Why are there so many data breaches: A growing industry of criminals is brokering in stolen data

James Martin, *Deakin University* and Chad Whelan, *Deakin University*

New details have emerged on the severity of the Medibank hack, which has now affected all users. Optus, Medibank, Woolworths, and, last Friday, electricity provider Energy Australia are all now among the household names that have fallen victim to a data breach.

If it seems like barely a week goes by without news of another incident like this, you would be right. Cybercrime is on the rise – seven major Australian businesses were affected by data breaches in the past month alone.

But why now? And who is responsible for this latest wave of cyber attacks?

In large part, the increasing number of data breaches is being driven by the growth of a global illicit industry that trades in your data. In particular, hackers known as "initial access brokers" specialise in illegally gaining access to victim networks and then selling this access to other cyber criminals.

The cyber crime ecosystem

Hackers and initial access brokers are just one part of a complex and diversifying cyber crime ecosystem. This ecosystem contains various cyber criminal groups who increasingly specialise in one particular aspect of online crime and then work together to carry out the attacks.

For example, one of the fastest-growing and most damaging forms of cyber crime – ransomware attacks – involves malicious software that paralyses a victim's device or system until a decryption key is provided following payment of a ransom.

Ransomware attacks are big business. In 2021 alone, they earned cyber criminals more than US$600 million. The huge amounts of money to be made in ransomware, and the rich abundance of targets from all around the world are fostering the development of a vast ransomware industry.

Ransomware attacks are complex, involving up to nine different stages. These include gaining access to a victim's network, stealing data, encrypting a victim's network, and issuing a ransom demand.

Specialist criminals

Increasingly, these attacks are carried out not by lone cyber criminal groups, but rather by networks of different cyber crime groups, each of which specialises in a different stage of the attack.

Initial access brokers will often carry out the first stage of a ransomware attack. Described by Google's Threat Analysis Group as "the opportunistic locksmiths of the security world", it's their job to gain access to a victim's network.

Once they have compromised a victim's network, they typically sell this access to other groups who will then steal data and deploy the ransomware that paralyses the victim's computer systems.

There is a massive and growing underground market for this type of crime. Dozens of online marketplaces on both the dark web and surface web offer services from initial access brokers.

Their access to companies can be purchased for as little as US$10, although more privileged, administrator-level access to larger companies often commands prices of several thousands of dollars or more.

Responding to the growing cyber threat

Over the past month, we have seen several instances of cyber criminals forgoing actual ransomware. Instead, they sought to directly extort companies by threatening to publicly release any data they have stolen.

While not as devastating as a ransomware attack, data breaches can cause serious financial and reputational damage to an organisation (just ask Optus chief executive Kelly Bayer Rosmarin), not to mention major problems for any customers or clients who now have their private information released online.

In the final six months of 2021, more than 460 data breaches were reported to government authorities. Even more worryingly, this number is almost certainly an underestimate.

While companies with a turnover of more than AU$3 million are required by law to report data breaches involving personal information, most small businesses are not subject to mandatory reporting laws. Therefore, they have little incentive to report a data breach that could scare off customers and damage their brand.

Taking action against cyber crime

So what can we do about it? In the first instance, companies need to rethink their approach to data. Data should be treated not simply as an asset that can be freely held and traded in, but also as a liability that needs to be carefully protected.

Some experts are calling for Australia to follow the European Union’s approach and to introduce stricter corporate regulations that better protect consumer data.

This week the federal government also introduced plans to fine companies that do not maintain sufficient cyber security and suffer repeated data breaches.

Reforms like this could help, particularly in preventing relatively unsophisticated data breaches, like the one that recently affected Optus.

On the other hand, punitive fines towards victims could further strengthen the hand of entrepreneurial cyber criminals – they could try to leverage these fines to further extort their victims.

There is no silver bullet to solving the threats posed by cyber criminals. At a minimum, both government and industry must continue to work together to improve our cyber defences and resilience. Through research, we must also work to better understand the global cyber crime ecosystem as it continues to evolve.

James Martin, Senior Lecturer in Criminology, *Deakin University* and Chad Whelan, Professor of Criminology, *Deakin University*