MANAGING RISKS ASSOCIATED WITH TECHNOLOGY & DATA SECURITY

BLESSING & CURSE OF TECHNOLOGY USE BY COMMUNITY ASSOCIATIONS

Presented By:
Joel W. Meskin, Esq., CIRMS

Introduction

A few things that everyone can agree upon is that technology is touching everyone's life, it is expanding and growing faster than any one of us can keep up with and it is here to stay. The Community Association Industry is not immune to the intended and unintended consequences of the reality of technology. Like with other issues confronting community associations that is not in the face of individuals is that community associations are common interest communities where the exposures of technology do not just impact the individual, but may impact the others in their community. Accordingly, when a board of a community association is considering the use of technology, they need to knowingly consider the cost benefit analysis for their community.

We Are Just A Community Association, What Do We Need?

Many technological advancements may make things easier and more efficient in community associations, but are there liabilities that the association is taking on that would not otherwise exist? Remember, community associations existed before most of the following items that many are using more and more:

- Online banking
- Unit owner online fee and assessment payments
- Virtual Board Meetings
- Voting online or by e-mail
- Board member e-mail communication
- Community Association Website
- Association electronic/online bulletin board
- Association Facebook page
- Association computer systems
- Drones
- Board member Google research (attempts to avoid professionals)
- Security Cameras (real and decoy)
- Management Company control of technology
- Audio or Video Recording of Board Meetings

The good news for the community is that so far, it has not been a primary target as opposed to many other industries such as banks, healthcare providers, department stores and many professionals. The question is not when the community associations will be impacted, but when. It has already begun. The following are some of the potential exposures and risks we have or anticipate will happen:

- Breach of Governing Documents for use of unauthorized technology
- Unauthorized Board meetings via conference call or webex
- Challenged decisions due to unauthorized use of technology
- Data breach of electronic and or hard copy paper
- Hacking and illicit wire transfers
- Manipulation of computer programs by employees and outside third parties
- Ransomware, viruses, malware, worms, and Trojan attacks in association or management company systems controlling the data
- Invasion of privacy rights
- Unintended consequences of Board member use of personal and Business email (do you want a subpoena served on your employer because you as a board member use business email?)
- Community association Manager created exposures for community associations (i.e. the CAM is hacked or loses equipment)
- Lost or Stolen equipment (president loses his or her laptop or iPad)
- Social Engineering/False Pretenses/Phishing
- Bad research results— Use of Google in lieu of Professionals and Experts
- Drone accidents and Breach of Privacy
- Defamation
- Cyber Bullying

Who is Concerned and What Are They Concerned About?

Industry leaders and Business Partners suggest that they have concerns with the use of technology, social media, and the Internet.

Recent well-publicized breaches of security, (Target, Presidential campaign hacking) have raised concerns about security risks inherent with the use of digital technology. However, most associations do not have much actual experience with system hacking and fraud that are impacting their daily work.

Industry leaders' concerns focus on their following observations

- Association management, in general, are significantly lacking in the confidence and usage sophistication to protect themselves
- A fear of digital unknowns and reluctance to invest in cyber security has also pushed down the urgency of these issues
- Frequent association management turnover and lack of consistent training contribute to barriers for smarter digital practices
- It is clear that the bigger the management company running an association and/or the more extensive third party control of finance and the internet, the more likely the better control and security in the association
- Several interviewees pointed out that in their view, bad behavior is just or even more likely among internal employees than external agents

Association Technology Habits: Email Use—Trap for the Unwary

- Most association communication between board members and management uses personal or buisness email accounts
- IT experts are in some disagreement as to the importance of this issue
- Everyone agrees that if anyone in association management is being sued, they run the very significant risk of legal discovery of all emails whether personal or business
- Email use strongly suggest the best practice of only using dedicated association email accounts and or intranet email

Association Technology Habits: Record Keeping and Storage

- Association record keeping runs the gamut from storing dozens of boxes in someone's office or board member residence to "hands-free" control by 3rd parties (e.g., banks, off-site management companies) of all resident data.
- Many of the associations do appear to separate financial records from general resident databases. Some even have Cloud storage of critical records.
- Control of finances is usually handled by limited access to financial records and requires multiple signatures on cash disbursements.
- Many associations have professional software programs (e.g., TOPS, YARDI, VMS) that are not infallible, but do have basic access controls.

Association Technology Habits: Social Media

- There is some reported association use of social media, primarily Facebook. There was only one reported case of fraud arising from a Board President revealing his travel schedule on the community Facebook page.
- There is concern from Industry Leaders and Business Partners for any social media platform where unit owners are free to share their thoughts and state their positions.
- Most community association websites limit control of site content to one or a few individuals.

Association Technology Habits: Association Meetings

- Association meetings do not seem to evoke much concern about potential security risks, at least with board members.
- The biggest concern with association meetings currently relates to potential defamation issues.
- One issue that is being debated is the use of electronic meetings either over video conference call or normal telephonic conference calls.

Applicable Law

- Over 32 states have current statutes regarding organizational use of computers in protecting employee/resident personal identification information and how breaches need to be handled.
- While several states have condominium and home owner association dedicated cyber security.

Risk Management For Technology And Data Security

- Cyber liability, data breach & technology expertise
- Privacy Breach Response Services
- Minimize exposure
- Proactive safeguards
- Insurance

Industry Expert Recommendations for Improved Technology Security

- Hiring of third-party experienced professionals to properly handle key association functions
- Avoiding or minimizing employees handling of and access to financial transactions (other than overall statements/budgets)
- Having back-up and secure (e.g., Cloud) storage of financial and resident databases
- Having sound policies and procedures for resident communications, information collection/storage and handling financial transactions that are recognized as meeting industry standards
- Invest in management software recognized by industry leaders as meeting industry standards for security
- Conducting thorough vetting of potential association vendors and employees
- Implementing constant education of employees on sound policies and procedures

Minimize and Manage Exposure

- Do not use technology! —Yeah, right.
- Discuss with legal counsel
- Discuss with insurance professionals
- Avoid open forums for unit owners— they can come to a meeting
- Board members should not communicate in writing as it is probably not authorized, and it defeats the purpose of a board meeting where all members are together to discuss and debate an issue.

Insurance

Most in the community association, as well as in any industry these days, do not really understand the potential costs and liability that a community association or the volunteer leaders may be exposed to from Technology and Data Security issues. There are really two categories. The first involves Data Breach Response Services. The potential costs include:

- Customer notification
- Credit monitoring
- Restoration expenses
- Forensic expenses, compliance assessment fees and public relations costs
- Anti-fraud protection for customers
- Security incident investigations
- Crisis management
- Insider data breaches
- Cyber extortion/ransomware costs

The second category is third party liability where someone or some entity may bring a claim or a suit against you for something you did to them. Accordingly, this involves the carrier defending the insured(s)and if liable, potential payment of an indemnity obligation. This could include defamation, invasion of right of privacy or other claims resulting from the use, theft or misappropriate of the individuals personally identifiable information in the Insured(s)' care, custody and control of a third party on behalf of the Insured.

- Attorneys to defend your Community Association
- Settlement costs (to resolve the lawsuit amicably)
- Court-ordered damages (if you're found liable)
- Miscellaneous court costs

In this brave new world, people are trying to find where the various costs association with the consequences of these new exposures may be covered by insurance. The following are key areas where insurance coverage may be found for various costs and damages.

- Cyber Liability and Data Breach Response Insurance
    - Information Security & Privacy Liability
    - Regulatory Defense & Penalties
    - Website Media Content
    - Crisis Management & Public Relations

- Directors and Officers Liability Insurance
    - Defense of Cyber Liability Claims where the D&O is silent on the issue
    - Defense of Personal Injury Offenses i.e. Defamation, invasion of the right of privacy
- Fidelity/Crime Insurance
    - Wire Transfer Fraud Coverage
    - Computer Fraud coverage
    - Social Engineering/False Pretense

Conclusion

The inherent nature of the risks and consequences in the world of Technology and Data Security if the certainty is that what is today will be different tomorrow and the day after. Accordingly, the issues addressed in this article are moving targets. In addition, there are technology and data security experts who are far more expert in these issues than I. Ultimately, FCAR can and must track the topics over time and provide both a Best Practices Report and Generally Accepted Procedures (GAP) Report to be incorporated into CAI management education courses.

Acknowledgements

This article and the program being presented on these topics were made possible by the Foundation for Community Association Research and the FCAR Think Tank Task Force on Technology and Data Security. I would particularly like to acknowledge Kevin Davis and Mike Hardy. I would further like to acknowledge Christine Danielson Isham, FCAR Research Committee Chair and especially Melinda Kelejian Director of Development Foundation for Community Association Research. Finally, I have to acknowledge the team at Strategic Research Partners without whom this research project could not have been realized.