ProWriters
Professional & Management Liability Insurance

HOA Cyber Risk Management: Four Steps to Take Now

A homeowners association (HOA), like any organization, faces risk. From failing to maintain community common spaces to inadvertently omitting pertinent documents to homeowners, HOAs may encounter a number of claims against them. As HOAs now largely rely on digital platforms to operate, they too have become a target for cyber crime.

While it's been commonly believed that cyber actors seek out large-pocketed targets, this is no longer the case. Small organizations, especially those that collect sensitive data on individuals, are faster, easier, and more lucrative marks for the millions of hackers that specifically target low-hanging fruit.

As HOAs generally acquire private information on the homeowners that belong to their association, they often store a wealth of personally identifiable information (PII), such as:

• Property addresses • Dates of birth • Social security numbers • Bank account information • Credit card numbers

Should any of this information fall into the wrong hands, the HOA could be held liable for the damages their members suffer as a result.

Four Steps to Take to Reduce the Risk of a Cyber Attack

There's no foolproof way to reduce all risks, especially cyber risks. However, with these four simple steps, HOAs can prevent a number of potential risks and ensure they're protected when they do fall victim to a cyber event or data breach.

1) Maintain a Cyber Insurance Policy

We put this at the top of the list for a reason. Cyber risks evolve at such an overwhelming rate they're impossible to prevent altogether. A Cyber Insurance policy is the only way to ensure an HOA is protected from the vast financial damages they may face when hit with a cyber attack.

2) Adopt Strong Passwords

A strong password is a complex password. Hackers use easily accessed software that can guess thousands of password combinations in seconds (so don't even think about using Password123). A secure password includes a combination of upper and lower case letters, numbers, and symbols. The longer the password, the better.

3) Utilize Multi-Factor Authentication

Multi-factor authentication requires that users input a code or PIN number that's sent to them separately, often via email, text message, or automated phone call. They're then required to provide this code to prove their identity, making hackers face one more significant hurdle before they can access any sensitive information.

4) Conduct Regular Software Updates

While these notifications can be pesky as software updates are constantly recurring, they're important. Many software patches are completed after known vulnerabilities or glitches have been identified. Outdated software can leave a number of cracks and loopholes that cyber actors will take advantage of.