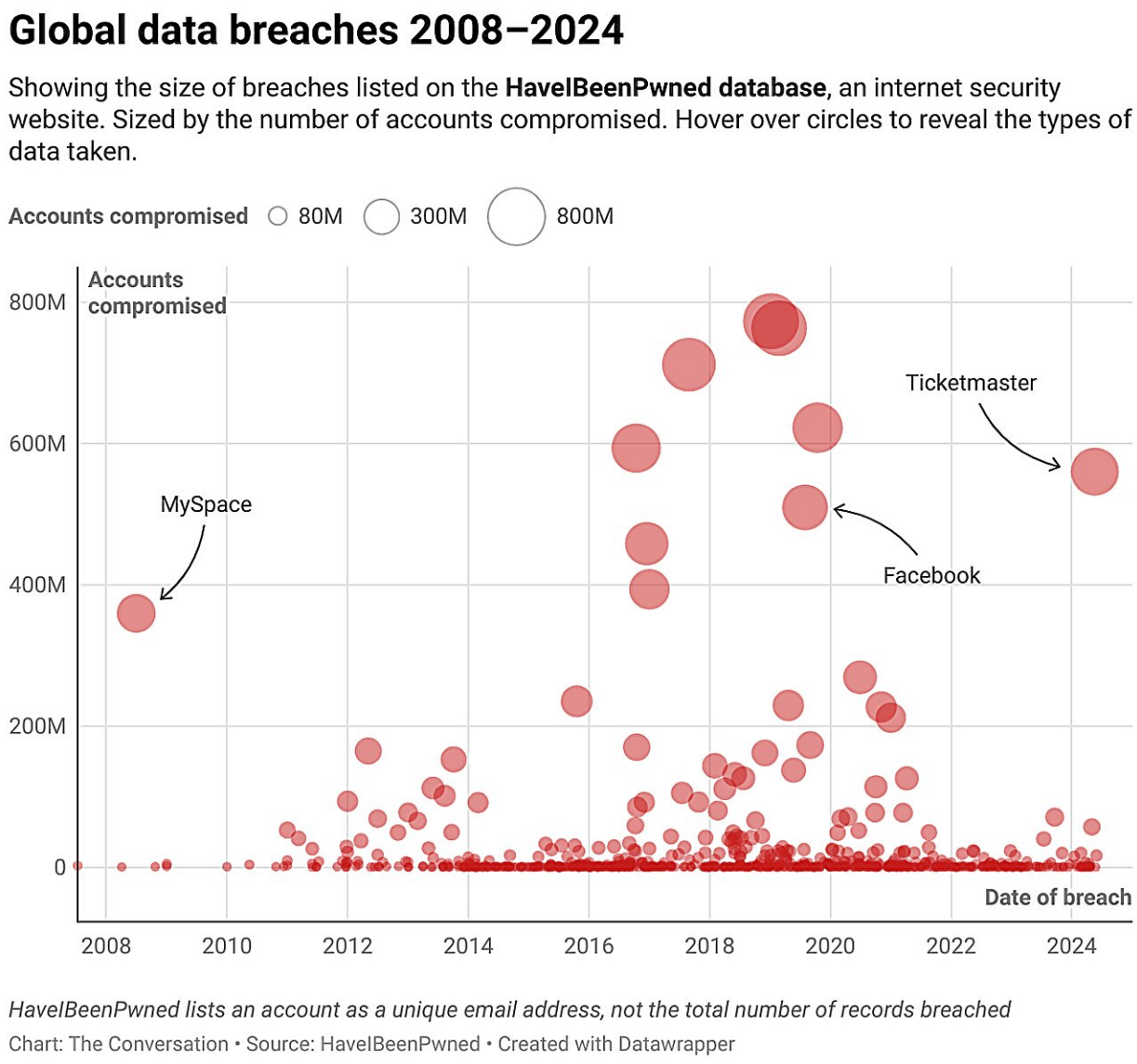
Are data breaches the new normal? Should we just assume our data isn't safe?

June 5 2024, by Sigi Goode



Credit: The Conversation

In recent days, both Ticketek Australia and Ticketmaster have experienced breaches which have exposed customer details to hackers. They join a growing list of high-profile data breaches that have put the privacy of millions at risk.

For example, in 2022, Optus disclosed a breach of 9.8 million records. In 2023, Latitude, the Australian financial services firm, experienced a data breach of more than 14 million records.

My own university, the Australian National University, experienced a data breach of 200,000 records in 2018. Dan Murphy's, Football Australia, Microsoft, Nissan, Dell, Roku, Suncorp and Shell have all experienced breaches so far in 2024.

Despite advancements in technology and increased awareness of cybersecurity threats, companies continue to fall victim to breach attacks.

It may feel like these breaches are becoming more frequent, and that seemingly any firm is a data breach target waiting to happen. But the situation is not quite so clear-cut.

What happens in a data breach?

A data breach is an unauthorized access or disclosure of sensitive, confidential or private information: customer identities, payment methods, account details, purchase histories and so on.

Breaches can happen when cyber criminals exploit vulnerabilities in computer systems, networks, applications or physical security to gain unauthorized access to protected data. They can also access data when

it's accidentally made available outside the organization, perhaps by an incorrectly addressed email or a lost USB memory stick.

Australia has actually seen a fairly steady rate of notifiable data breaches since 2020—around 450 every six months, according to the Office of the Australian Information Commissioner.

While these figures are higher than when the notifiable data breach program began in 2018, it's important to understand this is partly a consequence of requiring organizations to disclose breaches: the more you look for something, the more you're going to find it.

Even if the number of data breaches is not increasing significantly, the average cost and severity of these breaches has risen substantially. According to IBM, the average cost of a data breach was US$4.45 million (A$6.69 million), an increase of 15% over three years. So what's driving these increases?

The value of your personal data is going up

Increased demand for targeted advertising and the growing importance of data-driven decision making have fueled the need for richer customer data.

Many organizations—not just legitimate ones—want to know more about you, and at a much more granular level than before. The more comprehensive and accurate the data, the more valuable it becomes.

Increasingly stringent privacy regulations, such as the European Union's General Data Protection Regulation (GDPR) and Australia's Privacy Act have driven organizations to improve their data management practices and security measures to protect user information and avoid costly fines.

This has made it harder, not easier, for cyber criminals to acquire user data in bulk.

Meanwhile, markets for illicit customer data are becoming more popular as anonymising networks and tools become more user friendly. Tools for selling on the dark web have also become more advanced, allowing cyber criminals to collaborate and share information about in-demand data, potential targets and new attack modes.

Once a cyber criminal has obtained some data, finding a buyer is much easier than it was even a few years ago.

However, large firms are investing more in protecting and storing data. According to consulting firm Gartner, 87% of chief information officers in Australia and New Zealand will be increasing their cybersecurity budgets this year.

As a result, data and cybersecurity practices are becoming more complex, increasing the skill needed for a bad actor to make a successful attack.

How do I protect my data with so many breaches happening?

While our personal data continues to have value, there will be a market for it. Make sure you practice good cybersecurity habits.

- Regularly review and delete inactive accounts, and monitor your accounts for strange activity.
- Enable two-factor authentication (2FA) on your accounts and devices, so that you'll receive a prompt on your phone when someone logs into your account, or transfers money out of it.

Don't believe cold callers who want you to deactivate or give them your two-factor responses.

- Be very selective about the personal info you share online, particularly information such as birthdays, when and where you were born, and the names of pets and family members. This information can be used to defuse account recovery questions.
- Don't click on suspicious email links, regardless of how innocuous they might appear.
- Never provide sensitive information to unknown or unverifiable sources, especially cold callers who claim you have a virus, or are due for a refund. Authentic callers will be happy for you to call them back on an official number.

The best way to think about the data breach problem is not to think about how our data can be breached, but to think about how organizations get your data in the first place. The best way to protect yourself online—whether it's data breaches or an account compromise—is to guard your data jealously.

You only have one identity: don't give it away easily.

Provided by The Conversation

Citation: Are data breaches the new normal? Should we just assume our data isn't safe? (2024, June 5) retrieved 16 August 2024 from https://techxplore.com/news/2024-06-breaches-assume-isnt-safe.html