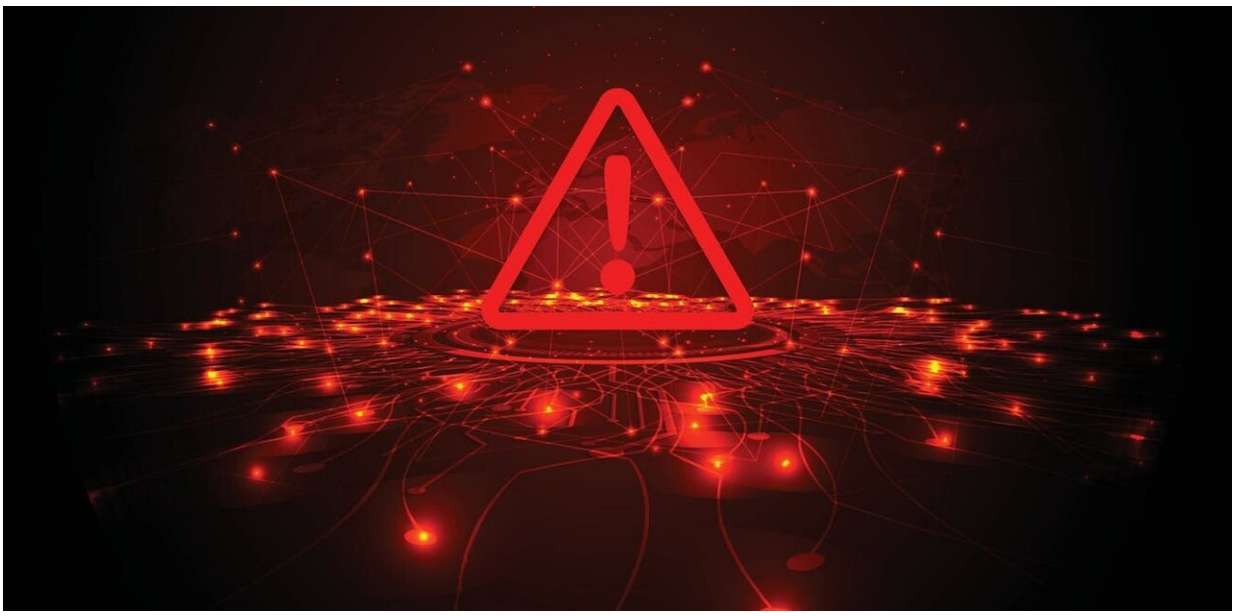
# Australia is considering a ban on cyber ransom payments, but it could backfire. Here's another idea

November 14 2022, by Jeffrey Foster and Jennifer J. Williams



Credit: Shutterstock

First Optus, now Medibank; in less than two months we've experienced two of the largest personal data breaches in Australia's history. In both cases the hackers attempted, and failed, to extort a ransom in exchange for not releasing personal data.

So far the Optus hackers have released only a small sample of data, and

claim to have deleted the rest. On the other hand, the Medibank hackers have released the records of more than one million people—and have threatened to release more data on Friday.

With this looming threat, the Australian government is looking to bolster its cybersecurity defences—including through a taskforce set up to retaliate against the Medibank hackers.

Minister for Cyber Security Clare O'Neil has said the government is also considering making ransom payments to cybercriminals illegal. The idea has picked up steam—but would this cure be worse than the disease?

## The response to the Medibank hack

The group behind the latest Medibank hack, currently being called "BlogXX", has been linked to Russian cybercriminal organisations by the Australian Federal Police. It has known links to the notorious REvil cyber gang (which was dismantled by Russia's Federal Security Service in January).

Large-scale cybercriminal gangs are able to extort high ransom payments from their victims. During REvil's arrest, authorities seized the equivalent of A$12.8 million in cash, $7 million in crytpocurrency and 20 luxury cars.

There are multiple ways to decrease the profitability of data breaches for criminal organisations. The first is to make hacks more difficult, making it more time-consuming for the hackers to break into computers.

This could be achieved by increasing fines for organisations that fail to follow best practices in cybersecurity—a privacy reform that was recently introduced in Australia and has passed through the lower house.

A second potential solution is to make ransomware payments illegal in Australia. Under some circumstances, it may already be illegal for Australian organisations to pay a ransom, such as if the payment funds further criminal or terrorist activity of groups under sanction by the United Nations.

However, the attribution of cyberattacks is difficult, and it's not always possible to know whether paying a particular group would be a crime. An organisation may pay a ransom, only to find out much later it has broken the law.

## When banning ransom payments works

The idea of banning ransom payments isn't new. In April, Nigeria criminalised ransom payments to kidnappers. However, not paying kidnap ransoms in Nigeria has also resulted in deaths, which suggests this approach may end up punishing victims.

Still, survey results show citizens and cybersecurity experts are generally in favour of banning ransomware payments. In a recent survey of UK residents by security firm Talion, 78% of respondents from the general public supported a ban, as did 79% of cybersecurity professionals.

A ban on ransom payments could quickly reduce the profits racked up by criminal gangs targeting Australia.

In cases like the recent Optus and Medibank hacks, where the ransom was demanded to "not leak" sensitive information, banning ransom payments may be a good idea. It could take the burden of making a decision away from the organisation targeted, and mitigate the public's judgment of that decision.

It would also reduce (but not entirely remove) the possibility of criminals

receiving ransom payments—and therefore make their operations less profitable.

## The problems with a ban

However, unlike the Optus and Medibank breaches, many ransoms are paid to unlock encrypted computers. Some ransomware attacks involve the hackers encrypting all of the computers, data and backups a company has. Failing to restore those data can, in many cases, cause the business to collapse.

In such instances, banning ransom payments may discourage organisations from declaring breaches. They may pay the ransom to be able to move on with business—even if it is a crime. Should this happen, it would reduce the overall transparency of reporting on breaches, and could lead to hackers blackmailing victims to not divulge the hack.

This particular concern has led the US Federal Bureau of Investigation to recommend to the US Senate Judiciary Committee to not ban all ransom payments.

For a ban on ransom payments to be effective, the penalties for paying the ransom would need to be more severe than the impact of the ransom itself. If the penalties are inadequate, organisations may simply pay the ransom and deal with the legal consequences so they can move on with normal operations.

## An alternative solution

Cyberinsurance policies often provide reimbursement for ransomware payments. In fact, it's a common tactic for cybercriminals to demand a ransom equivalent to the insurance reimbursement. While this means the organisation suffers fewer losses, the cybercriminals still profit.

A more nuanced approach may be to ban cyberinsurance reimbursements for ransom payments, which would reduce the overall percentage of breaches that result in a payment. This could reduce profits for criminal gangs, while still allowing a company to salvage its operations under the worst-case scenarios.

The decision to ban or not to ban ransomware payments is complicated, and a blanket ban is likely to cause more problems than it fixes. We need change, but the best solution would be a case-by-case approach.

In the end, these kinds of cybercrimes are unlikely to be eradicated by any single policy change. They will require a wide range of policies, laws and regulations that each chip away at specific problems. If we do this, eventually the cost to criminals could outweigh the profits.



Provided by The Conversation

Citation: Australia is considering a ban on cyber ransom payments, but it could backfire. Here's another idea (2022, November 14) retrieved 1 June 2023 from https://techxplore.com/news/2022-11-australia-cyber-ransom-payments-backfire.html