Cyber Risk Profiling for Agents and Brokers

In 2016, the cyber insurance marketplace was valued at $2.5 billion and industry experts forecast it will grow to $7.5 billion by 2020. Current models used by agents, brokers, and underwriters to assess an applicant's cyber risk profile is predicated on legacy understandings of how to reduce the likelihood of a cyber claim.

This approach exposes carriers to unnecessary risk of future claims as damages associated with cyber breaches and system disruption/ destruction becomes more cost intensive. These issues are compounded by regulatory mandates such as the General Data Protection Regulation (GDPR) or State of New York's Department of Financial Services (NYDFS) Cybersecurity law.

The biggest challenge to underwriters today is how existing questions limit the response of an applicant or more importantly, ***what questions are not even being asked.***

HEMISPHERE's President & CEO Carter Schoenberg began collaborating with the U.S. Department of Homeland Security (DHS) Insurance Working Group in 2013. This group of private and public sector leaders assessed what needs existed to improve cyber risk profiling. In 2015, HEMISPHERE worked closely with the National Association of Insurance Commissioners (NAIC) Cyber Working Group and insurance industry stakeholders to construct a better model that improves the evaluation criteria of any applicant seeking a cyber policy.

Our proprietary model is powered by HEMISPHERE's subject matter expertise and leverages decades of real world experience in root cause analysis, determining legal liability exposure, and costing of cyber risk; pre-event and post event. Unlike other offerings that attempt to illustrate ***maximum exposure***, we focus on controls and techniques to ascertain an applicant's ***most likely exposure*** and why.

Our online examination will allow any organization to rapidly complete an assessment to determine cyber maturity. Other surveys and quizzes are available online, so how is Cyber Risk Exam better?

- ◊ Materials are derived from lessons learned from insurance and cyber risk experts.
- ◊ Questions are designed to allow for multiple responses with an automated weighting system for each question answered.
- ◊ Industry stakeholders can create key performance indicators (KPIs) that drive future changes to stand alone cyber policies, technology errors and omissions—with defined cyber breach or cyber event coverages, or crime/ransom policy applications.
- ◊ Application cannot be "gamed" as it uses a questionnaire format that inherently assess accuracy and integrity of answers.
- ◊ White labeling styles available for competitive positioning.

Your Gateway To Cyber Risk Management

This model is predicated on the Capability Maturity Model Integration (CMMI) to provide better data affording:

- ◊ **Reduces labor costs of review process by over 50%.**
- ◊ **Better fidelity into what actually causes harm triggering a claim.**
- ◊ **Accounts for cyber risk as a business peril and not simply an information technology issue.**
- ◊ **Customizable to meet the rapid and dynamic cyber threat landscape through weighted scoring techniques.**

HEMISPHERE's capabilities allow us to translate cyber threats into business risk demonstrating how to reduce costs of ownership improving security and cyber risk investment strategies.

Email: contact@hemispherecyber.com

Office: (703) 881-7785

10432 Balls Ford Road, Suite 300

Manassas Virginia 20109