Portfolio Media. Inc. | 111 West 19th Street, 5th Floor | New York, NY 10011 | www.law360.com
Phone: +1 646 783 7100 | Fax: +1 646 783 7161 | customerservice@law360.com

Regulatory Wild West Mars Surging Cyber Insurance Market

By **William Shaw**

Law360, London (May 10, 2017, 4:21 PM BST) -- Demand is surging in the U.K. for insurance against cyberattacks, but lawyers say the market is hampered by fears of massive payouts and confusion as to how far new policies actually extend without a clear regulatory framework.

Reported attacks on U.K. financial institutions rocketed from five in 2014 to at least 75 in 2016, according to Financial Conduct Authority data, prompting Britain to double its funding for cyber protection over the next five years to £1.9 billion ($2.46 billion). And escalating attacks in Europe have pushed major regulators to protect insurers from dangerous levels of risk, which could lead to colossal liabilities if a household name suffers reputational damage in an attack.

The European Securities and Markets Authority, the European Banking Authority and the European Insurance and Occupational Pensions Authority are all now assessing the buildup of risk amongst insurers developing new cybersecurity policies to shield clients from cybercriminals. But lawyers say the industry still operates in a regulatory Wild West, with insurers unsure of what they might have to pay out, and customers uncertain of how far their coverage extends.

"An increasing number of U.K. insurers are issuing cyber policies, but there is no market standard," said Richard Mattick, counsel at Covington & Burling LLP.

"Because of the novelty and variety of the product, policyholders are worried about what they are buying," he added. "There is no specific regulation of the wording."

Attackers have hit some of the U.K.'s biggest high-street firms, prompting a boost in demand for coverage. In April payday loan firm Wonga said it was urgently investigating an illegal data breach that could have affected up to 270,000 customers in the U.K. and Poland.

Tesco Bank, part of the U.K.'s largest supermarket chain, suspended all online transactions from checking accounts in early November after 20,000 customers had money stolen in a cyberattack.

And in January 2016, HSBC Bank PLC revealed that its internet services in the U.K. had been hit by an attack that shut down its mobile and customer services for several hours.

"Cyber threats are growing, are changing rapidly and have the ability to cause widespread damage," said Helen Bourne, an insurance partner at Clyde & Co. LLP. "What's important is that the risks are taken

seriously within organizations so that appropriate cover can be secured."

Cyber insurance policies can be an extension of an existing policy, or be tailor-made from scratch.

But lawyers say a major problem is confusion in some firms about what their existing cyber protection actually includes. Some coverage includes nominal losses, but may not reach to reputational damage that could send clients fleeing and dent investor confidence.

"Insurers can model small fixed losses so they can price on the back of a low policy limit, but they can't model uncapped or high policy limits for cyber losses, so they can't price and can't offer it," said Benjamin Lyon, international counsel at Debevoise & Plimpton LLP.

The Law Society, a legal trade body, warns that standard professional indemnity insurance will cover firms for civil liability and most third party cover but not the cost of a forensics investigation after a cyberstrike.

At law firms, a professional indemnity policy may cover funds in a client account but not those in the office account, which would need specific cyber coverage.

“There are people buying cover and not completely understanding what they are covered for,” said John Bradley, managing partner at Reynolds Colman Bradley LLP. “Often they think it's a lot wider than it really it is."

As cybercriminals become more ingenuous, the harm they can inflict on household names opens sweeping new vistas of potential damage, most seriously to a firm’s hard-won reputation. This may simply be too high for some insurers to touch, though some insurers do provide extensive protection and coverage beyond £10 million, Bradley said.

“It's about having right broker in place and making sure they understand your requirements,” he said.

Ramping up the need for protection, the EU’s General Data Protection Regulation, which takes force in May 2018, could hit banks with fines equivalent to up to four percent of their global turnover for security breaches of personal data.

Lawyers say the regulatory package will also force forms to inform their customers of an attack, a move which insurers await with great anticipation.

"Potential hackers, the way they access private data is changing minute by minute," said James Scoville, partner at Debevoise & Plimpton. "It's increasingly leading to not just regulatory sanctions if there is a hack, but also potentially private litigation as well.”

Across the Atlantic, the market has been growing faster following a series of high profile attacks against major U.S. firms.

Internet giant Yahoo announced in December that data from more than 1 billion user accounts was compromised in August 2013, which at the time was the largest such breach in history.

Target Corp., one of the U.S.’s biggest discount retailers, revealed in December 2013 that hackers had stolen data from up to 40 million credit and debit cards belonging to its customers.

In response, U.S. property and casualty insurers wrote $1 billion in cyber-related premiums in 2015, Fitch Ratings Ltd. estimated on April 20. Lawyers predict similar trends in the U.K.

"Like everything, litigation and regulatory risks are greater [in the U.S] than they generally have been in Europe, but it's only a matter of time before these issues become costly," said Debevoise & Plimpton's Scoville.

Attorneys predict the market will adapt with better policies arriving that are capable of shielding the biggest firms from cyber disaster, ultimately forcing down prices.

"Premiums will grow, coverage will grow," said Debevoise & Plimpton's Lyon. "It's just going to take some time."

--Additional reporting by Mark Taylor. Editing by Rebecca Flanagan.
