Cyber

Introduction

Capital providers, ERM directors and regulators are beginning to ask questions about the insurance risk management of cyber (IT related) insurance. In particular, aggregated losses are a concern. While the science and technology of IT and its many uses have not in principle changed very much in recent years the emerging problem for insurers is most likely related to the way in which the insurance market has developed in response. For example, insurers have been providing both specialist and non-specialist policies - where the type of loss anticipated was some combination of the cost of service-based responses[1] and indemnity services such as consequential loss[2]. It could be argued that specialist providers have developed risk rating systems and aggregation management systems to this end, but it is much less likely that a marine insurer who provides such cover in a marine policy has done the same degree of work on the topic.

Stand-alone *cyber* policy providers are beginning to find that their colleagues in other lines of business are taking market share, often without any specific premium provision. Indeed many insureds are beginning to realise that their property policy etc. has, in effect, been providing IT failure-related cover at no cost, and with no specific wordings or risk analysis, for quite some time.

Rather than focussing on malicious attack and virus problems, insurers in general might do better to regard IT as a very common mechanism through which malice, acts and omissions may trigger an insurance policy. Aggregation of such losses may be caused by a common technical event[3] or by the way in which insurers have selected risks, or by both mechanisms.

Understanding the ways in which IT events may trigger traditional insurance policies and may trigger "cyber" policies is key to tackling risk rating, risk selection and potential aggregation.

In the last issue of the *Radar* journal I suggested that insurers analyse "type of loss" scenarios so that policy wordings could be made more explicit, exposure risk factors could be identified, new covers could be offered, classes of insurance risk could be created and claims trends made relevant to those classes. Prevention and mitigation measures, which actually protect the insurer as well as the insured, could be promoted.

Where necessary, triggers could be re-defined and questions about the meaning of causation and its proof could be addressed. In addition, the definition of 'event' would be crucial to the proper operation of re-insurance.

One problem with this approach is the multidisciplinary nature of the expertise required. Cyber specialists don't know enough about property insurance, UK motor insurers don't know enough about IT. It would help if there was an information exchange.

---

[1] Such as forensic investigation, notification of third parties, credit monitoring...

[2] At present, this is what people usually mean when they talk about "*cyber insurance*". However, the scope of IT-related failures which could trigger an insurance policy is much broader than this.

[3] For example,

- Power outage (policy affected = property, business interruption…)
- Software bug (policy affected = product liability, EL…)
- PayPal error
- Data loss (policy affected = cyber (malicious attack), business interruption…)
- CPU error (a bit like the problem envisaged for Y2K) (product liability, theft…)
- Bitcoin and other block chain services hack (e.g. at the password level)
- Experian hack

One way to do this would be to complete a simple table as follows[4]:

Type of loss "scenario"	Insurance Policy	Parties covered	Trigger	Intended loss types to be covered (if any)	Exclusions/specific terms applicable (if any). Sum limits.
Data loss	Stand-alone cyber*	1st party	Malice	Forensic examinations Notification Other services (legal PR…) Reputation	Enter the LMA code or bespoke code as appropriate. Enter sum of limits in this scenario.
			Accident	none	ditto
			Negligence	none	ditto
		3rd parties	Malice and negligence	Loss of credit rating Cash loss Physical damage	ditto
		Intermediaries	Malice, accident and negligence	Loss to policy-holder*	ditto
	Public Liability	3rd Parties	Negligence	Tort NOT pure financial loss	ditto
	Property	1st party	Malice	Property damage	Ditto e.g. data is not property clause
			Accident	Property damage	ditto
		3rd Party	Malice	Property damage	ditto
				Damage to data itself	ditto
	And so on for each insurance policy that could be triggered by data loss				
Intellectual Property Theft	Cyber	1st party	Malice	Loss of profits	ditto
			Accident is not covered	Forensic examination (coverage dispute issue)	ditto
		3rd party	malice	Loss of profits Fines Legal costs	ditto

[4] Note: These entries are for illustration purposes only.

				Forensic examination	
			Negligence is not covered.	Forensic examination (coverage dispute)	ditto
	And so on for each insurance policy that could be triggered by IP theft.				
And so on for each "scenario"					

Not only will commonalities of exposure become apparent, so will mechanisms by which losses could aggregate across different insurance policies.

Aggregation is most obvious where there are technical risk factors in common

- e.g. use of a particular data centre when the type of loss is 'data loss' or 'theft of IP'
- e.g. use of a particular water source when the type of loss is BI or property damage.

This observation leads to the development of 'aggregation potential' questions to be answered by policy-holders. If for example, the portfolio of insurance policies was mostly exposed to aggregation risk by the common use of a data centre, then the insurer should routinely ask for the names of the data centres in use and whether or not the type of loss envisaged is being mitigated at source. Insurers could ensure that no more than for example ten insured's use the same data centre. More complex would be where insured's use the same computer chips for controlling machinery; selecting insured's on the basis of chip selection would be problematic, but aggregation estimates would depend on knowing this information.

However, this analysis cannot answer the question of what the most probable maximum loss is. Nor does it help when a group of insurers all have the same re-insurer. For this it may be instructive to develop realistic disaster scenarios such as the sudden failure of GPS technology, corruption of the banking LINK system, disabling the RFID technology in shops, corrupting the data held by Experian, etc. RDS designers would have to specify a number of technical parameters in each case e.g. the degree to which shipping relies on GPS. Without a large data set of true IT insurance aggregation events, such technical parameters would of course be little more than fiction designed to illustrate effects of the event on insurance portfolios.

Limits on policies and a clear definition of event (for re-insurance purposes) may be the only certainties in the aggregation problem. However, where the item in question is traded e.g. computer hardware, then insurers can check where they are potentially exposed in the supply chain. The Arium CAP software will map out the supply chain for a given component/IT product and this will guide insurers in their investigation of aggregation. The same software will sum limits in the supply chain but it is a matter for expertise to refine this worst case into a realistic case. Perhaps the same software can be adapted to run a stochastic simulation of an event (using the various limits in the portfolio, deductibles and expert opinion as to where 'blame' or other triggers may attach) and so produce a version of PML.