cyber insurance policies as businesses show a greater interest in protecting themselves from data breaches and attacks, according to the Insurance Information Institute.

Dec. 15, 2016

U.S. insurers are becoming more skilled at underwriting and pricing stand-alone cyber insurance policies as businesses show a greater interest in protecting themselves from data breaches and attacks, according to the Insurance Information Institute (I.I.I.).

"More than 60 carriers offer stand-alone cyber insurance policies, and it is estimated the U.S. market is worth over $3.25 billion in gross written premiums in 2016, with some estimates saying it has the potential to grow to $7.5 billion," write Dr. Robert Hartwig, special consultant to the I.I.I., and Claire Wilkinson, author of the I.I.I.'s award-winning Terms + Conditions blog. They are the co-authors of the I.I.I.'s newly released white paper, Cyber Risk: Threat and Opportunity.

Cyber incidents were ranked as the third-highest global business risk in 2016, Allianz's Risk Barometer determined. The average cost of a breach in the United States reached $7 million in 2016, a Ponemon Institute survey cited in the I.I.I.'s report found. Most traditional commercial general liability policies do not cover cyberrisks.

Tailored to a business' specific needs, a stand-alone cyber insurance policy typically offers the following coverages, the I.I.I.'s white paper explains:

Liability—Covers the costs (e.g., legal fees, court judgements) incurred after a cyberattack, such as data theft, or the unintentional transmission of a computer virus to another party, causing them financial harm.

Crisis Management—Covers the cost of notifying consumers about a data breach

network that limits its ability to conduct business.

Cyber Extortion—Covers the "settlement" of an extortion threat against a company's network, as well as the cost of hiring a security firm to track down the blackmailers.

Loss/Corruption Of Data—Covers damage to, or destruction of, valuable information assets as a result of "viruses, malicious code and Trojan horses," the white paper states.

Criminal Rewards—Covers the cost of posting a criminal reward fund for information leading to the arrest and conviction of a criminal who has attacked a company's computer systems.

Data Breach—Covers the expenses and legal liability resulting from a data breach.

Identity Theft—Provides access to an identity theft call center in the event of stolen customer or employee personal information.

Cyberrisks, however, remain challenging for insurers to underwrite, Dr. Hartwig and Ms. Wilkinson acknowledge. The three reasons the paper cites include the constantly changing range of perpetrators, targets and exposure values; a lack of historical actuarial data; and the interconnected nature of cyberspace, which makes it difficult for insurers to assess the likely severity of cyberattacks.

Small Business