Forgiveness or punishment? Australia's proposed 'safe harbor' laws send mixed messages on cyber security

November 22 2023, by Greg Austin

Credit: Pixabay/CC0 Public Domain

Should companies experiencing cyber attacks be forgiven if they cooperate with the government to stop such attacks? That's the idea the

federal government is considering with its possible "safe harbor" laws.

Last week, the defense minister, Richard Marles, floated the idea of introducing a legally binding exemption from punitive government litigation if a company self-reports to the Australian Signals Directorate (the national signals intelligence agency) and invites its help.

The aim would be to drive more effective collaboration between the private sector and the directorate in dealing with cyber attacks, resolving them faster or preventing them altogether.

But the plan risks undermining the government's attempts to crack down on corporations that don't do enough to keep their clients' data safe.

Reluctance to work together

The government says it's struggling to overcome resistance by many Australian companies facing a cyber attack to work with the directorate to help defeat intrusions.

Companies are afraid to suffer the inevitable reputation loss if news of the breach leaks out.

They also fear exposing themselves to government fines or customer litigation of the sort being pursued by victims of data breaches at Medibank and Optus.

On the government side, the Australian Signals Directorate has complained their efforts to help companies under attack are being hampered by lawyers concerned mostly with minimizing the risk of the company being sued in the future.

This is in direct contrast to the practice of leading US tech companies

who prefer lawyers to be the first people involved in the response.

A so-called 'safe harbor'

The government's safe harbor offer would involve legislation.

The safe harbor principle is an exemption that can be granted for actions that might otherwise break the law if there's a larger public good at play.

This is used in other areas of regulation, such as bankruptcy law and tax law. It provides legal protections for administrators or accountants who have to take on risky business decisions in order to do their jobs.

Richard Marles claimed a safe harbor regime for self-reporting companies affected by a cyber attack would do two main things.

Firstly, he said, it would deliver the world-class capabilities of the Australian Signals Directorate to the affected company.

Secondly, Marles said it would help drive trust between the government and reticent private sector businesses.

The government has proposed that complying with the cyber safe harbor requirements would shield companies from further legal action by the government.

In its cyber security strategy, released today, the government committed to consultations with industry on a legislated measure to help build the sort of trust outlined in Marles' discussion of safe harbor.

But we don't have any other detail about how this version of safe harbor law would work.

And for most corporations, the government may be the least of their worries in cases of large-scale data breaches or breaches of sensitive intellectual property information.

They will be concerned about the reputational damage first and foremost.

For listed companies, this can lead to a sustained drop in share price and open a pathway to costly law suits from seriously affected clients or business partners.

Safe harbor laws don't do much to help with that.

Would laws like this work?

In cyber security, the concept of safe harbor is complicated and fraught with definitional and regulatory challenges.

Such laws for cyber security are used in several US states mainly for promoting stronger compliance with industry standards. This is done by promising companies a degree of protection from various types of litigation if they are certified by the government to be reasonably compliant with the standards.

An Australian study throws some doubt on the value of that process.

The research shows such standards are seen as a low bar, or even inappropriate in some situations.

Technology always moves more quickly than standards. For example, in May 2023 an intergovernmental working group found the security standards for 5G were "incomplete" and did not cover all security requirements. Australia has been using 5G technology since 2019.

The safe harbor laws may also be too weak to achieve what they set out to do.

A US study warns a safe harbor law for the US health sector "only offers some protection in certain circumstances".

Forgiveness or punishment?

The new Australian proposal, coming from the defense department in 2023, and raised in Senate Estimates in 2022 by an opposition senator, appears to support the defense portfolio's interest in better national security.

But there is a reasonable risk it will undermine the mission of the home affairs minister, Clare O'Neil.

She has staked much on the need to punish corporations who may have acted irresponsibly in allowing serious data breaches.

Corporations will remember her statement in September 2022 that fines of hundreds of millions of dollars for large privacy breaches might be more appropriate than the existing cap of $2.2 million.

By December, new legislation imposing penalties up to $50 million had come into force.

The moves were designed in part to dampen community outrage over the data breaches.

But the safe harbor idea might increase the consumer concerns O'Neil has been working to allay.

Not all cyber attacks involve a risk of exposing large amounts of

personal data, so there would be instances where the safe harbor option would not affect a person's rights to seek redress.

But by its very nature, the proposal will impact the rights of businesses and consumers to know if they have suffered damage or loss from a cyber attack.

The government has a moral obligation to inform victims of cyber crime.

At a time of escalating cyber uncertainties, increasing ransomware attacks, and stepped up Russian and Chinese cyber attacks, the safe harbor proposal will need careful consideration.

The government will want to avoid antagonizing public sentiment by limiting the rights of consumers.

So a solution that promises protection only against government litigation, but not civil litigation, may not be worth the political balancing act.

Provided by The Conversation