Cyber Insurance:

Not all Policies Are Created Equal

Cyber Insurance has been available in the insurance marketplace for well over a decade, but it is only in recent years that the healthcare industry has begun to embrace insurance as part of their overall risk management program. Driven in part by lower premiums, increased awareness of breaches and requirements in a multitude of funding contracts or data sharing agreements, healthcare entities of all sizes are now purchasing insurance with increased frequency.

How do you know what you're buying?

In traditional insurance products, such as general liability, auto or property, many insurance companies use standardized language as the basis of their policies. This has not been the case with the development of cyber policies. Each carrier develops their own policy language, and that language is evolving as rapidly as the technology it was designed to address.

This inconsistency in policy language has resulted in many unsatisfied policyholders at claim time when their claims are denied. The basis for these denials often lies in the policy language itself; in the definitions, exclusions, or endorsements.

When reviewing cyber coverage options, a comprehensive review of the coverage terms is critical in helping ensure that the policy will respond as you need it to in the event of a loss. It is not enough to review the limits and premiums. It is also important to note that premium is not a direct indicator of coverage. More expensive policies do not necessarily have broader coverage.

Below is a list of common policy limitations or language to consider when reviewing your cyber coverage options

What is the definition of protected or confidential information?

- Review limitations or overly specific requirements (ex. first and last name and another data set)
- Does coverage extend to both breach of individual information and confidential corporate information?
- Is there coverage if the data breached is employee data?

Does coverage extend to the following:

- Paper and electronic records
- Information in the possession of independent contractors?
- Information contained on non-owned servers or host sites? (ie cloud provider)
- Acts of rogue employees?

Are any of the following limitations or exclusions applicable:

- Violations of your own privacy policy?
- Breach of contract?
- Failure to maintain adequate security?
- Failure to maintain WPA wireless encryption?
- Unencrypted portable device?
- Cell phones or laptops?

Are the following coverages included:

- Data Breach Expenses
- Breach Coach / Legal Services
- PCI Fines and Penalties
- Regulatory Proceedings
- Computer Forensic Costs
- Cyber Extortion, Ransomware
- Business Income / Loss of Income
- Dependent Business Interruption
- Media Liability
- Network Damage
- Virus / Hacking Liability: defense and damages

Insurance is an important risk financing mechanism for healthcare entities of all sizes. Informed decision making around your cyber policy will help ensure that the policy responds the way you need it to in the event of a loss or breach.

Jennifer Wenzke Wallace
First Niagara Risk Management

FIRST NIAGARA RISK MANAGEMENT