Wired

2018 SURVEY OF CYBERSECURITY IN COMMUNITY ASSOCIATIONS

foundation.caionline.org | www.caionline.org

FOUNDATION FOR
COMMUNITY ASSOCIATION
research

community
ASSOCIATIONS INSTITUTE

MANAGING CYBERSECURITY RISKS IN COMMUNITY ASSOCIATIONS

Plato said, "A good decision is based on knowledge and not on numbers," but sometimes knowledge is in the numbers. That's why in 2017, the Foundation for Community Association Research (FCAR) surveyed more than 600 community association managers, board members, and the professionals who support associations to identify the risks and liabilities associated with using technology to conduct association business.

The survey is one part of a three-phase research project to establish a baseline of what common technological practices associations are using and to assess which local and state regulations affecting technology apply to community associations. The results of this research are presented here to help community associations and managers become more knowledgeable about technology software, cybersecurity, social media, third-party information, and payment portals.

This information establishes a baseline of awareness and will be used to develop tools to educate community leaders about cybersecurity issues arising from social media, community websites, and third-party payment portals. It also will be used to develop professional educational materials and best practices in cybersecurity for the professionals who work with associations. Check back for more information and developments at our website: foundation.caionline.org.

The Foundation leaders are grateful to the Foundation Think Tank, who identified the need for this research and provided funding for this project, and to the members of the Technology Task Force for their volunteer leadership that ensured successful implementation and completion of this research project.

FCAR Technology Task Force

Jim Baska, CMCA, AMS, PCAM
President, Trestle Management Group

Alan Crandall
Senior Vice President, West Region
Mutual of Omaha Bank

Christine Danielson
Quaker Engineering Company
and Tuscany Estates Association

Kevin Davis, CIRMS
President, Kevin Davis
Insurance Services

Alicia Granados, CMCA, AMS, PCAM
Vice President, HOA Banking
Pacific Premier Bank

Mike Hardy
President and CEO, TOPS Software

Joel Meskin, ESQ., CIRMS
Vice President, McGowan & Company

Ashish Patel
Founder and CEO, Pilera Software

Elise Saadi, ESQ.
President, Foundation for Community
Association Research

Think Tank Members

Adrian Adams, ESQ., PCAM
Kenneth Chadwick, ESQ.
Linc Cummings
Andrew Daniels
Kevin Davis, CIRMS
Alan DeTata
John Hammersmith, CMCA, AMS, PCAM
Mike Hardy
Garth Leone
Sabine Liedel, CMCA
Lori Long, CIRMS
Michael Mendillo
Joel Meskin, ESQ., CIRMS
Robert Nordlund, RS
George Nowack, ESQ.
Ashish Patel
Jim Rademacher
Elise Saadi, ESQ.
Ellen Shapiro, ESQ.
Steve Sugarman, ESQ.
Andrew Terrell, ESQ.
Debra Warren, CMCA, PCAM
Sue York

Contributors
Dawn Bauman, CAE
Dave Jennings, CAE, SPHR
Matthew Green
Jake Gold, CAE
Mark Mavilia
Anthony Nola
Caroline Record, ESQ.
Laurianne Riley
Amy Repke
Tom Skiba, CAE
Tifinni Teagan
Bruce Townsend, CPA
Project Manager, Melinda Kelejian

OVERALL RESULTS

Although technology and cybersecurity are not yet priority issues for most community association leaders and managers, interest in and awareness of these matters are increasing. As more security and data breaches occur, states are amending and adopting laws governing the protection of personal and financial information and how breaches in these areas must be reported and addressed.

Cybersecurity: Top Concerns

Half of respondents stated they are concerned or very concerned about all types of cybersecurity threats, but fraud and theft were the primary concerns cited overall.

52% Fraud, theft

51% Storing and destroying records properly

- Communicating or posting residents' personal information

50% Theft or misappropriation of association financial records

- Posting sensitive information on association social media

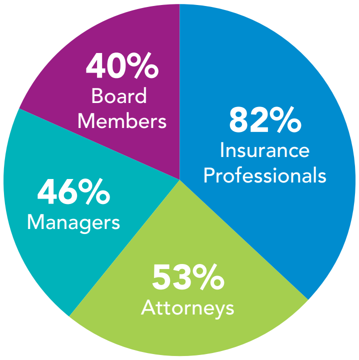
49% Security breaches in association management software

48% Defamatory posting about association management

- Defamatory posting about association residents
- Posting sensitive information on association website
- Lack of insurance for association liability/data breach events

Levels of Concern

Most respondents rated their level of concern about cybersecurity threats to their associations as strong or very strong.



Cybersecurity Breaches

Nine percent of survey respondents reported that their association, or the associations they represent, experienced some form of cybersecurity breach.

- **51 breaches** occurred within the past year.
- **Ransomware and phishing** were the most common forms of attack.
- Security breaches had **minimal financial impact** on the association. Some respondents cited lowered homeowner trust in managers/management.

Prevalence of Cybersecurity Breaches

The survey question asked: Over the past three years, has your association(s) experienced any hacking or cybersecurity breaches (e.g., hacking of association emails/communications, financial fraud using digital technology, ID theft)?

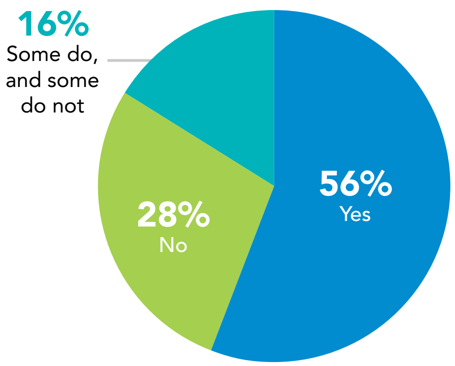
Less than 10 percent of all respondents were aware of any such breaches between 2013 and 2017. About 40 percent of the non-manager professional respondents indicated awareness of such incidents.

Number of Incidents	Management	Professionals*
None	93%	59%
1	5%	15%
2–4	2%	7%
5–9	0%	4%
10+	0%	15%

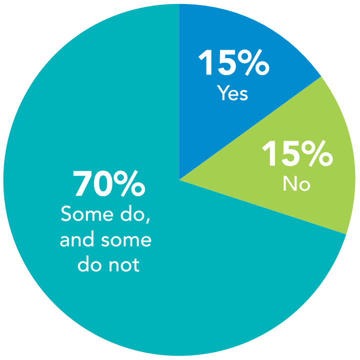
*Professionals include community association attorneys, accountants/CPAs, bankers, representatives of information technology, insurance, and security industries, and software vendors.

SAFEGUARDING MEMBER DATA

Does your association and/or the associations you represent have policies and procedures in place for collecting, storing, and protecting member information?



Does your association and/or the associations you represent keep records on paper?



What paper records does your association or the associations you represent keep?

74%	Contracts
59%	Financial records
56%	Resident contact information
34%	Resident financial records and payment data
12%	Other documents

CYBERSECURITY CASE STUDY

An insurance company revised its payment-authorization policy from single-person to two-person authorization and notified its bank that the policy change applied to all checks. The bank received the notice during a period when bank staff was being replaced, and the notice slipped through the cracks.

The head of the insurance company's accounts receivable department received an email that appeared to be from the company's president, who was out of town. The email, which included the president's signature, the company logo, and an email header, indicated that, although the president was out of town, he wanted to pay a consultant within 24 hours. Via this email, the president appeared to authorize accounts receivable to send a wire transfer for just under $10,000.

The following day, accounts receivable received another email from the president for an additional payment. By this time, however, the president had returned to the office. After some discussion, the president and the head of accounts receivable realized the company's bank account had been compromised.

Although the insurance company's president and accounts receivable manager contacted the bank immediately, they learned the money was gone. They deduced that the second email was a second attempt to get money, which may have worked if the president had not returned to the office.

Unfortunately, this scenario is common. Hackers identified the key players from the insurance company's website, which included the president's name and email address. The hackers also identified the insurance company employee responsible for processing payments. The hackers then created an email that appeared to come from the insurance company president's account requesting an amount just under $10,000—an amount that wouldn't raise red flags. Because the email looked exactly like others that accounts receivable had received, the request seemed legitimate.

The bank investigated and found that the insurance company's request for two signatures was not reflected in its account. The insurance company offered to split the loss, but the bank felt it was responsible and bore the full amount.

Lessons learned:

- Request an updated policy from your provider reflecting changes made (e.g., two signatures required for all checks).
- Include a "social engineering"* clause in your insurance policy.
- Consider listing fewer names or less contact information on your website so hackers cannot easily identify key personnel and create alias email accounts.

*Social engineering refers to cyberattacks that manipulate people to break normal security procedures.

SOFTWARE USE

Most respondents (92 percent) report that they use a software management program, and while Microsoft Excel is the most common software cited, a variety of industry-specific management programs are used by the majority of associations.

Criteria: Cost and program compatibility are the most common considerations when selecting software.

49%	Cost
46%	Compatibility with our systems
39%	Vendor or brand reputation
38%	Required by our management firm
33%	Recommendation from colleague or consultant
31%	Past experience with this company
25%	Recommended by bank, accountant, attorney
23%	Required by state law
9%	Other
7%	Saw demonstration at CAI conference

TRAINING

Who provides training on technology use and cybersecurity?

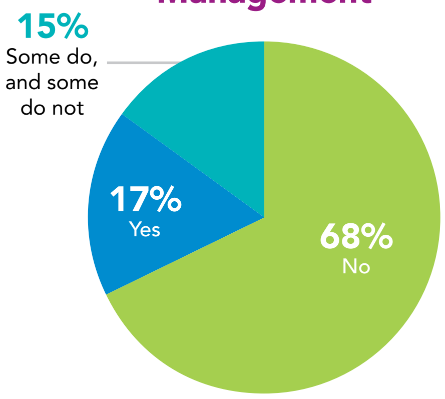
44%	No training
33%	Management company
19%	CAI
15%	IT consultant/company
10%	Attorney/law firm
7%	Bank
7%	Insurance professional/firm
5%	CPA/firm
4%	Other
3%	Independent association consultant

SOCIAL MEDIA

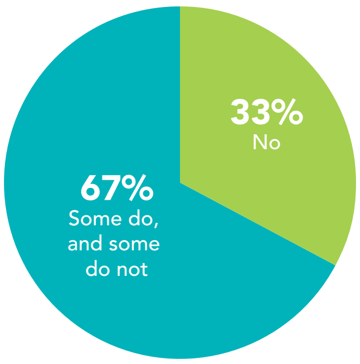
While using social media can encourage positive online interactions and build a sense of community, it also contains inherent cybersecurity risks for an association.

Are policies in place that restrict the use of social media by residents or managers in your association or those you represent?

Management



Professionals*



Most commonly used social media platforms

39%	Facebook
19%	Nextdoor
6%	Twitter

*Professionals include community association attorneys, accountants/CPAs, bankers, representatives of information technology, insurance, and security industries, and software vendors.

CYBERSECURITY CASE STUDY

A bank and a client association had established procedures for electronic transactions.

The board president's computer, which he used for association business, was hacked, and his personal email account was shadowed. When he went on vacation, he sent an email stating he would not have email access while he was away.

While he was gone, the management company received an email that appeared to be from the board president authorizing a large wire transfer. The staff assumed this was a legitimate request and submitted transaction information to the bank.

Fortunately, the bank's security protocols protected the association and management company from fraud. The bank flagged the transaction because the board president was not available for verification. Before releasing the funds, the bank took further steps to confirm the transfer, which it learned did not come from the board president.

Wire transfers are a primary target for cyber criminals, and many financial institutions now require verbal authorization (by phone or in person) before processing requests. Additionally, businesses that reconcile financial records monthly allow wire-transfer fraud to go undetected for 30 days or more. This delay makes it nearly impossible to trace and recover funds from a fraudulent electronic transaction.

The following are recommended procedures to safeguard against unauthorized electronic bank transactions:

- Require two people to authorize transactions over a certain amount.
- Maintain phone numbers and email addresses for authorized requestors.
- Refuse requests from anyone other than authorized sources.
- Require the bank to get verbal authorization, including the amount and purpose, to release funds.
- Limit the amount of a single transaction or the aggregate of multiple transactions within a short time.
- Allow wire transfers only to established and reliable association vendors or payees.

Other recommendations:

- Reconcile financial records daily or weekly to guard against unauthorized transactions. Most accounting software can be programmed to do this automatically and flag unusual transactions.
- Review and update association policies and procedures for authorizing electronic financial transactions. For example, policies should require authorization from two people for large transactions and prohibit wire transfers except in emergency situations.
- Require additional authorization to issue electronic payment to a new payee.
- Provide formal security training and written guidelines for those who handle financial information and transactions.
- Establish association-specific email accounts for board members and key volunteers to use for association communication.
- Use strong and effective software protection and competent IT support.

INSURANCE COVERAGE

More than half of survey respondents are aware that cybersecurity coverage is available or know of an insurance company that offers cyber-liability and data-breach coverage.

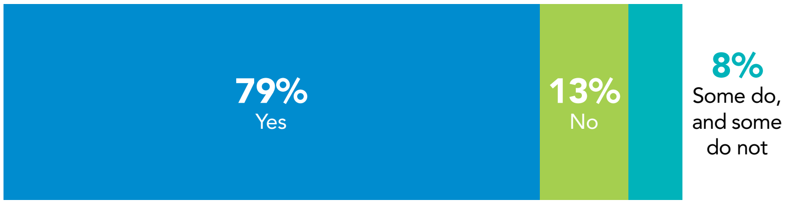
72%	Credentialed Association Manager
58%	Credentialed Management Company
50%	Non-Credentialed Management Company
36%	Association Officer or Board Member

Respondents' Top Suggestions for Minimizing Technology-Associated Risks

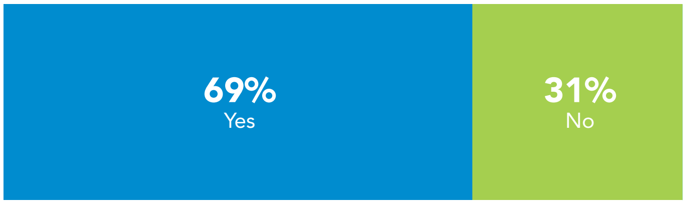
- Education, training, and seminars for community association officers and managers
- Appropriate insurance coverage and consultations with insurance agents
- Increased guidance and services from IT or cybersecurity professionals
- Adopt and implement community rules and regulations, policies, and procedures
- Password-protected community website, documents, and emails
- Restricted access to association records and data
- High-quality antivirus and malware-protection software
- Complex passwords that are changed often

Of the respondents who are aware that cybersecurity liability coverage is available, about half say they or their association clients have coverage.

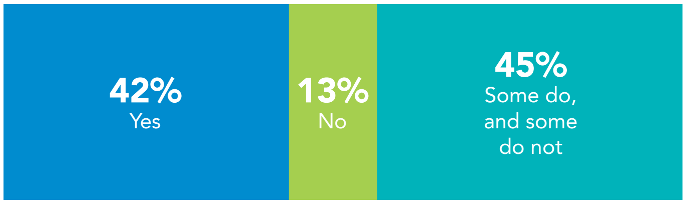
Credentialed Association Manager



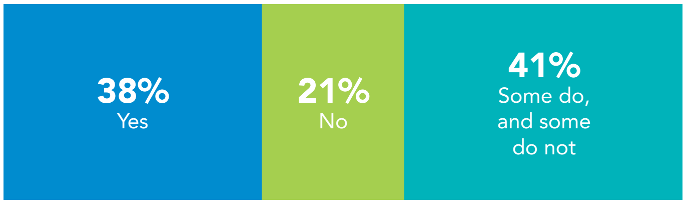
Association Officer or Board Member



Credentialed Management Company



Non-Credentialed Management Company



FOUNDATION FOR
COMMUNITY ASSOCIATION
research

ABOUT THE FOUNDATION FOR COMMUNITY ASSOCIATION RESEARCH

Our mission—with your support—is to provide research-based information for homeowners, association board members, community managers, developers, and other stakeholders. Since the Foundation's inception in 1975, we've built a solid reputation for producing accurate, insightful, and timely information, and we continue to build on that legacy. Visit foundation.caionline.org

community
ASSOCIATIONS INSTITUTE

ABOUT COMMUNITY ASSOCIATIONS INSTITUTE

Since 1973, Community Associations Institute (CAI) has been the leading provider of resources and information for homeowners, volunteer board leaders, professional managers, and business professionals in 342,000 community associations, condominiums, and co-ops in the United States and millions of communities worldwide. With nearly 40,000 members, CAI works in partnership with 36 legislative action committees and 63 affiliated chapters within the U.S., Canada, United Arab Emirates, and South Africa, as well as with housing leaders in several other countries including Australia, Spain, Saudi Arabia, and the United Kingdom.

A global nonprofit 501(c)(6) organization, CAI is the foremost authority in community association management, governance, education, and advocacy. Our mission is to inspire professionalism, effective leadership, and responsible citizenship—ideals reflected in community associations that are preferred places to call home. Visit us at www.caionline.org and follow us on Twitter and Facebook @CAISocial.

f caisocial

in Community Associations Institute

@caisocial and @caiadvocacy

6402 Arlington Blvd., Suite 500 | Falls Church, VA 22042 | www.caionline.org