Businesses today rely on technology to conduct business. How often do you think about what would happen if your computer system was breached? How soon would you know? Would you immediately know how much information was compromised? What if one of your employees lost a laptop, iPad, SmartPhone, or Thumbdrive? If you take credit card payments, are you compliant with PCI? (Payment Card Industry Data Security Standard) What if your own payroll information was lost or stolen?

All of these scenarios point to two things. First, as soon as information is breached, lost or stolen, state laws kick in which *may require* you to provide notification to your employees or clients *whether or not the information is actually compromised*. Second, you most likely have **no coverage** under your current program.

Whether a simple mistake, disgruntled ex-employee or an outside hacker, you are going to have costs before anyone even makes the first claim against you.

- Forensics costs to know what information was lost, stolen or breached
- Notification costs to let your clients or employees know there was a breach
- Monitoring costs for those people whose information was breached
- Patching the problem

For example, based on a breach of 1000 records, the cost for the internal investigation, notification and regulatory compliance is roughly $200 per record for a total cost of $200,000.

While we hear on the news about breaches suffered by large companies, small companies are also at risk. Privacy laws differ by state and may start the clock ticking even before you are aware of the problem. Laws apply based on where the client resides. Currently 46 states have laws that cover privacy and notification requirements.

Let us help you determine your risk, as a member of the Philadelphia Bar Association you have access to a proprietary Cyber Liability insurance policy designed just for you. Call or email Jenny Shazes at USI Affinity at 610-537-1456, jenny.shazes@usiaffinity.com