How to Avoid Having Your Cyber Claim Denied

As online threats continue growing, businesses need to consider securing cyber insurance policies that can help defray the costs of an attack on their network or a theft of their employees' or clients' personally identifiable information. For some companies coverage is an absolute necessity.

Businesses are faced with increasing threats and cyber criminals are constantly working to devise new ways to infiltrate organizations' databases and extract information or find some way to monetize their hacks, like in the case of ransomware.

Cyber insurance can help your business recover from these events, but as with all insurance, there are risks that are covered and those that aren't вЂ“ and you often will have a certain amount of time to file a claim once you've incurred damage.

Your claim may be denied if you file too late, don't understand your coverage, don't understand your exclusions or don't get the insurance company involved early enough, according to the insurance news website *PropertyCasualty 360*.

In order to best ensure that your claim gets paid, you should do the following:

1. File your claim on time

Most cyber policies are written on a "claims made" basis, meaning they will only cover claims that are made when the policy is in effect. If someone files a claim against your company after the policy expiration, it would likely be rejected.

Some policies may include language that allows claims to be made for a few months after the policy expires, but not all policies contain this language.

Also, if your organization experiences a cyber event that may eventually lead to a claim, it's important that you notify your insurer during the policy period. This is really important because if you fail to alert the insurer about it early in the process, they may deny the claim.

You need to communicate to your staff (particularly any information technology personnel) that they need to alert management about any suspicious activity on your networks. Make sure that you create a policy for staff to report all suspicious activity so that it can be investigated further to see if it merits reporting it.

2. Understand the depth of your coverage

Because cyber policies are a relatively new phenomenon and continuously evolving, coverage will often vary from insurer to insurer.

It's important that when purchasing a policy that you sit down with us to discuss your exposures (such as if you store client credit card information on your servers). This can help us find the right coverage for your organization.

Coverage will vary depending on the type of business you are running, the technology you are using and what data or company intellectual property you want to protect.

Some policies will also require that you have specific protocols and software in place to reduce the chances of your data being hacked. For example, policies will require that the policyholder applies security patches, uses encryption technology and has a secure-socket layer to protect credit card data.

If you fail to have this in place when your policy is in effect, the insurer may reject your claim if your systems are breached.

Other areas that cyber policies will often differ on include:

- Paying for any potential legal costs after a breach.
- Paying for tools to remediate any exposure.

3. Understand what's not covered

All insurance policies have exclusions, and cyber policies are no different. There are many exclusions in cyber policies, but again, they vary from insurer to insurer. Examples of exclusions include:

- If your data is compromised when sharing it with a vendor, such as a payroll provider.
- If you have a system pipeline into a client's network and the network is hacked.
- Fraudulent entry into certain parts of your network systems.
- Patent or copyright infringement.

Again, it's crucial that you read your policy before signing and that you evaluate whether any existing or future contracts with vendors or clients fall outside the policy's coverage area.

Two of the major areas of coverage you may want to look for in exclusions are:

- Will the policy cover data that is stored outside of your network, either on the cloud or on a vendor's network?
- Will externally generated data be covered if a breach occurs within your system?

4. Get the insurer involved early

Sometimes a breach is not readily apparent. You or an employee may notice that some programs are not performing as usual.

When in doubt, reach out to us or the insurance carrier if you think you've had a breach. Even if it's just asking questions or trying to clear up your uncertainty, it's better to contact the insurance company so that the event rises to its radar.

It's better to reach out early because it will give the insurer a chance to investigate the matter and determine if there has been any exposure.

This will give you peace of mind that you will be protected should the matter rise to the level of a genuine claim.

The worst thing you can do is to wait until after you've started receiving complaints from customers, vendors or regulators. At that point your insurer will have a much more difficult task on its hands.

Getting the insurer involved early will let it get ahead of the claim, which makes managing it easier вЂ“ and it can limit the amount of fallout.

*This material was created by Insurance Newsletters and authorized for use by Brown & Stromecki Agency

###