Brokers need to understand the growing problem of cyber crime if they are to avoid gaps in a wide range of clients’ insurance programmes, advises BEN BEESON

In today’s multi-channel, mobile and inter-connected world, every element of society including government, industry, commerce, charity, health, education and individual citizens is increasingly at risk. Increasingly sensitive data is stored on a computer system somewhere in the world and the risks are constantly evolving as technology develops.

These risks are likely to become more acute as new generations of smart phones effectively become mobile wallets, which will place ever greater volumes of personal and financial data at risk. Cyber crime is not a fictional concept – it is a very real problem with someone falling victim every 19 seconds.

Regulators take action
Regulators across the world are waking up to the fact that changes in data privacy laws are required. The Obama administration in the USA, and the European Justice Commissioner, Viviane Reding, are both proposing new national and cross-border data breach notification and data privacy laws.

The EU data privacy proposals include fines of up to 2% of global annual turnover if a company breaches the proposed data laws and a requirement for companies with over 250 employees to appoint a data protection officer, and for all breaches to be reported to the regulator – ideally within 24 hours.

Data breaches are becoming more common and dealing with them increasingly costly, complex and damaging for the organisation that ‘owns’ the data. Norton’s Cybercrime Report for 2011 estimates that the cost of stolen cash and the cost of time spent on identifying and resolving data breaches to businesses and governments is around $388 billion globally. Risk managers and finance directors realise they need to develop a greater understanding of how to predict and prevent data breaches.

As the frequency and severity of cyber data risk increases, so the insurance world is becoming more concerned about the associated financial risks.

There is a growing insurance market for both first and third party data liability business, and also first party business interruption cover. These products and covers are likely to continue to develop over the coming years.

While elements of this risk exposure may be covered with a full civil liability insurance broker professional indemnity wording, there are many areas where your exposures may not be.

Looking ahead
London is a pre-eminent market for this business due to high levels of innovation and its ability to provide specialist and tailored cover. We expect that the introduction of mandatory reporting of data breaches for companies handling EU citizen’s data inside or outside Europe will significantly speed up the rate of new product development in 2012 and beyond.

Data privacy is, and will continue to be, one of the biggest emerging risks for businesses in the 21st century. Insurance can provide essential financial assistance and access to highly experienced legal, IT forensic and crisis PR advice – which can help companies preserve reputation and get back to trading as rapidly as possible.

Ben Beeson is a Partner at Lockton who are BIBA PI Initiative accredited brokers