machado
be ready for the next.

Maintain Cyber Insurance Compliance

Cyber Insurance only works when you comply with the terms.

Maintaining compliance with cyber insurance coverage is a challenge for many businesses. The following are some ways that you can take steps to ensure your business remains compliant.

1. Understand the Cyber Insurance Policy "Who" and "What"

The first step in maintaining compliance is understanding what your policy covers and how it works. Cyber insurance typically covers two types of parties:

- First-party coverage - applies to you, the policyholder
- Third-party coverage - applies to anyone else who has been effected by the event, including your customers, vendors, and others

If your policy includes third-party liability coverage, make sure that you understand who is covered under this type of coverage. You may be required to provide proof of third-party liability coverage before any claims are paid out. In addition, you need to know whether there are exclusions or limitations on the types of damages that are covered.

You should have a clear understanding of what your policy covers and what it doesn’t. This includes knowing which services are included in your policy, such as email hosting, cloud storage, backup, disaster recovery, and so forth. It also means knowing what isn’t covered, such as social media monitoring or content moderation.

A policy could focus specifically on certain types of attacks or accidents. This means that you won't qualify for coverage unless you meet those triggers. Are there any exclusions pertaining to your business practices? Some policies may exclude coverage for events that occur due to BYODs. If you allow employees bring their own devices, a policy with a BYOD exclusion will not be appropriate.

When purchasing the policy, you should also have specified what types of events are covered. These might include Network Security Coverage, Privacy Liability Coverage, and Media Liability Coverage.

- Network Security often includes theft of IP or sensitive data, ransom demand, network failures, and data breaches.
- Privacy Liability covers things like theft of devices, human error, and almost anything that network security didn't cover, like fines, crisis management, and forensic investigation.
- Media Coverage covers things like libel, trademark or copyright infringements, and online defacement (websites).

2. Know Your Responsibilities

You must also understand your responsibilities as a business. These include providing documentation and information about your organization's network infrastructure and security practices; conducting regular audits of your systems and processes; and keeping records related to incidents that occur on your networks.

3. Conduct Regular Audits

An audit ensures that your policies are being followed and that your systems are secure. A good way to conduct these audits is through a risk assessment. If you don't already do this, you should set up a system that will allow you to regularly assess your risks.

4. Have a Plan in Place

Finally, you should have a plan in place to help you respond to potential threats. This could involve having a crisis management team ready to handle situations like data breaches or other major problems.

5. Stay Current

As technology changes, so does your insurance policy. Make sure you stay current with the latest updates to your policy.

6. Be Vigilant

You need to be vigilant when it comes to cyber attacks. When you see something suspicious, report it immediately. Remember, you might not realize that something is wrong until after damage has been done.

7. Keep Records

When you notice anything unusual, take note of it. That way, you can look back at old reports later and determine if the same thing happened again.

8. Use Technology

Technology can help you monitor your networks more effectively and keep you informed about any issues that may arise.

9. Get help from an MSP

A Managed Services Provider like Machado can you help you assess your current policy and technology, establish a technology road map (a plan), and help you with ongoing maintenance and compliance.

Managed services providers are the best option for companies that need to reduce IT costs without sacrificing service levels or security.

There are many benefits of using managed services:

- Protect your systems, and monitoring and maintaining compliance with your cybersecurity policy.
- Develop a technology roadmap to understand what technology and software you have in your business today, what you need to implement to be compliant, and what tech you need to upgrade in the future.
- Reduce capital expenditures and operating expenses by outsourcing some or all of your IT infrastructure.
- Improve operational efficiency by reducing time spent managing IT operations.
- Increase productivity by freeing up resources to focus on core business activities.
- Ensure high availability and reliability of critical applications by leveraging expertise in application development and deployment.
- Enhance customer experience by ensuring that customers always receive the highest quality service.