

Cyber Liability Insurance and Why You Need It Now

By Janet Jay

*Agency Sales and Service Representative
Physicians Insurance Agency*



News stories abound of sensitive information that was lost, stolen, or otherwise compromised. Subsequent stories follow of the dreadful effects these incidents have had on the responsible organizations as well as the affected individuals. As mobile and compact as our data has become, it's easy to understand why we are seeing increasingly frequent and large data breaches. It's convenient to store thousands of records on a keychain thumb drive, but if this data falls into the wrong hands, there's no telling

what a thief might do with it.

Our Claims Experience

At Physicians Insurance, we've seen it. With a relatively new data compromise endorsement provided on most of our professional liability policies, our insureds have begun reporting claims. The number one cause of loss in our experience – and this matches national trends – is simple negligence. Examples are missing CDs or other portable devices and laptops stolen after being left unattended.

Another area of top concern, according to a recent Ponemon study¹, is a system glitch, such as a computer virus or an error caused by software or an operator, which inadvertently leaks data or allows for easy access to the data. A few cases have made national news after Web sites leaked personal information for several minutes, hours, or even months before anyone discovered the error.

Increasing Regulation

Many states have enacted laws to protect individuals from identity

theft and to hold organizations accountable for privacy violations. Federal regulations hold health care entities to additional rules, namely HIPAA. The latest “omnibus” rule modifies and strengthens previous provisions of the privacy and security, enforcement, and breach notification rules. The US Department of Health and Human Services posts case examples of enforcement activity on its Web site², describing incidences of data breaches, and in some cases, the resulting penalties and resolutions between HHS and the responsible organizations.

The Need for Cyber Liability Insurance

Cyber liability, network security, and data compromise policies vary greatly. When purchasing a policy, it is important to know what type of risk the policy affords. Some policies simply help you notify your clients of an inadvertent release of their private information. This coverage might include assistance in determining which records were released and provide your clients with credit monitoring services. Other policies are more

comprehensive and can include additional features such as:

- Third-party liability coverage for claims alleging financial loss due to a network security or privacy breach;
- Coverage to replace your data that gets damaged, erased, or corrupted;
- Expenses associated with cyber extortion threats;
- Business interruption and extra

expense for your loss of income due to a covered loss;

- Claims alleging copyright infringement; and
- Fines and penalties associated with HIPAA and the HITECH Act.

Whatever type of policy you choose, you and others in your office who may need to access the coverage at some point (e.g., IT personnel) should be aware of what the policy covers, as well as its limitations.

¹<http://www.ponemon.org/news-2/45>

²<http://www.hhs.gov/ocr/privacy/hipaa/enforcement/examples/index.html>

Janet Jay is the Agency Sales and Service Representative for Physicians Insurance Agency. You can contact her by e-mail at janet@phyins.com or telephone at (206) 343-7300 or (800) 962-1399.

Reprinted with permission from the Oregon Healthcare News. To learn more about the Oregon Healthcare News visit orhcnews.com.