Silent Cyber Assessment Framework

The (re)insurance industry is faced with a growing risk related to the development of information technology (IT). This growth is creating an increasingly digitally interconnected world with more and more dependence being placed on IT systems to manage processes. This is generating opportunities for new insurance products and coverages to directly address the risks that companies face. However, it is also changing the risk landscape of existing classes of business within non-life insurance where there is inherent risk of loss as a result of IT events that cannot be or have not been excluded in policy wordings or are changing the risk profile of traditional risks.

This risk of losses to non-Cyber classes of business resulting from cyber as a peril that has not been intentionally included (often by not clearly excluding it) is defined as non-affirmative cyber risk and the level of understanding of this issue and the Cyber peril exposure from non-Cyber policies varies across the market. In contract wordings the market has remained relatively "silent" across most lines of business about potential losses resulting from IT related events, either by not addressing the potential issue or excluding via exclusions. Some classes of business recognise the exposure by use of write-backs. Depending on the line of business the approach will vary as to how best to turn any "silent" exposure into a known quantity either by robust exclusionary language, pricing or exposure monitoring.

This paper proposes a framework to help insurance companies address the issue of non-affirmative cyber risk across their portfolios. Whilst the framework is not intended to be an all-encompassing solution to the issue, it has been developed to help those tasked with addressing the issue to be able to perform a structured analysis of the issue. Each company's analysis will need to tailor the basis of the framework to fit their structure and underwriting procedures. Ultimately the framework should be used to help analysts engage with management on this issue so that the risk is understood, and any risk mitigation actions can be taken if required.

Also included is a worked example to illustrate how companies could implement the framework. The example is entirely fictional, is focused on non-life specialty insurance, and is intended only to help demonstrate one possible way in which to apply the framework.

Visesh Gosrani
Chair, Cyber Risk Working Party
December 2019