CYBERRISKS&LIABILITIES_

4 Components of Cyber Risk Management

If your company stores data and information digitally, you should have a cyber risk management program that addresses prevention, disclosure, crisis management and insurance coverage in the event of a data breach. Good cyber risk management requires the planning and execution of all 4 of these components.

1. **Develop Strategies to Prevent a Data Breach**
Your data breach prevention strategies may include encrypting all devices used by your employees, such as laptops, tablets and smartphones. Encrypting these devices will prevent unauthorized access if a device is lost or stolen. Unencrypted devices are often not covered by a cyber liability policy, so make sure you know whether you need to encrypt the devices or not.

Your strategies may also include educating employees about phishing and pharming scams. Remind them not to click on anything that looks suspicious or seems too good to be true.

Analyze your cyber risks from three different perspectives: technology, people and processes. This risk assessment will give you a clear picture of potential holes in your security. Revisit and revise your plan regularly, because new risks arise often, sometimes even daily.

2. Know Your Disclosure Responsibilities
If you experience a data breach, you may be legally required to notify certain people. If your company is publicly traded, guidelines issued by the Securities and Exchange Commission (SEC) make it clear that you must report cyber security incidents to stockholders—even when your company is only at risk of an incident.

The SEC advises timely, comprehensive and accurate disclosure about risks and events that would be important for an investor or client to know. It's important to evaluate what information and how much detail should be released.

Notifying a broad base when it is not required could cause unnecessary concern for those who have not been affected by the breach.

Some extreme cases of a data breach may cause you to go further than just assessing and disclosing the information. You may have to destruct or alter data depending on its sensitivity.

3. Have a Crisis Management and Response Plan
Preparedness is key when developing your cyber risk management program. When you experience a data breach, you need to be prepared to respond quickly and appropriately. This is where your crisis management and response plan come into play.

Determine when and how the breach occurred, what information was obtained and how many individuals were affected. Then assess the risks you face because of the data breach and how you will mitigate those risks.

While managing a crisis, let your clients know what actions you are taking, but also be sure you're not disclosing too much information. It's a delicate balance. Focus on improving future actions—this will restore trust in your stakeholders and clients.

Your in-house lawyers, risk managers and IT department should work together to create and refine your plan. Everyone should be on board and know their responsibilities when a breach happens.

4. Protect Your Data—and Your Business
Your cyber risk management program should include cyber liability insurance coverage that fits the needs of

your business.

Cyber liability insurance is specifically designed to address the risks that come with using modern technology—risks that other types of business liability coverage simply won't cover. The level of coverage your business needs is based on your individual operations and can vary depending on your range of exposure.

Your cyber liability insurance policy can be tailored to fit your unique situation and can be written to include the costs of disclosure after a data breach. Contact Medical Society of Virginia Insurance Agency to learn more about cyber liability insurance and how you can protect your business from a data breach.