Cyber's empty space

Michael Mainelli points to the need for a cyber-crime insurance market in which significant risks could get underwritten

You will have heard a lot of stories about cyber-crime. It exists. Moreover, it hurts financially partly because it is difficult to insure.

One proposal by the Long Finance initiative, set up by Z/Yen Group and Gresham College, is Cyber Reinsurance (Cyber Re). This originated last year in frustration at inaction by authorities over cyber-enabled thefts on the carbon markets, though an earlier version was proposed during Y2K/Millennium Bug preparations.

In January 2011, more than €45m was stolen from the carbon markets linked to the EU Emission Trading System. They were closed on 19 January and fitfully reopened after that. Those attacks were preceded by others in 2009 and 2010. One 2010 phishing theft of 250,000 carbon emission permits netted €3m and also closed the markets. The authorities did virtually nothing until pushed by the City of London Corporation last year, and then not much. The insurance response was to launch some products that claimed to guarantee future permit purchases were valid.

Cyber-crime insurance is a market where it is hard to get significant risks underwritten. Market cover is sporadic once demand moves beyond covering a handful of computers and fades completely above £100m. Insurance for cyber-terrorism, e.g. state-sponsored terrorism, does not exist.

The problem resembles UK property insurance. After the April 1992 bombing that devastated the Baltic Exchange for shipping, insurers withdrew cover for acts of terrorism. In response, the UK government formed Pool Re. Insurers can reinsure liabilities from terrorism with Pool Re, typically in excess of the first £75m. 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." Pool Re was emulated by the US after 9/11.

Why do we not 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 would take responsibility for business interruption risks above a point, say £100m. Below that, normal insurers would write cyber policies that help spread information and best practice and bear the risks up to £Xm on a single incident, or £Ym on combined incidents.

> Market cover for cyber-crime fades completely above £100m

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 range of business interruption insurance to shippers, fleets, ports and facilities. The client states how much a day's outage will cost and this both sets the premium and the claims. For example, a day's outage costs £5m, the retention is the first two 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.

There are issues, not least the need for clearer definitions of "business interruption", "cyber", and "UK business". But with a functioning market, the UK would be more attractive to information and communications technology (ICT) businesses such as financial exchanges and large internet firms.

Cyber Re could confer competitive advantage. After the 1992 bombing, when insurers refused to provide cover against acts of terror, financial services firms said they had trouble locating or expanding. Cyber Re would make the UK attractive to those dependent on computers, particularly financial and internet firms, as it would be the only country that indemnified for failure to protect against cyber-crime at scale. There are three points about Cyber Re:

- it would exist not to insure but to provide reinsurance, which gives regulators confidence that cyber insurance can be safely underwritten;
- it would create a club atmosphere, thus encouraging information sharing among members and government, and risk reduction as well as market growth;
- the operation should be quite small and run at minimal cost.

How would we know when government and industry were working together on cyber-crime? A realistic comparison would be burglary insurance. Cyber-crime would be under control when people contracted with insurers in commercial terms they understood, with contracts they knew and financial risks and rewards for good behaviour they could assess.

Discussions with government bodies, military institutions, insurance brokers, underwriters, insurers, reinsurers, financial markets firms, trade bodies, lawyers, ICT firms, think-tanks and academics have been encouraging. Financial and ICT services would like the cover; insurers would like the reinsurance; and government entities see the gains. Perhaps the real goal for government is to create a framework where insurers want to write cyber-crime business because they know it pays.

***Michael Mainelli** is executive chairman of Z/Yen Group*