Addressing Cyber Risk with a Captive Solution

Nuno Antunes

is head of multinational and alternative risk at AIG in EMEA.

Mark Camillo

is head of cyber products at AIG in EMEA.

Adrian Sykes

is a global fronting underwriter at AIG in the EMEA region.

Nuno Antunes, Mark Camillo, and Adrian Sykes discuss addressing the growing issue of cyber related risks with a captive insurance policy.

For the management of any company, the most vital tools needed for it to function in today's world often centre on things like email, online files, CRM or point of sale systems. While all of these assets are exposed to the standard physical threats including flood, fire, theft or malicious damage, they are equally vulnerable, if not more so, to a host of new cyber-related threats. Many of these threats are understood far less, yet have the capacity to be just as devastating. A captive programme can be an attractive solution for addressing cyber risk.

While neither the statistics nor individual cases fully capture the changing nature of cyber risks, they do help to illustrate the challenges such risks pose. PwC's 2014 Global Economic Crime Survey found that 17% of businesses and 39% of the financial sector had been victims of cyber crime. While these risks are costly for individual firms, they also pose a wider systemic problem. Cisco forecasts that, by the end of the decade, there will be 50 billion interconnected devices – up from 12.5 billion in 2010. For example, the Heartbleed vulnerability in Open SSL software, discovered in April 2014, revealed not only the potential for common weaknesses with half a million websites susceptible, but also the fragility of the 'internet of things' with connected printers, video-conferencing and even thermostats among the devices affected. Organisations as diverse as the UK portal Mumsnet and Canada's tax authority announced that hackers had stolen some of their data by using the bug.

While the source and nature of potential damage to a business' systems are developing with incredible speed, the risks posed are evolving with equal rapidity. Extending beyond the fairly well-recognised damage to digital assets, they include non-physical business interruption and even directors and officers liability (D&O). For example, business interruption is a critical risk for companies that host clients' data. There is also increasing pressure on private organisations to bolster security or pay the price for not doing so.

Potential liabilities and threats are both on the increase, and it is safe to say that total security is unachievable. Whether it is due to activists, nation states, criminals, suppliers or insiders (employees are considered to be the greatest threat to information security, according to a survey by the British Standards Institute), organisations of every size must assume that a breach at some point is inevitable. The question then is what do you do to protect your business.

Mind the gap

Insurance is clearly a very useful tool in helping businesses to respond to these threats, and there is no doubt that the take-up is growing. According to Marsh Risk Management Research Benchmarking Trends: More Companies Purchasing Cyber Insurance published March 2013, the number of clients buying cyber insurance rose by 21%. Insurers are also increasing both capacity and the number of products available. Cyber insurance carriers announced 38 new cyber-related products in 2013 compared with 32 in 2012, based on insurance company press releases sent to Advisen Ltd.

While it appears choice is increasing, in fact, policies remain almost exclusively focussed on losses from data breaches and first party losses. There is no doubt that this remains a very real and important risk; especially in the US where state law on data breach notifications can result in substantial costs; in Europe the existing regulation on data protection and privacy is less demanding. However, proposals to introduce much tougher legislation are moving through the European Parliament and these contain an explicit consent requirement, a right to erasure and substantial fines based on percentage of global turnover for breaking the rules.

Most traditional insurance products do not address network exposures and, in some cases, carriers have begun specifically excluding data and technology-related risk from their policies. For example, in the case of Commercial General Liability (CGL), most cyber claims don't involve

continued >

physical injury to either people or tangible property and electronic data is not considered tangible under a typical liability policy. Equally, property policies focus on the physical damage, theft, or destruction of tangible assets (buildings, machinery, equipment, inventory, etc.). With computer breaches, information is often copied without authorisation, with no loss or damage to the original information. As a result, property polices may not cover cyber claims or provide adequate coverage.

AIG has taken steps to bridge this issue. CyberEdge PC is a first-of-its-kind umbrella product that fills these gaps with excess and drop-down cover for underlying property, casualty, aerospace, marine, environmental, healthcare, E&O, D&O, cyber, or fidelity insurance policies. This additional layer of protection helps organisations to manage the risk of physical damage posed by cyber attacks, provides them with peace of mind and allows them to stay ahead of the cyber risk curve.

Keeping it captive

So, the obvious question is whether risk retention is a possible way forward for businesses to manage these risks, and should risk managers be considering putting cyber risks into their captives? Given some of the confusion in the insurance market and the complexity of the risks, the benefits of retaining those risks via a captive and thereby gaining a better understanding of the losses and expenses, having greater risk oversight, and potentially reducing the overall cost of risk may be very appealing. A captive can be a useful tool to retain risk within the burn layer and also assume broader cover not available in the traditional risk transfer market.

According to several studies by brokers however, only a small number of companies are taking steps to consider captives for their cyber risks. For example, Marsh's 2014 Captive Benchmarking Report showed only 17 captives covering cyber risks of 1,148 it examined. While in Aon's 2014 Captive Benchmarking Tool, which captured data from over 1,000 Aon managed captive clients, the number of captives writing cyber currently is reported at 1%; a number which has remained static since 2012.

The reluctance for many organisations appears to be driven by the difficulty in estimating cyber risk exposure and quantifying the consequences of cyber events. This challenge is not dissimilar to that faced in considering whether a policy from the commercial insurance market is the solution.

Small steps

Applying captives to emerging risks, such as cyber, presents challenges and opportunities. For example, do you know what the risk is? Can you gather the data needed to understand the nature of that risk? Can you price and reserve for it? Do you know the infrastructure you need to service that risk? These questions need to be asked and answered, particularly when dealing with new or emerging lines. Nevertheless, when commercial insurance coverage for cyber risk is unavailable or prohibitively expensive, a captive can be used to build a statistical base, which can make securing excess coverage at acceptable terms and pricing easier. It can also be used for covers that might not be readily available in the market such as future lost revenue or first-party loss of inventory due to technology failure. It is also possible to arrange cover for highly correlated risks, such as cyber and reputation, which may not be packaged in the commercial market.

Including new lines also helps to provide greater diversity and stability to a captive programme. Under the provisions of Solvency II in Europe, which impacts captives as well as the commercial insurance market, there is an incentive for a captive owner to diversify its portfolio of exposures. For example, insuring cyber in the captive in addition to say property and casualty creates an additional risk diversification which may support the captive's capital requirements, particularly in a Solvency II environment because the additional line is not correlated to the other business. This may have the impact of reducing the amount of capital that the captive needs to hold in order to maintain the minimum solvency level.

Making it work

As with other emerging risks, it is possible to use the captive as a 'risk incubator' for cyber threats by using the intelligence gained as a way to understand the exposure better and make more informed decisions about how to manage and finance the risk. That assumption is however predicated on claims actually occurring. If they don't, then little can or will be learned, although retaining the risk may give the business a greater risk management focus on cyber.

This focus could include:

- An overview of the digital assets and a list of threats.
- Identification of cyber risk scenarios through a workshop with key stakeholders.
- An assessment of the direct (i.e. financial loss, destruction of digital assets or business interruption) and indirect consequences (i.e. reputational damage, errors & omissions claim or loss of customers) followed by quantification of both.

The other key ingredient is, of course, actually protecting the business from cyber risks where possible. For example, capabilities such as firewalls, system operational procedures, etc., should be assessed and benchmarked against industry and risk-appropriate standards, such as ISO 27000 and the NIST frameworks.

continued >

Addressing Cyber Risk with a Captive Solution

A broader view

Even a casual read of the many cyber case studies reveals the breadth of these risks faced by almost every business. The picture can only become more complex as regulatory regimes around the world develop further and the nature of cyber risk evolves. As with all complex risks, the management of them lies in a mixture of proactive internal steps such as risk transfer through insurance and increasingly, some risk retention. This is certainly the experience of many of the clients with whom we have worked so far, where a 'blended' solution is very much the way forward and the structure of captive programmes is such that the captive takes a reasonable per occurrence/aggregate retention in the primary exposure, with the catastrophe losses transferred to the insurance market. Our CyberEdge PC product is just such an umbrella product that works in conjunction with the conventional insurance policies to offer excess and difference-in-conditions for cyber security failures.

There can be no doubt that cyber liability is an issue no organisation can afford to ignore and now is the time to be thinking about whether risk transfer, retention or a combination of both is the right solution for the risks a business faces. The fact that cyber exposure is difficult to quantify, both in terms of cost and consequence, may be deterring businesses from either buying a cyber policy or including it in their captive. The solution lies in risk managers working together with brokers and underwriters to understand and articulate the company's risk profile so that it can get the best cyber protection programme available in the marketplace.

For more information, please visit **www.aig.com/captives**, or contact:

Nuno Antunes at 44.207.651.6494
nuno.antunes@aig.com

Mark Camillo at 44.207.651.6304
mark.camillo@aig.com

Adrian Sykes at 44.207.651.6120
adrian.sykes@aig.com

AIG Bring on tomorrow