INSIGHT

# Insurers target cyber threats to evolving 'internet of things'

**The threat posed by cyber attack has hit the headlines in the wake of the Heartbleed bug, which exposed company websites to downtime, and a rash of other attacks in an increasingly digitised world. Meanwhile insurers are expanding the nascent cyber insurance market, which has traditionally been focused on data breaches, into new areas**

Neil Ainger
UK correspondent

The news earlier this month that thousands of websites around the world had to reset passwords or implement a patch after the Heartbleed bug exposed OpenSSL cryptography software to attack from cyber criminals has led to renewed interest in the evolving cyber insurance marketplace.

Until now the cyber insurance market has mainly been focused on covering corporate losses from data breaches or privacy concerns or rolling the legal, operational and business risks of a hack attack into other comprehensive policies. But this is now changing, with new add-on or standalone products emerging.

This week AIG launched an insurance product that will compensate corporates for cyber attacks against their property or people. The insurer says the expansion of the CyberEdge PC product line is driven by the rise of the "internet of things" – which means more and more everyday products are now connected to the internet, from medical pacemakers to cars and building management systems, making them vulnerable to attack.

Earlier this month Aegis London launched a rival product called Cyber Resilience, which is designed to protect operational technology and assets, before and after a cyber-attack (see box).

The fact both companies are coming to the market shows the increasing interest in the sector. The nascent cyber insurance market is growing beyond mere data breach protection and insurers clearly believe it is worth investigating because it offers huge growth opportunities.

**Heartbleed bug**

Publicity surrounding recent attacks such as the Heartbleed bug is also likely to drive boardroom interest and uptake. The OpenSSL software attacked by the bug powers encryption across the global web and displays the IT security padlock icon in your browser, so the revelation by Codenomicon and Google researchers it was vulnerable to attack caused consternation.

For some online businesses such as Mumsnet in the UK the Heartbleed bug led to downtime and possibly lost revenue, while the Canada Revenue Agency (CRA) subsequently lost the social insurance numbers and details of 900 people, with thousands of others potentially victims of data theft as ongoing investigations continue.

Brokers say attacks such as these will lead insurance buyers to reassess their level of protection against cyber attacks. "I don't necessarily think Heartbleed will lead to an immediate upturn in insurance business but it will cause firms to look again at their cover," Peter Hacker, chief executive of the global communications technology and media practice at broker JLT, says.

Hacker estimates three out of 10 corporates will buy cyber risk or data breach cover at the moment, with many looking to business continuity planning and resiliency instead for protection. "This could change, however, as laws [and costs] strengthen, so there is room for growth in a digitalised world, especially as hack attacks proliferate and the cloud computing trend grows," he says.

"Remember, you can outsource processing but you cannot outsource the responsibility and as more and more corporate and customer data resides in the cloud with third-party processors some may turn to insurance to cover their risk instead of operations."

JLT estimates the cyber risk market at the moment is worth approximately £700m ($1.18bn) worldwide in terms of premium volumes but could double to £1.4bn by 2020 as cloud usage escalates. However, this depends on the future legal landscape and loss ratios, Hacker warns. It is also dependent on underwriters getting the pricing and policies right, he says.

Conversely, PricewaterhouseCoopers' (PwC) Daljitt Barn, a cyber-security director at the consultancy and ex-chairman of the UK Cyber Risk & Insurance Forum, estimates the market is worth around $1.3bn a year in the US and anywhere between £50m and £130m in the EU.

Hacker dismisses the term cyber risk as a bit of a buzz word, preferring instead to categorise it as a technology risk that should reside in an intangible asset risk portfolio approach that offers protection against intellectual property loss, data breach notification laws, legal fines and other risks, not just downtime tech risk.

It is also necessary to differentiate between standalone data breach insurance – popular in the US where laws covering this are strong but commonly underwritten in London – and the more holistic intangible asset risk approach favoured in London as a company-wide risk-management solution.

Expanding horizons are further evidenced by the recent AIG and Aegis London product launches, which show more and more types of risk emanating from technology vulnerabilities are now being covered.

Growth of the cyber insurance market is also likely to be spurred on by other recent hack attacks such as US retailer Target's loss of 110 million customer records earlier this year, including credit card numbers and customer addresses. As Tom Draper, technology and cyber practice leader at Arthur J Gallagher in London, says: "Heartbleed is simply another example of recent security breaches, following on from Target, Neiman Marcus, Michaels Stores and so forth, which demonstrate companies can only go so far to protect themselves [operationally].

"The cyber insurance market has established itself since the early 2000s as an effective risk-transfer mechanism and safety net for these [data breach] risks." It now has new growth avenues to explore.

Many insurers are now offering more of a service than simply risk transfer, with data breach response teams to assist insureds in the event of the claim, Draper says. "Most of the insureds purchasing coverage are from the US at the moment, with the focus being on the heavy data-collecting sectors such as healthcare, retail, and the public sector."

As many other jurisdictions – for example the EU, Australia and South Africa – look to mandatory data notification laws in the near future and regulatory fines, however, affected companies will start to purchase the covers as the risk increases, he adds.

**London calling**

According to Richard Horne, a cyber-security partner at PwC, most of the global insurance players are offering something in the cyber security arena or at least testing the water, but specific cyber risk standalone products, as opposed to data breach products, are rare in Europe.

"The US cyber insurance and data breach protection market is far more advanced than Europe at the moment, mainly because of their more stringent data breach security and privacy laws; these lend themselves to the development of clear risk policies," he says.

"In Europe at present we're behind the US, but I expect this to change as new EU [data breach] laws come into force and cyber risk goes up the corporate agenda. London underwrites much of the cyber insurance market at present, as you'd expect as the world's leading risk centre, but there isn't a fully developed or exploited 'home' [data breach] market yet."

It is a point Draper agrees with, pointing out the US is at present the main territory buying cyber insurance, but London offers innovation. "With more than eight Lloyd's syndicates, six companies and four specialist managing general agents, London is the market producing new products, combined with experienced underwriting and claims teams. Consequently, significant US, EU and global businesses are now looking to London for this expertise."

The threat to businesses' operations was illustrated at the turn of the year when the World Economic Forum identified cyber security as one of its top five risks facing the global economy in its 2014 Global Risk Report and even mentioned the possibility of a "cyber-geddon".

At the time, Axel Lehmann, chief risk officer at Zurich Insurance Group, said: "Trust in the internet is declining as a result of data misuse, hacking and privacy intrusion. Some reports indicate that 70% of net users have been attacked at some point and it can take firms 230 days to realise they've even been attacked… cyber-security is a reputational and share price issue for senior management and the board."

Zurich released its own report this month on the threat of cyber risk. Authored with the Atlantic Council, a thinktank based in Washington DC, the report invites readers to view the developing global reliance on technology as potentially as big a risk as the interconnectedness of financial institutions in 2008 before the crash.

"Just imagine if a major cloud service provider had a 'Lehmann Brothers moment', with everyone's data there on Friday and gone on Monday," Lehmann says. "If that failure cascaded to a major logistics provider or a company running critical infrastructure, it could magnify a catastrophic ripple running throughout the real economy in ways difficult to understand, model or predict beforehand. Especially if this incident coincided with another, the interaction could cause a crash or collapse of much larger scope, duration and intensity than would seem possible – similar to the series of events that struck the financial system in 2008." (see graphic)

Zurich's report also claims there were 740 million data files potentially viewed without permission or stolen worldwide in 2013. Data breach is a problem therefore, but the real interest of the report is in the interconnected cyber risk that is fast developing alongside the "internet of things". The threat this potentially poses to a world economy that is ever-more reliant on technology is what is animating the industry and causing it to act.

Where there is risk, there is opportunity, and the insurance sector is waking up to the growth possibilities in this area. ■

## Cyber cover evolution

Both AIG and Aegis London launched cyber insurance products in April, with the former offering protection against property and bodily damage from hack attacks via its expanded CyberEdge PC product line, while Aegis has launched its own Cyber Resilience product.

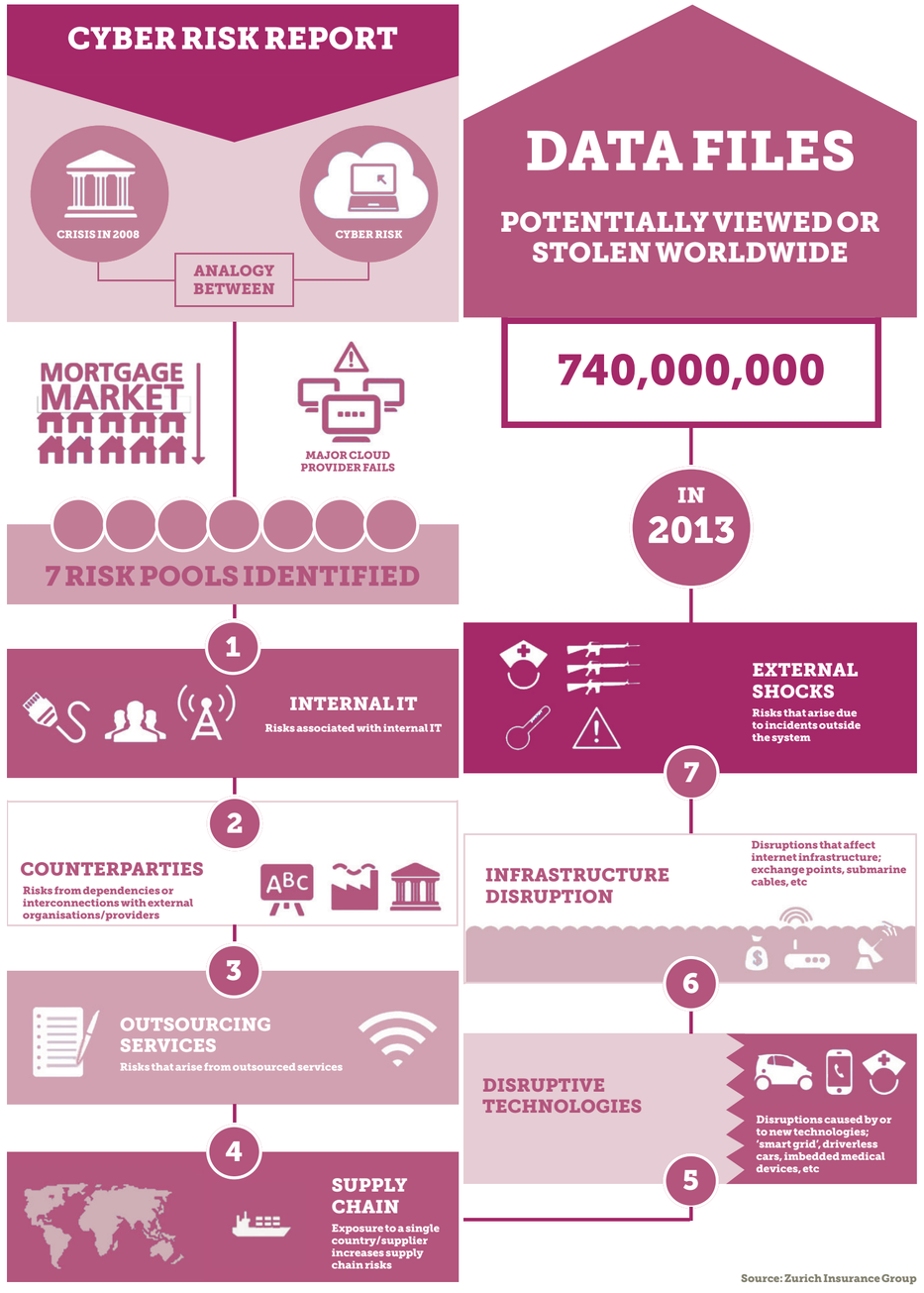
AIG's launch is particularly interesting as it seeks to protect power generation sites, building-management systems or pacemakers, effectively merging the corporeal and virtual worlds. The add-on to AIG's existing CyberEdge PC product line is aimed at commercial industries seeking to protect against equipment failure and physical damage to property and people. For example, industries using automated supervisory control and data-acquisition systems – like a power station – are concerned about the threat of computer viruses like Stuxnet, which reportedly damaged almost one-fifth of Iran's nuclear centrifuges, after the US and Israel allegedly unleashed the bug to impede Iran's nuclear programme.

Most cyber insurance policies cover the costs and liabilities associated with data breaches, cybercrime and hacking, but very few insurers will cover physical property damage and associated business interruption resulting from a cyber-attack or faulty software. CyberEdge PC enhances a customer's existing commercial lines insurance programme by providing cyber event protection on an excess and difference-in-conditions basis, AIG says. It addresses coverage gaps in property/casualty, energy, aerospace, marine, environmental, healthcare and financial lines policies, the insurer says, where cyber-related exposures may at present be excluded or coverage too limited.

Aegis London's Cyber Resilience launch is designed to protect operational technology and assets, before and after a cyber-attack. The product combines liability, business interruption and terrorism coverage with a service-based offering that consists of cyber underwriting assessment, risk-management consultancy, loss control, threat analysis, incident response and vulnerability management.

**"Heartbleed is simply another example of recent security breaches, following on from Target, Neiman Marcus, Michaels Stores and so forth, which demonstrate companies can only go so far to protect themselves [operationally]"**

**Tom Draper**
**Arthur J Gallagher**




Source: Zurich Insurance Group