Market must work with US government on cyber

The re/insurance industry has a responsibility to work with the US government to develop relevant regulation on the issue of cyber coverage in addition to actually providing products to clients.

That is the belief of Nancy Millette Bewlay, Swiss Re's head of underwriting for casualty in the US and Canada, who, when speaking on a panel discussion at the PCI conference, explained one of the factors affecting re/insurers' ability to provide coherent and comprehensive cyber coverage to clients is the concern over jurisdiction.

"I think there is a responsibility from the insurance sector to not only provide products on cyber, but to work with governments as well, and in particular cyber regulation," said Bewlay.

"One of the issues that we have as either an insurer or a reinsurer is that jurisdiction matters, and coverage opinion changes depending on where you go in the US."

"I do believe that innovation is there [from the re/insurance industry], but we cannot do it independent of what regulation can do at the same time. It's really up to us to influence what our government can control."

Despite these concerns, the cyber re/insurance market remains a growing industry. High profile cyber breaches and attacks involving companies such as eBay, Sony and Target have all highlighted the exposures companies face with firms ultimately facing costs valued at hundreds of millions of dollars, if not more.

Indeed, Andrew Marcell, chief executive of Guy Carpenter's US operations, believes there is plenty of growth potential in the sector.

"Cyber is front and center [of corporates' thinking] and is a great opportunity for the insurance market. [But] reinsurers need to run to risk and not run away from it and be helpful and deploy their capital."

Those same sentiments are shared by Bryon Ehrhart, chief executive of Aon Benfield Americas, who also believes cyber risk is growing market for the industry. However, as highlighted by Target which, despite facing financial losses that exceeded $1bn, is understood to have only had $100m of cover in place, there is a disparity between the level of protection companies are prepared to buy and what their actual exposure is.

Cyber is certainly a growing market and we have received a number of demands from large retail customers asking us and the reinsurance business what additional capacity can be brought in.

Bryon Ehrhart, chief executive of Aon Benfield Americas

Part of this disparity can partly be explained by companies possibly not understanding how large their potential exposure may actually be, but another aspect is the prohibitive cost of buying cover that protects them to such a degree.

"Cyber is certainly a growing market and we have received a number of demands from large retail customers asking us and the reinsurance business what additional capacity can be brought in," said Ehrhart.

"We have been as an industry pretty innovative to bring $100m to $300m worth of capacity to large corporations, but [those limits are] largely to do with the cost and nothing to do with the ultimate financial consequences to that company. So there's room for some more innovation around it. Obviously the industry at a primary level has got comfortable with thinking about what the frequency could be to the individual enterprise, but I think there's a great amount of uncertainty around that estimate given everything that continues to occur… [At the same time], the products on offer in the cyber market are actually not that responsive."

Tad Montross, chairman, president and chief executive of Gen Re, said the premium levels demanded for cyber liability cover often deter potential buyers.

"Part of the problem of the liability side of cyber is that there has not been appetite at some premium levels to purchase. We have to be careful not to confuse innovation with a market clearing price."

Ehrhart added: "The liability is an ongoing concern, [and] I just don't know how the insurers and reinsurers are going to partner up and come up with a product that is cheap enough that people might buy it."

Another problem associated with this evolving section of the re/insurance industry is the ability of companies to actually define what "cyber insurance" actually means. Many re/insurers and brokers have different interpretations about what should and should not be covered, while the importance attached to different elements of the protection can also divide opinion.

"There's no definition of cyber insurance," said Montross, "There are hundreds of different policy forms and products out there. And while we can be hard on the industry, I actually feel it's been pretty responsive in developing a set of cyber responses in the last few years.

"We know the exposure is increasing geometrically daily – every single week there's another very significant cyber issue. They're all different and we don't know what's causing them so it's an area of huge opportunity and it's an area that I think the industry has responded well too. But I think it's also important [to be sensible and not just jump in because you] run the risk that it's not understood or mispriced."