INSURANCE FOCUS

CYBER SECURITY LIABILITY

Cyber security issues potentially impact all businesses, including community associations. Just as you lock the windows and doors of your community association in the real world, so too must you take protective measures in the cyber world.

What are the cyber-related issues we should be aware of?

Community associations face four main types of cyber security issues:

Cyber Breach

Theft, loss, or unauthorized disclosure of any personally identifiable non-public information or third party corporate information.

Example: When a laptop belonging to an executive of a real estate management company was stolen, management feared criminals would gain access to sensitive tenant data or personally identifiable information. The potential breach required that roughly 18,000 customers spread across 22 states be notified and their credit monitored.

Cyber thieves are after two things: information and money. All associations have bank accounts and many collect payments electronically from owners.

Cyber Hacking

Unauthorized users or organized criminals access systems to inflict financial and/or reputational damage through theft of data, data destruction, data leaks, or transmission of malware.

Example: The computer systems of a Midwest hospitality chain were attacked by "Backoff" malware, a malicious virus that targets point-of-sale systems used throughout the industry. The malware scrapped memory containing consumer payment data and injected keylogging functionality on multiple corporate machines. IT specialists worked to recover lost data and secure the networks. Approximately 96 hours were spent on the data recovery efforts.

Exposure to Social Engineering

Hacker uses non-technical methods (trickery) to induce people to break normal security procedures and create a financial exposure to a company.

Example: A scammer pretending to be the CEO of a large real estate development company emailed the firm's Director of Treasury in an attempt to induce the transfer of $50,000. The scam email claimed the funds were needed to finalize a transaction. Fortunately for the company, the quick-thinking director noticed several red flags, including the fact that the request did not follow company protocol.

June 2018

Volume 31

Number 1

Cyber Extortion

Cyber attack resulting from ransomware and the threat that involves a demand for money to avoid or stop the attack.

Example: A property manager noticed a problem, and confirmed the network was attacked by ransomware. The ransomware locked files on the main server which was the fileserver, domain controller, and active directory server, and the perpetrator demanded anonymous payment via bitcoin. The attack on the servers and computers caused the network to be unusable, and the server disconnected from workstations. As a result, new servers and a firewall router needed to be purchased and installed by a technician. Total cost of this attack came to $16,500 and 30 days of lost productivity.

Why is there cyber crime?

Cyber thieves are after two things: information and money. All associations have bank accounts and many collect payments electronically from owners.

Personally-identifying information of residents and employees, such as names, addresses, and credit card numbers, are commonly held in the computer systems of community associations. If this information is breached, it could—

- put community association members at risk for identity theft,
- cost the association money (loss of funds, compensation to members, and penalties)
- interrupt the business of the community association,
- damage the reputation of the community association, and
- put the community association at risk for lawsuits.

The simple truth is that every community association that conducts business over the internet, stores data on servers, or simply uses email is at risk.

DO YOU KNOW?

If a hacker or virus destroys computer software or data or shuts down a network, how well would your community association function?

- Would your community association members' personal data be compromised?
- Would critical operations, such as security, be affected?
- Would an incident cause loss of revenue?

Who is committing these crimes?

Information security breaches are widespread and diverse. Intruders could be professional criminals, but they could also be a teenager or an employee.

How do we keep information secure?

Safeguarding sensitive data in your files and on your computers is just plain good business. After all, if that information falls into the wrong hands, it can lead to fraud or identity theft. A sound data security plan is built on five key principles:

1. *Take stock.* Know what personal information you have in your files and on your computers.
2. *Scale down.* Keep only what you need for your business.
3. *Lock it.* Protect the information in your care.
4. *Pitch it.* Properly dispose of what you no longer need.
5. *Plan ahead.* Create a plan to respond to security incidents.

What does the law say?

In the U.S., a patchwork system of state and federal laws and regulations governs data security, privacy, and state disclosure requirements, and the laws often change. Community associations could face expensive litigation in the event of a data breach. Each community association should seek legal counsel to determine the data it owns, the implications of the loss or misuse of said data, and the steps the association would have to take in response.

Will insurance cover a cyber security breach?

Traditional policies, such as standard property and commercial general liability insurance, do not adequately deal with cyber security. The coverage is still new and not standardized, and most coverage on these policies cover hardware (computers, routers, etc.) but have little to no coverage for cyber liability exposures. The policies that do exist could cover the following:

First Party Property Coverage would address exposures such as viruses or malware, forensic expense, cyber extortion, denial of service attacks, and business interruption.

Third Party Liability Coverage would provide for such items as regulatory notification expense, legal settlements, and PCI fines and penalties.

Cyber security insurance for community associations should cover three primary areas:

- Failure to protect private data
- Failure to prevent transmission of a computer virus through the community association's web site
- Failure to provide notification of a security breach

Although policies vary, the following coverages are available:

- Business interruption
- Criminal rewards
- Cyber extortion
- Cyber terrorism
- Data breaches
- Defamation, libel, slander, infringement of copyright or plagiarism
- Identity theft
- Invasion of privacy or breach of confidentiality
- Liability arising out of data breaches
- Loss/corruption of data
- Public relations
- Restoring, recreating, regaining access to software, data, or other electronic information
- Theft of a community association laptop

Cyber risk insurance is written on a claims-made basis, providing coverage only if a claim is made during the policy period or any applicable extended reporting period.

As with all insurance, community associations must consider the types of incidents, liabilities, and related costs that these new and specialized policies will cover. An experienced broker should be able to advise the community association regarding what coverages are available and the potential strengths and weaknesses of the proposed policy.

What should we do about contractors?

Community associations should consider requiring service providers to enter into indemnity agreements covering cyber security liability.

What's the bottom line?

In today's electronic society, the need for cyber security and the insurance to cover potential liabilities is evident. If you have any questions or need further information, please contact one of the following:

- Steve Dickerson (703–205–8788 or Steve.Dickerson@usi.com),
- Theresa Melson (703–205–8753 or Theresa.Melson@usi.com),
- Jessica Knutsen (703–205–8722 or Jessica.Knutsen@usi.com), or
- Andrew Schlaffer (410–773–4312 or 703–205–8764 or Andrew.Schlaffer@usi.com).

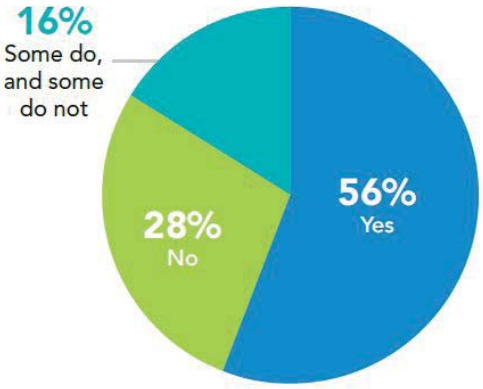
2018 SURVEY OF CYBERSECURITY IN COMMUNITY ASSOCIATIONS

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 results of this research are intended to help community associations and managers become more knowledgeable about technology software, cybersecurity, social media, third-party information, and payment portals.

The overall results showed that 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. Below are two major findings. The free report is available here: https://foundation.caionline.org/wp-content/uploads/2018/05/2018WiredBrochure.pdf. Reprinted with permission of Community Associations Institute. Learn more by visiting www.caionline.org, writing cai-info@caionline.org or calling (888) 224-4321.

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?



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

USI Insurance Services LLC

3190 Fairview Park Drive • Suite 400 • Falls Church, VA 22042
703-698-0788 • 610-362-8377 (fax)

335 Clubhouse Road • Hunt Valley, MD 21031
800-792-9800 • 610-362-8377 (fax)

Editor: Shannon R. GaNun