THE COUNCIL

The Council of Insurance Agents & Brokers

joel.wood@ciab.com or
joel.kopperud@ciab.com

CYBER INSURANCE

BACKGROUND

Cyber insurance is important because every business that maintains electronic data or systems is at risk of a cyberattack or data breach. Insurance creates incentives that drive behavioral change. The simple act of applying for insurance forces insureds to assess their intangible asset risks and the strength of their cyber defenses. This process is a critical risk mitigation tool being led by brokerage firms across the country.

The main components of a cyber insurance policy include Liability, Event Response, Business Interruption and Cyber Extortion. Tangible property, bodily injury and loss of company funds are generally excluded, although some carriers are starting to offer property damage policies in the market. In the face of increasing buyer demand, the insurance industry is focused on educating clients, addressing capacity and pricing issues in certain sectors, and quickly innovating to develop creative solutions.

Cyber risk is a relatively new peril so there is not much historical data on the likelihood and cost of a cyber loss event, which is needed to underwrite and price the coverage. Time will help solve this deficiency, but in the meantime, the Department of Homeland Security (DHS) has established a working group, comprised of CISOs and CSOs from various critical infrastructure sectors, insurers and other cybersecurity professionals, to design a Cyber Incident Data Repository (CIDAR).

THE COUNCIL'S MARCH 2016 CYBER INSURANCE SURVEY

- 25% of respondents' clients purchased some form of cyber insurance
- Policyholders continue to prefer – and were advised to select – standalone cyber policies (66%) over embedded coverages (34%), which respondents believe tend to be less comprehensive
- Capacity is generally available to meet policyholder needs, but it can sometimes be a challenge to get adequate limits for clients in the high-target industries, such as technology, finance, and healthcare
- Only 35% of respondents' clients had an information security program in place with capabilities covering prevention, detection, containment and response/eradication

OUR POSITION

The Council believes that the cyber insurance market must be allowed to grow and mature without undue government and regulatory intervention, however, The Council supports:

- Legislation that would replace the patchwork of state data breach notification laws and create a single national standard for reporting data breaches. This would ease some of the compliance burden that businesses face in the wake of a data breach.
- Legislation introduced by Rep. Ed Perlmutter (D-CO) , "The Data Breach Insurance Act" (H.R. 6032), which would provide a tax credit equal to 15% of cyber insurance premiums to organizations that purchase this coverage and

joel.wood@ciab.com or
joel.kopperud@ciab.com

adopt the NIST Cybersecurity Framework. Such financial incentives could make companies safer by encouraging them to adopt more robust cyber defenses, while their cyber insurance would help them recover after a breach incident.

- DHS's work facilitating the creation of cyber incident repository. Because DHS does not intend for this repository to be housed in the government, a private sector entity will need to stand up and maintain such a repository if it is ever to become a reality.

ABOUT US

The Council of Insurance Agents & Brokers is the premier association for the top regional, national and international commercial insurance and employee benefits intermediaries worldwide. Council members are market leaders who annually place 85 percent of U.S. commercial property/casualty insurance.