Cyber risk is one of the most pressing public topics being addressed as a strategic priority in corporate boardrooms and in governments across the globe. The growing concern with cyber risk is driven by the increased global reliance on technology and the rising number of cyber attacks. As industrial control systems for critical infrastructure migrate to cyber, and as we become increasingly dependent on e-commerce and cloud computing, the susceptibility to cyber risk increases exponentially.

In its broadest form, cyber risk is synonymous with information technology (IT) risk. According to the ISACA Risk IT Framework Excerpt, 2009 it is “The business risk associated with the use, ownership, operation involvement, influence and adoption of IT within an enterprise.”

Cyber attacks represent a present and growing danger that threatens businesses irrespective of size and sector.

Risk aggregation is another concern for businesses, insurers and reinsurers, given the possibility of single attacks leading to losses across a large number of firms. The nature of cyber risk makes it possible for re/insurers to suffer losses from a vast number of insureds spread across different geographies as a result of a single event. A large systemic risk has not yet materialised, but this does not mean the risk is not present.

Physical losses are a growing concern, both in terms of severity and frequency, given the interconnectedness of cyber space and the physical world. One example of this new category of risk can be seen in the way that industrial control systems operate in the energy sector. These new generation control systems expose the sector to a host of cyber security risks that are only just beginning to be understood. The current size of the cyber breach and privacy market is approximately $2 billion and is expected to grow to approximately $5 billion over the next five years as the number of first-time purchasers increases at a rapid pace. Cyber-related risk mitigation efforts and post-event remediation are gaining importance, as shareholders, regulators and rating agencies are increasingly focused on enterprise risk management (ERM).

The potential catastrophic loss and the size of remediation costs following an industrial infrastructure event or a data breach have not been widely known to insurers. There is limited history, lack of data and emerging exposure, making it difficult for insurers to measure cyber risk and calculate capital needs.

Cyber risk is already an embedded feature of the global risk landscape, not only as a privacy/network liability, but also as a peril affecting traditional insurance lines. As such, insurance has the potential to greatly enhance cyber risk management and resilience for a wide range of organisations and individuals who are exposed to its impacts.

The re/insurance market is grappling with how the peril of cyber and its exposure can be managed within specialty, casualty and property reinsurance programmes. The insurance market has developed a dedicated product line to address the initial risks faced by companies, such as data breach and business interruption due to network failure.

Underwriters of traditional insurance businesses have also responded, in some cases, with the introduction of several endorsements to address disclosure or access of confidential personal information within the commercial general liability policy. This has created a complex picture with a mix of implicit and explicit cover as well as a number of exclusions to contend with.

With this mix, ascertaining the true level of cover for any given cyber risk scenario can be a challenging exercise.
Cyber gaps and exclusions in traditional policies, along with the emergence of standalone cyber insurance solutions for new risks, produces a situation where businesses struggle to fully comprehend the boundaries of their cover.

**OPPORTUNITIES AND CHALLENGES**

There are significant opportunities for the re/insurance industry. For re/insurers, there is an opportunity for innovation with the development of models that can measure and quantify cyber risk to determine pricing, correlated loss and capital support.

With the opportunities come challenges. Data will be a key factor for enabling further analysis and the development of models to enhance the understanding of cyber risk. The systemic, intangible and constantly evolving nature of cyber threats presents significant challenges for gathering the data required to achieve accurate quantification of the risk for insurance portfolios that could trigger a wide range of economic losses on a global basis.

The key function of modelling is trying to determine what the likelihood of an event occurring is and, once that happens, what the size of that loss might be. But, the level of historical data that has been used to build probabilistic models for natural catastrophes does not yet exist for cyber risk. Re/insurers have little information when assessing the severity and frequency of possible cyber catastrophe scenarios. Add in the potential for multiple insureds being implicated in a single breach, and the scope of the necessary modelling needed in this emerging risk class is daunting.

Re/insurers meeting these challenges would benefit by enhancing the quality of data available and continuing the development of probabilistic modelling, particularly regarding potential loss accumulations.

**SOLUTIONS**

In efforts to quantify potential loss, much of the industry continues to rely on multiple models and actuarial approaches that encompass items such as model applications, probable maximum loss estimates, realistic disaster scenarios, experience and exposure ratings to create a broad set of scenarios and deterministic views.

New data and modelling applications are being synthesised and adapted within existing model frameworks allowing carriers to better underwrite and manage these risks. Other applications involve identifying and quantifying emerging ‘aggregating’ exposure concentrations such as those resulting from global supply chain dynamics. Other niche models, such as Guy Carpenter’s MetaRisk Reserve, can focus on various ‘crystallising’ emerging threats emanating from the accumulation of systemic reserves over multiple years.

As the level of sophistication and tools for deterministic modelling capabilities increases, the next step that arises is the more challenging leap toward a more probabilistic and holistic model approach.

A casualty catastrophe model must consider the complexities of damage and liability that will not be contained in one geographic area or one industry.

GC ForCas has been developed as a platform with model components to cover US commercial lines losses resulting from casualty catastrophes. It is an experienced-based model that groups historic losses into three main perils: sudden disasters, financial institutions and cyber. GC ForCas leverages a variety of industry sources to model loss scenarios and line of business dependencies. Through the modelling process industry portfolio concentrations will be uncovered by mapping exposures and analysing the interrelationships among those industries.

The GC ForCas Cyber component has been developed to examine cyber liability risk at the portfolio level. Events may include data breach/privacy liability, network security liability, business interruption and data asset protection, among others.

As re/insurers place more emphasis on ERM, proper assessment requires relative quantification of the various risks to the firm, including cyber, in addition to the absolute quantification of each of them. These risks relate to underwriting, reserve/payout pattern, reinsurance and traditional catastrophe risk. Guy Carpenter’s MetaRisk and BenchmaRQ are standardised economic capital models empowering decision makers with a deeper view of risk drivers.

Guy Carpenter has developed these and other tools and solutions to help our clients better understand, manage and quantify their cyber risks, with the goal of turning them into opportunities for growth.

For more information visit: www.guycarp.com