NAR INSURANCE PROGRAM

QUARTERLY RISK REPORT

Q2 2023

IN THE SPOTLIGHT:

DATA PRIVACY AND CYBERSECURITY

Nationwide, there recently have been high profile data breaches and an increase in identity thefts. With REALTOR® associations managing a great deal of information which includes sensitive financial data, it's important to be diligent with data privacy and to ensure cybersecurity. Already there has been an increase of seven times (7x) the number of cyber claims filed on the NAR professional liability policy than in all of last year. The following are common cybersecurity and data risks that REALTOR® associations should guard against.

1. Email Hacking

The fraudster hijacks or impersonates business email accounts (often the CEO or senior staff) to defraud the company by tricking its customers, partners, or employees into sending money or sensitive data to the attacker. Often, the fraudsters hack into the company's email by initially targeting a lower-level employee at the company. This can happen by gaining access to the account by either trying common passwords or sending employees a fake email to reset their password giving them access to confidential information.

2. Network Intrusion

Fraudsters forcibly enter a digital network without the permission of the network owner. One way fraudsters infiltrate networks are through innocuous trojan horse malware, worm viruses often hidden in peer-to-peer file exchanges (email attachments), which open the backdoor to unfettered access to a network and all its data. These viruses actively seek out specific types of confidential information and send the data to intruders waiting outside of the network.

CLAIMS REPORTED: 18

13 active demands/lawsuits | 5 potential claims

4	Employment
3	Professional Standards
3	Cyber
2	Copyright
2	Governance
1	Defamation
1	MLS
1	Membership
1	Other

3. Ransomware

Here fraudsters use malicious software to encrypt a victim's files or lock an operating system and demand a ransom payment to make them functional again. Hackers will steal and threaten to publish sensitive files if their demands are not met. Ransomware is designed to spread across a network and target database and file servers, so it can quickly paralyze an entire organization. But ransomware also can target individuals and companies of all sizes.

Weak passwords account for eighty percent (80%) of hacking-related breaches. Traditional user login and password access, known as single factor authentication, is often easy for criminals to hack into, other layers of protection are needed to prevent cybercrime losses. Multifactor authentication systems offer a second line of defense and reduce the risk of compromise to these fraudsters.

REALTOR® association executives should be aware of the risks facing not only its association, but also its members, and educate staff and members about preventative steps they can take to prevent falling victim to cybercrime.

BEST PRACTICES

DATA PRIVACY

- Collect and use information about members only where the REALTOR® association reasonably believes it would be useful (and allowed by law) to the members.
- Maintain reasonable security standards and procedures regarding access to all confidential information.
- Review agreements with vendors who handle member data and other sensitive information for data privacy safeguards and indemnity provisions.
- Do not provide any personally identifiable information to a third party without first ensuring they have data privacy safeguards and comply with applicable law.

CYBERSECURITY

- Require all staff to take annual cybersecurity and data privacy training.
- Ensure your staff know how to identify and properly handle suspicious links and attachments.
- Routinely patch and update business software and equipment.
- Backup data and files regularly, following the 3-2-1 backup strategy; 3 copies of the data in 2 different formats with 1 copy stored off-site.
- Consider using a third-party vendor to conduct phishing tests with staff.
- Require staff to change their password at least once every three months.
- Implement a multifactor authentication process requiring additional steps such as verifying user authenticity via a text message before receiving access to an email.

NAR RESOURCES

DATA PRIVACY

Data Privacy and Security Topic Page

Data Security and Privacy Toolkit

Window to the Law: Creating an Effective Data Security Plan

Window to the Law: Managing Business Records Efficiently

Window to the Law: Enforcement of Data Privacy Laws

CYBERSECURITY

Webinar: Cybersecurity Risk Opportunities for Associations

Window to the Law: Protecting Your Business from a Ransomware Attack

Window to the Law: Cybersecurity: What You Need to Know

Cybersecurity Checklist: Best Practices for Real Estate Professionals

Phishing Scams Are 'Tip of the Spear' for Cyber Threats

Safeguard Your Data

How to Thwart Hacking Threats

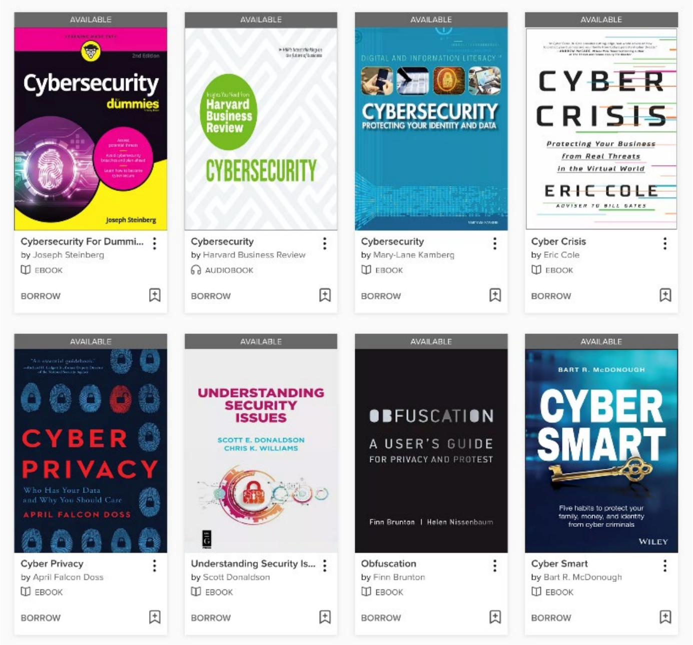
Held at Ransom

'Smishing' Texts from Scammers a Growing Cyber Threat

NAR INSURANCE PROGRAM
QUARTERLY RISK REPORT
Q2 2023

CYBERSECURITY EBOOK COLLECTION

The NAR Library & Archives has compiled a collection of eBooks about data privacy and cybersecurity to help you better understand your obligations and risks. Share this valuable collection with your board members and remind them that they have access to these books, and many more.



Cybersecurity For Dummi...
by Joseph Steinberg
EBOOK

Cybersecurity
by Harvard Business Review
AUDIOBOOK

Cybersecurity
by Mary-Lane Kamberg
EBOOK

Cyber Crisis
by Eric Cole
EBOOK

Cyber Privacy
by April Falcon Doss
EBOOK

Understanding Security Is...
by Scott Donaldson
EBOOK

Obfuscation
by Finn Brunton
EBOOK

Cyber Smart
by Bart R. McDonough
EBOOK

To access these eBooks and the entire NAR library collection, log in to NAR's eBooks site using your NAR Member ID. Be sure to select "National Association of REALTORS®" as your primary library in the drop-down menu on the sign-in page.

EPL TIP

How should an association intelligently adopt employment-focused AI tools?

Employment focused AI driven tools promise and deliver significant operational efficiencies, cost savings, and enhanced workforce and workplace outcomes. These AI tools include tools related to recruiting, talent assessment, communication, disability accommodations and safety.

However, there is no clarity on how the use of AI will be regulated by Congress, regulatory agencies and the courts, particularly in light of heightened public concern that AI algorithms are capable of discriminatory bias. Forward thinking corporations can take a pragmatic approach in adopting these AI processes.

1. Consider whether you need AI. Even if a tool promises to address your entire business, start with a specific use case—one key business activity you want to enhance—and make sure that the anticipated improvements to that process that this AI will bring will be critical to your business.

2. Investigate multiple vendors and tools and ask detailed questions: how the product was tested to ensure absence of legally significant bias; what warranties, indemnity, or other support the vendor will supply if litigation results; whether the vendor has qualified testifying experts on hand to explain and defend their work product; and whether the vendor can provide confidential references of others who have used the tool for that same purpose.

3. Once you've adopted the tool, conduct or obtain initial testing to ensure legal standard are met and work with the vendor on any necessary enhancements. Document all your efforts and review your results to make sure that the test is leading to the desired outcomes without creating a disparate impact.

This employment practices tip, and dozens more, are available to you on the EPL Assist™ website. Be sure to take advantage of this valuable benefit, which provides policy templates, sample documents, risk management resources, and advice and counsel on common employment law issues facing associations.

NAR INSURANCE PROGRAM

QUARTERLY RISK REPORT

Q2 2023

CYBER COVERAGE SUMMARY

If you experience a cyber incident, please call the Chubb Cyber Crisis Hotline 1-800-817-2665 24/7 for immediate assistance.

The NAR policy includes both **Cyber Liability** and **Cyber Response** coverages, each with a $1,000,000 limit. Cyber Liability covers losses related to network intrusion, including digital data recovery, unintentional violation of a privacy or cyber law, extortion (ransomware), and failure to properly handle, manage, or store protected information.

Cyber Response coverage includes expenses (up to $100,000 each) for services including public relations, forensic investigation, compliance with privacy laws, and specialized legal services.

Chubb offers access to enhanced benefits and services through various third party service providers to deliver extra assurance and specialized attention for their cyber policyholders.

The NAR Insurance Program provides professional liability and limited patent coverage to all eligible associations, affiliates, and MLSs.

COVERAGE CORNER

ADDRESSING COMMON POLICY QUESTIONS

Q: ***Does the policy cover losses when a vendor is attacked?***

A: Yes. The policy covers “Cyber Incidents” which includes data recovery costs for the failure of a “Shared Computer System.” A Shared Computer System is one operated for the benefit of an Insured by a third party under written contract with an Insured, including data hosting, cloud services or computing, co-location, data back-up, data storage, data processing, platforms, software, and infrastructure-as-a-service. Chubb will determine the extent of coverage when a claim is made.

Have coverage questions?
Check out these ***Professional Liability Policy FAQs*** .

RISK MANAGEMENT WEBINAR

DOLLARS AND SENSE:

FINANCIAL GUARDRAILS FOR ASSOCIATIONS

OCTOBER 5 | 1:00 PM CT

REGISTER NOW!