All businesses, from restaurants to landscapers to car dealers , collect some data about other people. This data collection is personally indentifying information from employees, customers or even suppliers and vendors. Right now, there are laws in place in 47 states that govern when and how a business must respond to a potential data compromise. There are also federal laws such as the recently enacted
FACTA and Red Flag laws
. In addition, it is estimated that the average cost of repairing a data compromise is currently $203 per compromised client. With the number of clients, employees and vendors that a business has, it becomes imperative that each business owner understand and give some consideration to data compromise insurance.

Despite your best efforts to protect the data that you collect, data compromises can happen in 4 different ways. There are electronic compromises where your electronic files are hacked, phished or pharmed. Your data is also vulnerable to physical compromise which includes theft of physical files or a device which contains personally indentifying information such as a laptop or backup drive or a computerized cash register. Also, your data is vulnerable to procedural compromise where someone in your organization makes a procedural mistake. Examples of this could be mistakenly posting personally indentifying information on the internet or perhaps accidentally including the social security number on a mailing label. Last of all your data is vulnerable to fraud related compromise where a sham third party company may purchase your data under fraudulent pretenses.

So what is this data compromise insurance? Well, this protection is a relatively new form of coverage and is usually simply added to an existing businessowners insurance policy . The coverage forms will vary greatly from company to company so you should read the form carefully to be sure that you know what you are purchasing. One important point: Most of these coverage forms will only pay for damages if the personally indentifying information is information that is not already public knowledge. If the only information compromised is the name and address or phone numbers, then the protection will typically not apply.

Also, while coverage forms do vary, generally this protection will pay for one of more of the following three things:

Legal and Forensic Technology Review – Provides professional legal advice as to what is required to respond to a suspected data breach. This can include the cost of the attorney as well as the cost of the computer experts to find out what was lost and how to protect data in the

future.

Notification to affected individuals – Reimburses you for your expenses of notifying the people whose data has been compromised.

Service to affected individuals – This coverage is to help the affected individuals repair their credit of take necessary steps to fix any problems that were created for them when your business experienced a data compromising event.

There are several things to consider when purchasing this protection. Always check to see if this extra protection has its own limit of liability that is different from the businessowners general liability policy limit. This is usually the case. Next, check to see if this coverage form has a different deductible than your businessowners policy. Last of all, check to see if this is a claims made type policy form or an occurrence based policy form.

At Clinard Insurance Group, in Winston Salem, NC, we work hard to help all insurance buyers become better informed consumers. If we can help you with your business insurance, please call us, toll free, 877-687-7557 or visit us online at www.ClinardInsurance.com .