HOT TOPIC

IS THE INSURANCE INDUSTRY READY FOR A CYBER FUTURE?

Liz Booth examines the fallout from the recent WannaCry cyber attack and sees how the insurance industry would have coped had more firms been insured

Is cyber the new asbestos for the insurance industry? That was just one of the questions industry insiders were asking as the WannaCry cyber attack unfolded in mid-May.

Luckily for the insurance industry, this time around few of the affected entities had cyber insurance. Had they had cover, the question for the industry is whether or not it could have coped.

WannaCry, a ransomware programme, is reported to have infected more than 230,000 computers in 150 countries. Hackers demanded payment in bitcoins to allow users to access their own data.

Among those infected were several large companies, including a major American parcel delivery company, a European car manufacturer and a Spanish telecom company. It disrupted the operations of Britain's National Health Service and affected some operations of German rail network Deutsche Bahn.

The insurance industry appears to have got off lightly, however. Kenneth Dort, partner at Drinker Biddle, says: "In our experience, entities that do not take reasonable steps to protect their data through patching or regularly backing up data, would very likely not have gone the extra step to obtain cyber insurance as they are likely already tightly controlling IT costs.

"Further, entities that are not updating and patching would probably not be able to pass a baseline audit from a cyber insurance carrier. As a result, cyber insurance would likely have not been a consideration for many of the entities that were victimised by the WannaCry attack."

SCRATCHING THE SURFACE

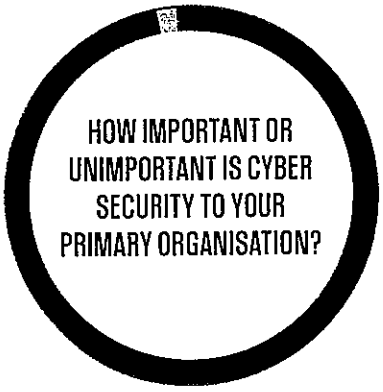
Fortinet, a security company, has warned, however, that this attack could be just the tip of an iceberg of problems waiting to happen. And the general view is that companies need to be proactive in terms of security and in terms of buying insurance.

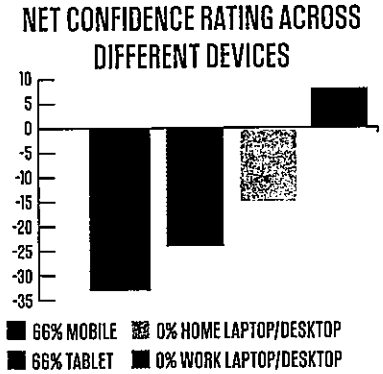
This is backed up by figures from the UK's Institute of Directors (IoD), which reveals in a report published before the WannaCry attack, that:

- Some 95% of 1,000 business leaders surveyed consider cyber security to be very or quite important to their business and yet 45% do not have a formal cyber security strategy;
- IoD members are aware of the threat but just above 50% have protected all of their devices and less than a third use virtual private networks;
- If the victim of an attack, some 40% would not know who to contact
- Only 44% have laid on cyber awareness training and many leave gaps of more than a year between training programmes;
- Some 73% have a process in place when receiving invoices and requests for electronic payments to verify their legitimacy.

According to insurer Allianz, however, companies are becoming increasingly aware of the need to protect themselves.

This is why the cyber insurance market promises to be the next blockbuster in the insurance space, according to Hartmut Mai, chief underwriting officer for corporate lines at Allianz Global Corporate & Specialty (AGCS).





Source: IoD Policy Report March 2017: Cyber Security

Cyber insurance is already a mature market in the US, with estimated premium volume of $3bn. However, "the more the industry integrates supply chains and processes, and digitalises production into 'smart factories', the more vulnerable the long-established industrial companies become as well", says Mr Mai. He adds: "For them, the risk of business interruption tends to be paramount."

And the threat does not always come from hackers. Many times, it is a technical failure or an employee deliberately or accidentally introducing viruses or paralysing computer systems.

When a crisis unfolds, compensation for financial loss is important, but the support services that often accompany cyber insurance are invaluable. Computer forensics, data and systems recovery, as well as professional crisis communication, can help a policyholder get back on its feet quickly.

"Assistance services, which we provide ourselves or through our partners, are therefore becoming increasingly important," says AGCS's Mr Mai.

There are issues, however. "We lack historical claims data. Also, companies shun publicity when they have been victims of a hacking attack because they are worried about their reputation," he adds.

Another major consideration is accumulation risk. "At the moment, the accumulation risk is still manageable because not many companies in Europe, Asia and Africa have cyber insurance yet," Mr Mai points out.

However, just like directors and officers liability coverage, cyber insurance is expected to become the standard for companies over the medium term. "Cyber insurance will be a blockbuster - and we must prepare ourselves for it. When the much stricter data protection regulations take effect in Europe in 2018, not just big corporations but also mid-market and smaller companies will want to buy cyber coverage," Mr Mai says. ↘