Just 25% of Australian businesses are insured against cyber attacks. Here's why

November 8 2022, by Jongkil Jay Jeong and Robin Doss

Credit: AI-generated image (disclaimer)

In the past financial year, the Australian Cyber Security Centre received 76,000 cyber-crime reports—on average, one every seven minutes. The year before, it was a report every eight minutes. The year before that, every ten minutes.

The growth of cyber crime means it is now arguably the top risk facing any business with an online presence. One successful cyber attack is all it takes to ruin an organization's reputation and bottom line. The estimated cost to the Australian economy in 2021 was $42 billion.

To protect itself (and its customers), a business has three main options. It can limit the amount of sensitive data it stores. It can take greater care to protect the data it does store. And it can insure itself against the consequences of a cyber attack.

Cyber-insurance is a broad term for insurance policies that address losses as a result of a computer-based attack or malfunction of a firm's information technology systems. This can include costs associated with business interruptions, responding to the incident and paying relevant fines and penalties.

The global cyber-insurance market is now worth an estimated US$9 billion (A$13.9 billion). It is tipped to grow to US$22 billion by 2025.

But a big part of this growth reflects escalating premium costs—in Australia they increased more than 80% in 2021—rather than more business taking up insurance.

So coverage rates are growing slowly, with about 75% of all businesses in Australia having no cyber-insurance, according to 2021 figures from the Insurance Council of Australia.

Challenges in pricing cyber-insurance

With cyber-insurance still in its infancy, insurers face significant complexities in quantifying cyber risk pricing premiums accordingly—high enough for the insurers not to lose money, but as competitive as possible to encourage greater uptake.

A 2018 assessment of the cyber-insurance market by the US Cybersecurity and Infrastructure Security Agency identified three major challenges: lack of data, methodological limitations, and lack of information sharing.

Lack of historical loss data means insurers are hampered in accurately predicting risks and costs.

Because of the relative newness of cyber crime, many insurers use risk-assessment methodologies derived from more established insurance markets such as for car, house and contents. These markets, however, are not analogous to cyber crime.

Companies may be hesitant to disclose information about cyber incidents, unless required to do so. Insurance carriers are reluctant to share data pertaining to damage and claims.

This makes it hard to create effective risk models that can calculate and predict the likelihood and cost of future incidents.

So what needs to be done?

Deakin University's Centre for Cyber Security Research and Innovation has been working with insurance companies to understand what must be done to improve premium and risks models pertaining to cyber insurance.

Here is what we have found so far.

First, greater transparency is needed around cyber-related incidents and insurance to help remedy the lack of data and information sharing.

The federal government has taken two steps in the right direction on this.

One is the Consumer Data Right, which provides guidelines on how service providers must share data about customers. This came into effect in mid-2021.

The other is the government's proposal to amend privacy legislation to increase penalties for breaches and give the Privacy Commissioner new powers.

Second, insurers must find better ways to measure the financial value and worth of the data that organizations hold.

The primary asset covered by cyber insurance is the data itself. But there is no concrete measure of how that data is worth.

The recent Optus and Medibank Private data breaches provide clear examples. The Optus event affected millions more people than the Medibank Private hack, but the Medibank Private data includes sensitive medical data that, in principle, is worth far more than data regarding just your personal identity.

Without an accurate way to measure the financial value of data, it is difficult to determine the appropriate premium costs and coverage.

Cyber insurance is a new, specialized market with significant uncertainty. Given the ever-increasing risks to individuals, organizations and society, it is imperative that insurers develop robust and reliable risk-based models as soon as possible.

This will require a consolidated effort between cyber-security experts, accountants and actuaries, insurance professionals and policymakers.

Provided by The Conversation