What is Cyber Insurance Coverage?

Cyber insurance is one of the fastest growing lines of insurance. There are over sixty insurance companies that are now offering standalone policies. Many more insurance companies will add some form of cyber coverage to a package or E & O policy. Yet it is one of the most misunderstood coverage. Cyber risks are more difficult to understand because those risks are both liability and property involving both first and third party issues. Plus like all professional disciplines, the insurance industry has its own jargon.

Most Cyber Policies are written on the Claims Made bases like Directors & Officers or Errors &Omissions. I have found that most of us, including insurance agents, do not fully understand claims made coverage. The most important point is that you must keep coverage in force without any lapse in coverage to preserve your retroactive date from the inception of the policy or before. Once a policy is in force, claims made policies should not be changed just for lower pricing. They should be changed if the terms are modified in such a way as they are no longer acceptable.

The most common cyber type coverage an association maintains is the computer fraud part of the crime policy. That is a property coverage to replace money taken from bank accounts by an unknown third party. The coverage is very specific and in my opinion not the most important coverage an association should write. The bank actually has the responsibility to safe guard your funds from such cyber-attacks.

There is another property lines' cyber coverage called Social Engineering Fraud. Social Engineering is when someone intentionally misleads you to send them money. The most common way is you receive an e-mail that looks like a legitimate request from a vendor or company official with instructions to pay something. If you look at the email very closely you will find it is a fraud. A good fake but a fake. They have tricked you into sending, but it is not a computer fraud claims, as you did so willingly. I have seen a couple of these claims. One in 2016 with a loss of $200,000 in several transfers. According to the adjusters handling them, they are the fasting growing claims-by-numbers and uninsured losses. Social Engineering coverage has only been available for a few years and there are only a few insurance companies that issue endorsements or policies. The number will grow as the risk continues to develop.

Cyber coverage includes both first party coverage and third party coverage. First party coverage are costs incurred by the named insured to repair or replace data, computer equipment, software and notification of affected individuals as required by law. Third party losses are to cover the cost of defense, payments to affected individuals and penalties imposed by government agencies. Policies vary and some only insure first party loss or only third party losses. Many have extensive exclusions based on what the named insured did or did not do before the loss. When purchasing this line of insurance it is very important to use the services of an agent who actually understands the risk.

The following is a quick check list. Not each business needs each of these coverages. I placed (* s) after each for exposure to common interest communities and management firms. One (*) means only if you have employees. Two (**) can be included with your crime/fidelity policy. Three (***) are the most common that will cause claims. No (*) in my opinion CICs generally do not needed that line. Does the cyber policy include?

Your computer equipment, software, data (1st Property) ***

Cyber Extortion/E Commerce Extortion (1st Property & Liability)

Security/Crises Management Expense (1st Liability) ***

Computer Fraud (1st Property) **

Social Engineering Fraud (1st Property) ***

Funds Transfer (1st Property) **

Liability for Data/Security Breach (3rd Liability) ***

Employee Privacy Liability (3rd Liability) *

Electronic Media Liability Liable and Slander (3rd Liability) ***

Security Breach Exposure (3rd and 1st Liability) ***

Regulatory Proceedings (1st Liability)

Publisher Liability (1st Liability)

H E P A (1st and 3rd Liability)

Every association is different and what data is stored and who owns the server and IP address that is breached all help determine what coverage is necessary. The size of the HOA or the management firm is important in setting limits. The equipment and software owned plus, and again, most important is the actual data stored. Do you have employees and what security measures are in place? Purchasing this coverage would be a business decision of each CIC. Coverage is available so if you do make the business decision not to purchase insurance you are, in fact, self-insured.

Why should you maintain this type of coverage? You are responsible for any website you have; for any information you have. Most CIC and Management firms have bank account numbers stored for the automatic payments of assessments. Stored are names and addresses with e-mails and phone numbers to contact members plus employee information and records. There are over fifty Federal and State laws that make you liable for losses of affected individuals when protected data is taken from you or your agent. Other than those direct losses, you are responsible for continued credit monitoring of affected individuals. Banks and other service providers that incurred expense changing accounts and EFT cards can also recover their cost from you. It is good business practice to safeguard your assets and money from loss. Cyber-attacks and Social Engineering are increasing in frequency while traditional property loss risk is less frequent. Large businesses are putting into place more safeguards to stop these cyber thieves. They have more resources in tracking these hackers down. So the hackers are now moving to small business. Most of us have first-hand experience receiving a fake e-mail or computer virus. Data is sold on the internet just to be used for identity theft. The main goal of these computer hackers is not to disrupt or upset you. It is to obtain money or steal data that can be sold for money. My opinion is that most associations and every community management firm needs to include cyber coverage as part of the insurance program they maintain.

By Mark S Coolman, CIRMS, EVP Western Risk Insurance Agency

Western Risk Insurance

Where your needs matter most!