UK actuaries devise cyber risk assessment scenarios

19 October 2018

Published in: Risk management, Corporate strategy, Solvency II, Associations, UK, Software - IT

Companies: Institute and Faculty of Actuaries

The UK's Institute and Faculty of Actuaries (IFoA) has costed three potential cyber risk scenarios - and proposed ways to mitigate and deal with the operational risks that arise.

The three scenarios, put forward in a research paper by the IFoA's cyber risk investigation working party, each attempt to calculate the expected loss in an incident with a 1-in-200 year return period.

They are:

- An employee leaks data at a motor insurer with records of 4m customers. This could cost £210m ($273.8m) or 2% of the fictitious company's total revenue, mainly comprising customer compensation and regulatory fines
- Cyber extortion of a life insurer with annual gross written premiums of £3bn and annual profit of £300m. This could cost £180m, or 6% of annual revenue, mainly due to business interruption and lapses on in-force policies.
- A hack of a motor insurer's 500,000 telematics devices, which involves the publication of locations, photos and journey of high-profile policyholders. This could cost £70m, or 18% of annual revenue, about half of which is the cost of replacing vulnerable devices.

For each scenario, the IFoA has summarised possible mitigating actions. For example, in the case of an employee leaking data at a general (non-life) insurer, the research recommended staff training relating to data protection laws and corresponding penalties for breaches. It also suggested incentives for reporting problems, concerns and whistleblowing.

When designing an operational risk scenario, the IFoA stressed it is important to think through a range of factors relevant to the scenario such as:

- structure and size of the company;
- types of insurance products written; and
- IT systems used within the business including dependencies/contingencies in place and third-party dependencies.

Overall, the paper said: "The investment in understanding cyber risk now will help to educate senior management and could have benefits through influencing internal cyber security capabilities."

Ronan McCaughey