in protecting the association, its residents, and its assets.

Online Payment Platforms

Online payment platforms present some of the highest cybersecurity risks for community associations because they handle sensitive financial and personal information for large numbers of homeowners. Common vulnerabilities include weak security controls, phishing schemes, and the failure to require multi-factor authentication (MFA).

Attackers frequently target owners by sending fraudulent emails that appear to come from the association or its management company, directing recipients to fake payment portals designed to capture login credentials. In other cases, hackers gain access to legitimate accounts that are protected only by a username and password. A single successful breach can expose the financial information of all owners, allow payments to be redirected, or result in unauthorized withdrawals from association accounts.

Associations should require multi-factor authentication on all payment systems and exercise heightened scrutiny when sending or responding to payment-related communications.

Maintenance Management Systems

Maintenance management platforms are essential operational tools, but they can be exploited when access controls are weak or system activity is not closely monitored.

If attackers gain access, they may alter or delete maintenance records, submit fraudulent work orders, or manipulate service histories. In some cases, false work orders may be used as a pretext to gain physical access to units or common areas. Because maintenance systems often contain detailed information about buildings, schedules, and access points, they can create both digital and real-world security risks if not properly secured.

MULCAHY LAW FIRM, P.C.
3001 East Camelback Road Suite 130, Phoenix, Arizona 85016
Phone: 602.241.1093; E-Mail: info@mulcahylawfirm.com
www.mulcahylawfirm.com

User access should be limited based on role, system activity should be monitored, and boards should recognize that digital maintenance records can enable physical access.

Communication Tools and Resident Portals

Resident portals and communication platforms are attractive targets for cybercriminals, particularly when passwords are weak or users are not trained to recognize impersonation attempts.

Hackers may pose as board members, community managers, or vendors to gain access to sensitive information, including budgets, contracts, owner lists, meeting minutes, and governing documents. Once inside the system, attackers may download data, distribute malware, or use trusted communication channels to further exploit residents or vendors.

Strong authentication requirements and ongoing user education are essential, as secure portals protect far more than routine communications.

Financial and Accounting Software

Financial and accounting systems face heightened risk due to the immediate financial impact of a breach. Threats include malware infections, brute-force login attempts, phishing attacks, and compromised computers or mobile devices.

Once unauthorized access is obtained, attackers may redirect vendor payments, alter accounting records, or transfer funds out of association accounts. These losses can occur rapidly and may not be discovered until substantial damage has already been done.

Financial systems require the strongest security controls because breaches can result in immediate and significant losses.

Visitor Management and Access Control Systems

Digital visitor management and access control systems present unique risks because they directly affect building and resident safety.

When credentials are not regularly updated or former vendors, contractors, or employees retain access, unauthorized entry becomes possible. In addition, access logs and entry data can reveal patterns about resident occupancy, potentially creating personal safety concerns.

Digital access systems must be regularly audited, as digital credentials directly translate into physical access.

Security Cameras and Monitoring Systems

Security cameras and monitoring systems are often compromised due to default passwords, weak network protections, or outdated firmware.

Unauthorized access can allow attackers to observe resident routines, disable live monitoring, or delete recorded footage to conceal criminal activity. These systems are frequently overlooked during cybersecurity planning, despite their importance to community safety.

Surveillance systems should be treated as critical infrastructure and secured accordingly.

Document Storage Platforms

Cloud-based document storage systems are at risk when permissions are poorly managed or access rights are not routinely reviewed.

Sensitive records, including financial statements, contracts, legal correspondence, and owner information, may be downloaded, altered, or shared without authorization. In some cases, financial documents may be manipulated to conceal fraud or mismanagement.

Document access should be tightly controlled, logged, and reviewed on a regular basis.

Managed Wi-Fi Networks

Association-managed Wi-Fi networks are common entry points for cyberattacks, particularly when guest networks are unsecured or networking equipment is outdated.

Once attackers gain access to the network, they may intercept personal or financial data or move laterally to access other association systems.

Wi-Fi networks should be segmented, encrypted, and maintained through regular updates and security reviews.

Smart HVAC and Building Systems

Smart building systems, including HVAC and other automated controls, often operate on outdated software and lack proper separation from administrative or financial networks.

Attackers may enter through these systems and then move laterally to access sensitive data or disrupt building operations.

Smart building systems must be isolated and secured like any other network-connected platform.

Cross-Cutting Cyber Risks

Across all technologies used by community associations, common cybersecurity risks include default settings left unchanged, phishing and human error, third-party vendor breaches, and ransomware attacks targeting financial and personal data.

While vendors may manage or host many of these systems, responsibility and liability for cybersecurity incidents ultimately rest with the association and its board.

Best Practices to Reduce Cyber Risks

Community associations can significantly reduce exposure by:

- Using strong, unique passwords and multi-factor authentication on all systems
- Verifying that payment platforms use encryption, fraud monitoring, and secure workflows
- Keeping software and firmware fully updated
- Encrypting sensitive data both in transit and at rest
- Vetting vendors and clearly defining cybersecurity responsibilities in contracts
- Conducting regular cybersecurity audits and testing
- Training board members, staff, and residents to recognize phishing and scams

Cyber insurance coverage may be available through a general liability policy, Directors & Officers policy, or a standalone cyber policy and should be reviewed with qualified insurance professionals.

Conclusion

Cybersecurity planning is an essential component of responsible community association governance. Associations that take a proactive, informed approach to managing technology risks are better positioned to reduce financial loss, legal exposure, and reputational damage. Boards that remain engaged, ask informed questions, and prioritize cybersecurity make their communities significantly less attractive targets for attackers while safeguarding residents, assets, and long-term stability.