

Pivoting to Fortify our Digital Self: Revealing the Need for Personal Cyber Insurance

Authors : Richard McGregor, Carmen Reaiche, Stephen Boyle

Abstract : Cyber threats are a relatively recent phenomenon and offer cyber insurers a dynamic and intelligent peril. As individuals en mass become increasingly digitally dependent, Personal Cyber Insurance (PCI) offers an attractive option to mitigate cyber risk at a personal level. This abstract proposes a literature review that conceptualises a framework for siting Personal Cyber Insurance (PCI) within the context of cyberspace. The lack of empirical research within this domain demonstrates an immediate need to define the scope of PCI to allow cyber insurers to understand personal cyber risk threats and vectors, customer awareness, capabilities, and their associated needs. Additionally, this will allow cyber insurers to conceptualise appropriate frameworks allowing effective management and distribution of PCI products and services within a landscape often in-congruent with risk attributes commonly associated with traditional personal line insurance products. Cyberspace has provided significant improvement to the quality of social connectivity and productivity during past decades and allowed enormous capability uplift of information sharing and communication between people and communities. Conversely, personal digital dependency furnish ample opportunities for adverse cyber events such as data breaches and cyber-attacks thus introducing a continuous and insidious threat of omnipresent cyber risk-particularly since the advent of the COVID-19 pandemic and wide-spread adoption of 'work-from-home' practices. Recognition of escalating inter-dependencies, vulnerabilities and inadequate personal cyber behaviours have prompted efforts by businesses and individuals alike to investigate strategies and tactics to mitigate cyber risk - of which cyber insurance is a viable, cost-effective option. It is argued that, ceteris parabus, the nature of cyberspace intrinsically provides characteristic peculiarities that pose significant and bespoke challenges to cyber insurers, often in-congruent with risk attributes commonly associated with traditional personal line insurance products. These challenges include (inter alia) a paucity of historical claim/loss data for underwriting and pricing purposes, interdependencies of cyber architecture promoting high correlation of cyber risk, difficulties in evaluating cyber risk, intangibility of risk assets (such as data, reputation), lack of standardisation across the industry, high and undetermined tail risks, and moral hazard among others. This study proposes a thematic overview of the literature deemed necessary to conceptualise the challenges to issuing personal cyber coverage. There is an evident absence of empirical research appertaining to PCI and the design of operational business models for this business domain, especially qualitative initiatives that (1) attempt to define the scope of the peril, (2) secure an understanding of the needs of both cyber insurer and customer, and (3) to identify elements pivotal to effective management and profitable distribution of PCI - leading to an argument proposed by the author that postulates that the traditional general insurance customer journey and business model are ill-suited for the lineaments of cyberspace. The findings of the review confirm significant gaps in contemporary research within the domain of personal cyber insurance.

Keywords : cyberspace, personal cyber risk, personal cyber insurance, customer journey, business model

Conference Title : ICMCCP 2023 : International Conference on Management Cybernetics and Core Principles

Conference Location : Sydney, Australia

Conference Dates : March 27-28, 2023