The Z/Yen Group

Cyber Re Centre for the Study of Financial Innovation

Cyber Threats To Financial Services – A Growing Problem, Or An Opportunity For The Insurance Industry?

A round-table discussion with David Nordell (New Global Markets), Michael Mainelli (Z/Yen), Dave Clemente (Chatham House) and Martin Jordan (KPMG).

Tuesday, October 23, 2012 from 12:30 to 2:15 pm.

At the Association of British Insurers, 51 Gresham Street, London, EC2V 7HQ.

Professor Michael Mainelli's remarks:

Z/Yen is a commercial think-tank in the City of London. We solve problems, typically where finance meets science & technology, often for a social purpose. As well as cyber-crime issues, we run Long Finance, the Global Financial Centres Index and the Global Intellectual Property Index, and help analyse the effects of new trading structures or new markets such as gambling.

In 1996 we, with the Ministry of Defence and the then CSSA, now Intellect, created the industry Taskforce 2000 for the Millennium Bug. We conducted a fairly damning study a decade ago which found nearly half of the City's secured wifis were still using default administrator passwords, and produced a detailed critique of the costs-not-benefits of the Anti-Money Laundering regime back in 2005 for the City of London. For my part, I've been involved in cyber-security since being a real hacker developing cryptographic systems and helping IBM develop RACF in the 1970s, to being a director of the Defence Evaluation Research Agency in the 1990s managing some ITSEC and cyber-security projects, to commercial work with banks and publishers on protecting assets.

You'll already have heard a lot stories, many real, about the effects of cyber-crime. I can personally tell you about banks hiding scandals, or exchange shenanigans or publishers who have been blackmailed. Cyber crime is real and it hurts financially. And I'm here with a financial, not a technical, hat on.

How would we know when government and industry are working together on cyber-crime? A realistic comparison would be burglary insurance. People contract with insurers in

commercial terms they understand, with contracts they know and financial risks and rewards they can analyse. A realistic economic goal for government is to create a framework where insurers want to write broadly-based cyber-crime business, because they know it pays. The government-commerce dysfunction is due to some degree a lack of common financial measurement and not looking at a systemic solution to a wicked problem.

Our, Z/Yen and Long Finance, proposal is Cyber Reinsurance (Cyber Re). Cyber Re is a proposal to provide a solid foundation for financial solutions in a business interruption reinsurer. The proposal originated with reactions and inactions by authorities to cyber-enabled thefts on the carbon trading markets associated with the European Trading System, though a version of it was proposed in 1997 during Y2K/Millennium Bug preparations. In January 2011 over €45 million was stolen from the carbon markets. Carbon markets were closed on 19 January and have fitfully reopened since. The January 2011 attacks were preceded by attacks in 2009 and 2010. A 2 February 2010 phishing theft of 250,000 carbon emission permits was reported to net €3 million and also closed the markets.

The authorities did virtually nothing till pushed very hard by the City of London Corporation, and even then not very much. The only insurance response was to try out some products that would guarantee your permits were valid – though by the time you got the cover you knew the permits you were buying were valid. Another variant of the insurance industry selling white goods guarantee products.

Cyber-crime insurance is a weak market where it is hard to get significant risks written. Market cover is sporadic above a handful of computers (cyber equivalent of white goods appliance insurance) and fades completely above £100 million. Cyber-terrorism, e.g. state sponsored terrorism, insurance doesn't even exist. This market problem resembles property insurance in the UK in 1992. Following the 10 April 1992 bombing which devastated the Baltic Exchange for shipping, international insurers withdrew cover for acts of terrorism and the UK government formed Pool Re rapidly.

At the moment, insurers in the UK can reinsure liabilities from terrorism, in excess of the first £75m, with Pool Re. A Pool Re member's retention is proportionate to their participation in the scheme. Interestingly, the exclusions applying to the terrorism cover of Pool Re are in respect of: *"war and related risks; and damage to computer systems caused by virus, hacking and similar actions."*

The Z/Yen Group

Why don't we have a Cyber Re (or extend Pool Re) where government helps the insurance industry fund the extreme losses of cyber-crime? As an example, government takes responsibility for risks above a point, say £100 million. Below that point normal insurers write cyber policies which help spread information and best practice and bear the risks up to £X million on any single incident or £Y million on combined incidents. There are issues, not least clearer definitions of business interruption, cyber, and 'UK business', just to get started. But I can't cover these in seven minutes.

It is likely that the business interruption model might be most appropriate. A good example of business interruption or "loss of earnings cover" is The Strike Club, originally for industrial dispute insurance but now providing a wide range of business interruption insurance to shippers, fleets, ports and facilities. In a business interruption model, the client states in advance how much a day's outage will cost and this both sets the premium and the claims, e.g. a day's outage costs £5M, the retention is the first 2 days, followed by payments for the next 10 days, for a premium of £500,000. When claims are made the estimated day's outage costs must be reasonable, but otherwise the model is simple.

With a fully functioning market, the UK would be more attractive to ICT businesses such as financial exchanges and large internet firms. Three points of note emerge from the above:

- Cyber Re exists not to insure, but to allow insurers to insure by providing re-insurance, in turn providing regulators with the assurance that cyber insurance can be safely underwritten;
- Cyber Re is focused on creating a club with members, thus encouraging members to share information and reduce risk by sharing information with government, such as near misses, as well as to grow their market;
- Cyber Re should be quite small operationally and operate at close to no-cost.

Cyber Re can confer competitive advantage on the UK. The 10 April 1992 St Mary Axe bombing was a significant catalyst for Pool Re. As insurers refused to provide cover against acts of terror, financial services firms, noting what had happened to the Baltic Exchange, stated that they had troubles locating or expanding in London and the UK generally. With Cyber Re, the UK would have definite attractions to firms that depend on computers, particularly financial and internet firms, as it would be the only country that indemnifies when it fails to protect against cyber-crime at scale.

The Z/Yen Group

So far, Z/Yen has held discussions, in formal or informal fora with, among others, government bodies, military institutions, insurance brokers, underwriters, insurers, reinsurers, Lloyd's, financial markets firms, trade bodies, lawyers, ICT firms, think-tanks and academics. Discussions so far have been encouraging - financial and ICT services would like the cover; insurers would like the reinsurance; government entities see the gains.

We have two cultures, government and commerce, that need to work together. How would I know the two cultures are working together? For me it's when I can easily buy cyber-crime insurance. That means government has successfully de-risked the long tail to the point insurers can step in. Then I can contract with the insurer in commercial terms I understand, with contracts I know and financial risks and rewards I can analyse. Perhaps the real economic goal for government is to create a framework where insurers want to write cyber-crime business, because they know it pays.

— Professor Michael Mainelli FCCA FCSI FBCS, Executive Chairman, Z/Yen Group.

After a career as a research scientist and accountancy firm partner, Michael co-founded Z/Yen, the City of London's leading commercial think-tank, to promote societal advance through better finance and technology. Michael's third book, based on his Gresham College lecture series from 2005 to 2009 and co-authored with Ian Harris, "The Price of Fish: A New Approach to Wicked Economics and Better Decisions", won the 2012 Independent Publisher Book Awards Finance, Investment & Economics Gold Prize.