Securing data has become a costly yet fundamental part of modern business. But even as the threat of cybercrime mounts, British CIOs are largely avoiding cyber insurance.

Cyber insurance has failed to achieve the sort of take-up in the UK it has in the US, despite growing evidence that businesses are under attack like never before. Research released in April revealed that 93% of companies, including 87% of SMEs, experienced at least one data security breach in 2012. The 2013 Information Security Breaches Survey (bit.ly/17ftGvK), carried out by PwC for the Department for Business, Innovation and Skills, outlined a rise in the number of security breaches and showed the average damage caused by the worst breaches has never been higher, costing large companies between £450,000 and £850,000, and SMEs between £35,000 and £65,000.

Despite the escalating frequency and cost, a delegate poll at insurance broker Marsh’s recent digital threats conference found only 12% of organisations have cyber insurance despite 71% of respondents indicating cyber risks had risen in the past year.

While these take-up rates appear bleak, impending EU data security regulation could provide cyber insurance providers with a much-needed shot in the arm. And, considering the current corporate sentiment towards cyber insurance, data regulation cannot come soon enough.

A GAME OF CAT AND MOUSE
Another reason for the poor take up of cyber insurance is that CIOs question whether insurance firms are able to

With cyber attacks on the rise, the need for businesses to insure against threats is imminent. Arvind Hickman talks to the experts about why prevention is better than cure.

**IS INDEMNITY THE BEST POLICY?**

**COVERAGE CONFUSION**
British businesses are getting better at detecting cyber threats but are largely unconvincing about the benefits of cyber insurance, which has now been offered in the UK for more than a decade.

CIOs tell Chartech there is confusion over what cyber policies actually cover and a preference to invest in preventative security measures such as firewalls, virus software and information security officers. Christian McMahon, managing partner of board and CIO advisory at consultancy Jamaza, says cyber policies are ambiguous.

"Having read through many cyber insurance policies from different insurers and vendors, you are never quite sure what is being covered, even when you question the insurance company or broker," he says.

The ambiguity of cyber insurance is partly due to the unpredictable nature of cyber attacks. In the event of a breach, it is often difficult for companies and insurance firms to pinpoint exactly what data has been breached, who is at fault, and the motivation behind the attack, whether it is financial, competitive or political.

“You wouldn’t have a contents insurance company insure a building if they could see a burglar through the windows,” explains Kris McConkey, a director in PwC’s cyber security practice. “Similarly, in cyber insurance it’s actually quite difficult for insurers to get that perspective. For example, how do you know if a company is currently being compromised? Insurers are struggling to get robust actuarial data about the extent of cyber risks and potential impact of those risks, such as the value of losses.”
provide coverage for ever-changing cyber threats. “I’m probably a little bit cynical about whether insurance companies fully understand the risks and would properly compensate you for what may happen,” says Martyn Croft, the CIO of Salvation Army UK. “The cyber threat landscape is changing every day so how do you insure against anything and everything?”

There is a school of thought among many CIOs, particularly those with a strong technical aptitude, that companies should take responsibility for their own data security rather than outsource the risk. Croft, who has been the CIO for Salvation Army for nearly four years, falls into this

data prevention camp: “If you identify the risks then you have to deal with them rather than try to pass it on. That’s like admitting the lock on your front door is broken and increasing your insurance because you know there is a greater chance you’ll be burgled,” Croft says.

The Salvation Army has 7,000 staff in the UK, 5,000 of whom have access to IT networks. The major cyber threat against charities is reputational damage from a data breach. “If that becomes damaged then it is very difficult to fundraise and you lose support,” Croft explains.

Ben Booth, who has been a CIO at several global companies, has another explanation for why companies tend to shy away from cyber insurance. “If your company’s reputation is based on you keeping your clients’ data safe or on the reliability of the information you provide, your reputation is almost priceless. A cyber breach would destroy the business reputation of your business and it’s very hard to insure against that,” Booth says.

AN IMMATURE MARKET
Insurance firms are all too aware of the challenges they face in selling cyber insurance. In London, there are at least 24 insurers offering cyber products but none has been able to create a foothold in the sector unlike in the US, where the AIG and Beazley are considered market leaders.

Chartech approached insurance brokers Aon, Marsh and Sutcliffe & Co and insurance underwriter Hiscox to find out why cyber is such a hard sell.

Aon’s Keith Tracey, managing director of risk solutions, professional services, believes many companies are not fully aware of the risk potential of cyber threats and some of the benefits of insurance, such as access to PR, forensic and technological support.

Stephen Wares, Marsh EMEA cyber practice leader, points out that part of the problem is that the cyber insurance market in the UK is still in its infancy. “The products are not standardised yet, it’s not a commodity product and there is a huge amount of innovation by individual insurers on their own products,” he says. “It is a very difficult market to navigate.”

BREAKING DOWN AMBIGUITY
At present, cyber insurance policies focus on two areas. The more common is the unauthorised release of personal data (or privacy breaches), such as the legal and regulatory costs of data loss, and crisis management costs once a data breach occurs. The second area is business revenue losses that are caused by IT outages, such as hacker attacks.

To ensure clarity, Wares says cyber insurance should be siloed into specific risks relating to the unauthorised release of personal information (or privacy breaches) and business interruptions. “In the US, the vast majority of purchases that have been made are really privacy insurance rather than cyber insurance. If we renamed that part privacy insurance it would make a lot more sense to business and CIOs,” he says. “Then we can talk about business interruption from IT events and ring-fence that as a risk issue.”

Sutcliffe and Co specialises in cyber policies for SMEs. In February, the broker partnered with underwriter AIG to develop a product tailored to SMEs. Prior to this, cyber insurance was being sold “by the big boys to the big boys” and policies would typically cost a minimum of £10,000, says Sutcliffe managing partner Duncan Sutcliffe.

It is too early to predict how SMEs will embrace cyber insurance, but Sutcliffe predicts interest will pick up towards the end of the year.

THE REGULATION TRIGGER
Companies of all sizes could soon be forced to consider cyber insurance as new EU data rules, likely to be introduced in 2014, will require companies to notify customers of all data security breaches or face fines of up to 2% of revenue.

“When the EU data rules are introduced, the whole insurance market believes that there will be a significant increase in the take-up rate of cyber insurance because the arrival of breach notice law in America was the catalyst for success of this product over there,” says Wares, while pointing out that in 2012 Marsh grew cyber insurance client numbers by 33%.

Whether or not the threat of regulation will encourage companies to take up cyber insurance, it is clear that insurance firms still have their work cut out to make it mainstream. A good start would be breaking down cyber insurance into clearer, ring-fenced products that tackle privacy and business interruptions, providing clarity over coverage.

A larger challenge will be developing products that have the agility to keep up with the murky world of cybercrime.