TISAtalk **12th March 2014**

INVISIBLE (Waking Shark 2!)

I don't know about you, but when I am in a cinema watching a Sci Fi film, things go on that I don't really understand or see how they work. I guess the same can be said for certain technologies in that as long as it does what it is supposed to, then you don't even have to worry about what goes on inside the device or application.

However, one of the items I have been meaning to get on to our agendas in TISA's Distribution or Wrap & Platform Policy Councils is Waking Shark 2, or something similar which is relevant to us in adviser and platform world.

Waking Shark is really aimed at the UK's banking, payments and markets systems. Operation Waking Shark 2 took place last November with every high street bank taking part in a one-day 'war game' simulating the impact of a major cyber attack on the payments and markets systems on which the UK's financial system depends.

An outside consultant has designed the test, which is to assess the ability of Britain's core financial services providers to withstand attacks by cyber criminals as well as state-sponsored terrorist attacks on the UK. The exercise comes two years after the FSA launched the Original Operation Waking Shark to test the strength of the online defences.

In our own world, I am picking up indications that simpler frauds or attempted fraud could be happening in adviser distribution world.

Threats today also come from criminal networks and foreign governments that deploy cyber weapons. Here these assailants are trying to make thousands of pounds at the expense predominantly of banks but others may want to steal sensitive commercial information or disrupt the financial payments system and criminal's techniques are constantly evolving with investigations taking some time. Recent reports by the British government and the United Nations have demonstrated the international nature of cyber threats. A report by the Cabinet office estimates that the cost of cybercrime to the UK economy could be as high as £27 billion. A cyber attack on a major financial institution which paralysed systems could cause misery to millions of personal customers and enormous numbers of businesses, which is why governments, law enforcement organisations global bodies and banks are taking this menace so seriously.

The banks are taking on many new staff to combat financial crimes and information sharing between banks, the police and other parties being a vital part of the work. Many banks are now participating in the government Cyber Security Information Sharing Partnership that allows data on cyber offending to be shared.

What about the rest of us in the financial services community. Combating cyber crime is not some nerdish preoccupation of the banks. It goes right to the heart of one of the industry's central aims which is protecting our customers and their assets. Perhaps then I should put this subject on the next agenda at both of our Policy Council meetings to see if anyone else shares my phobia.

Peter Smith, Head of Distribution Engagement