



The rise of Australian mega data breaches

Analysis of 6,000 Notifiable Data Breach reports since 2018



Introduction

“The Notifiable Data Breach scheme requires Australian businesses to report any data breach involving personal information to the OAIC if it could result in serious harm.

“Our report analyses every NDB report submitted to the OAIC since the scheme’s inception in 2018 – more than 6,000 in total. It reveals an alarming trend of major breaches affecting 1,000 or 10,000 individuals and a doubling of mega breaches involving more than 1,000,000 people.

“The data also shows how different industries diverge on data breach response. The Australian public sector is notably poor at both identifying and responding to breaches in a timely fashion. But at least the public sector is reporting to the OAIC. The data suggests that underreporting is a chronic issue in the private sector.”



**Ajay Unni, StickmanCyber
CEO and founder**

Key findings and methodology

In October 2024, StickmanCyber sent a Freedom of Information request to the OAIC and received data on 6,000+ reports submitted to the Government under the notifiable data breach scheme between February 2018 and October 2024.

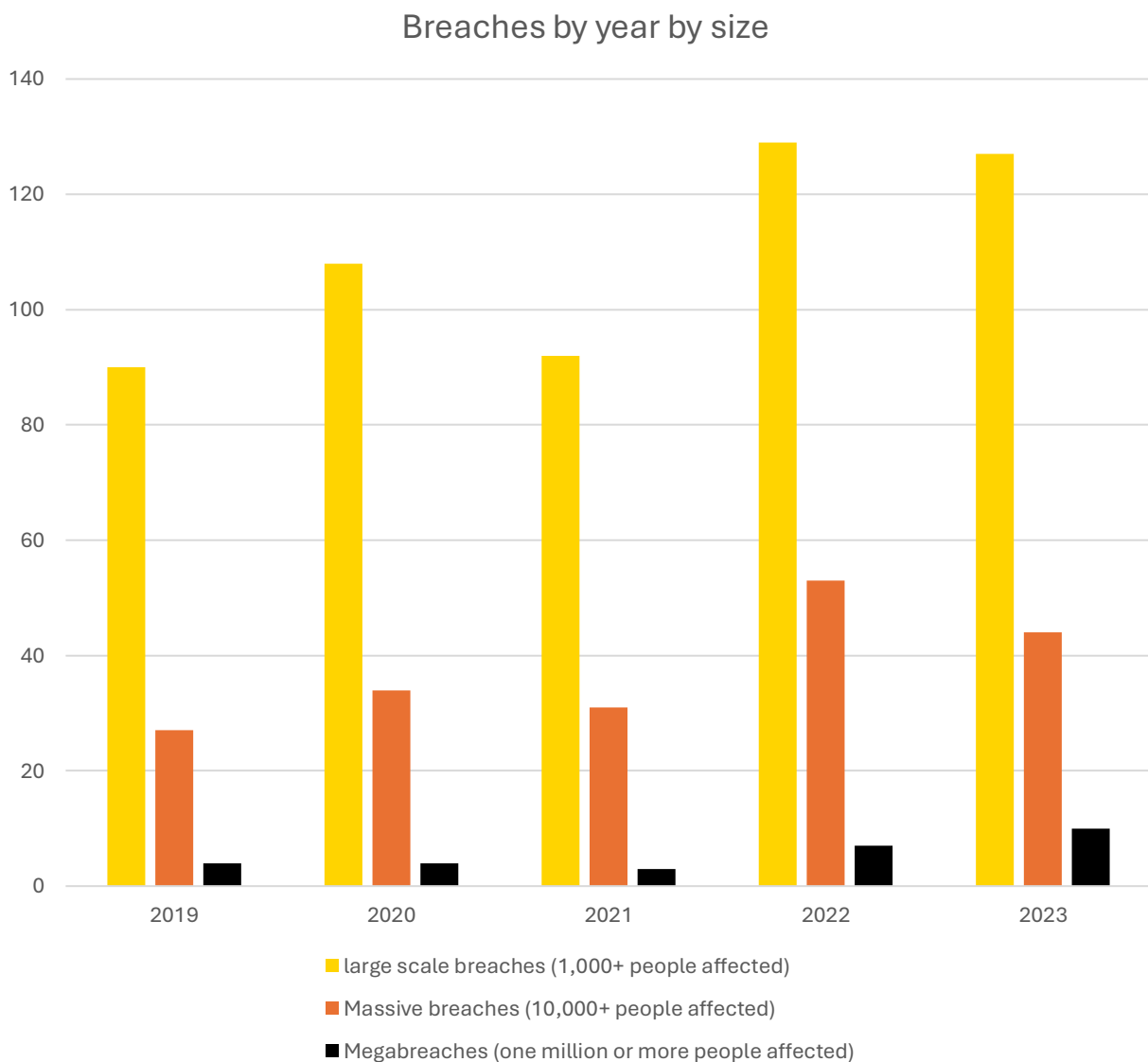
Stickman conducted analysis of the information provided, including analysis of as yet unreleased OAIC data. Key findings include:

- Large scale data breaches involving 1,000 people or more have increased by 40% in the last 5 years. Breaches involving one million people or more have doubled
- Nearly a third of these megabreaches (28%) stayed undetected for weeks (30 days or longer)
- Australian Government organisations are among the worst at identifying data breaches. They are nearly twice as likely to take 30 days or more to spot a breach
- The healthcare and finance sectors report the most data breaches to the OAIC, but Stickman believes that breaches are chronically underreported nationwide
- Healthcare and Education sectors are plagued by user error. So far in 2024, 60% of all education breaches are the result of user error
- Australian businesses may be missing a third of data breaches reported in the peak of summer holidays – reports submitted in January are 33% lower than the average month
- Businesses are slower to report data breaches in January than in any other month

Rise of large scale and mega data breaches

Headlines about massive data breaches affecting millions of people have become a common occurrence in recent years, but it's important to note how drastically and quickly this trend has emerged.

In 2019 and 2020, there were just 4 breaches involving one million people or more per year according to OAIC NDB reports. In 2022 and 2023, there were 7 and 10 respectively. There were also significantly more breaches involving 10,000 individuals or more in 2022 and 2023 compared to previous years.

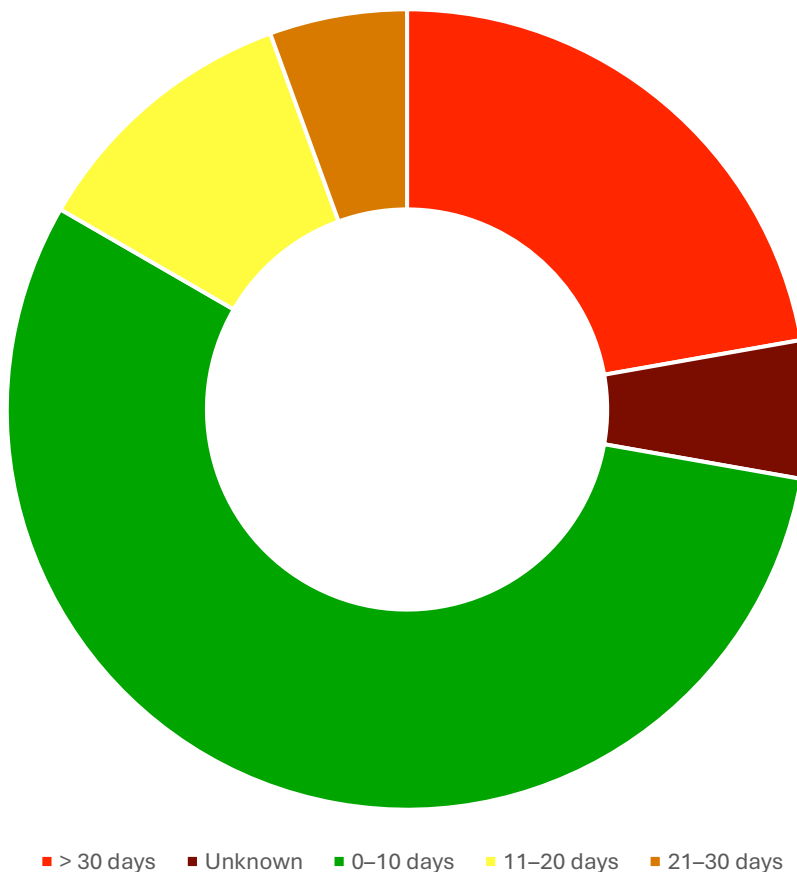


Megabreaches remain undetected for weeks

Of the 36 mega breaches involving 1 million people or more since 2018, 10 took longer than 30 days to be identified, or the organisation involved failed to provide an identification date in its report to the OAIC.

We are routinely forced to trust large enterprise organisations with our data. It's completely unacceptable that any organisation with data on millions of individuals could take weeks to discover it was the victim of such a large breach. Or could not provide an accurate identification date in its report to the OAIC. The fact that this happens in nearly a third of all mega breaches is staggering.

Mega breaches - Time to identify

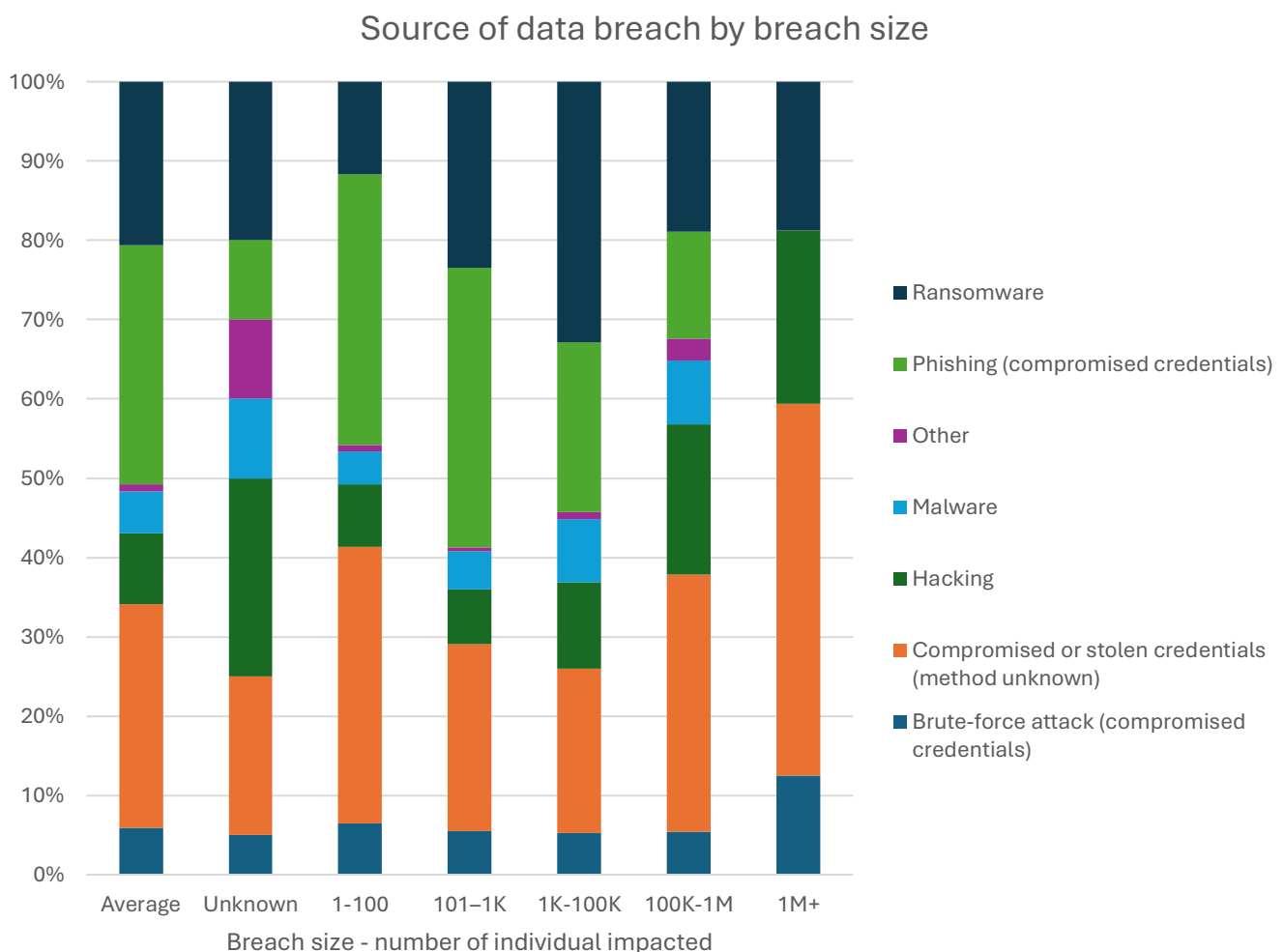


Why mega breaches happen

The OAIC has shared source of data breach statistics by breach size for 2,600 data breaches that were the result of a cyber incident – this does not include breaches that were the result of other breaches such as physical theft, social engineering etc.

Cyber incidents leading to data breaches involving 1m records or more are relatively rare, so we should add the caveat that this is a small sample size. However, it's interesting that none of Australia's mega breaches were the result of malware or phishing. Instead, the vast majority were the result of compromised credentials. It's proof that even the biggest organisations, which we expect to have the most advanced security, can be undone if an employee reuses credentials, their credentials are lost/stolen in another breach, or an attacker finds other means to obtain them.

It's alarming that *how* these credentials were stolen is “unknown” in nearly half of all mega breach incidents. Large enterprise organisations typically conduct thorough investigations of data breaches precisely to discover details such as this.

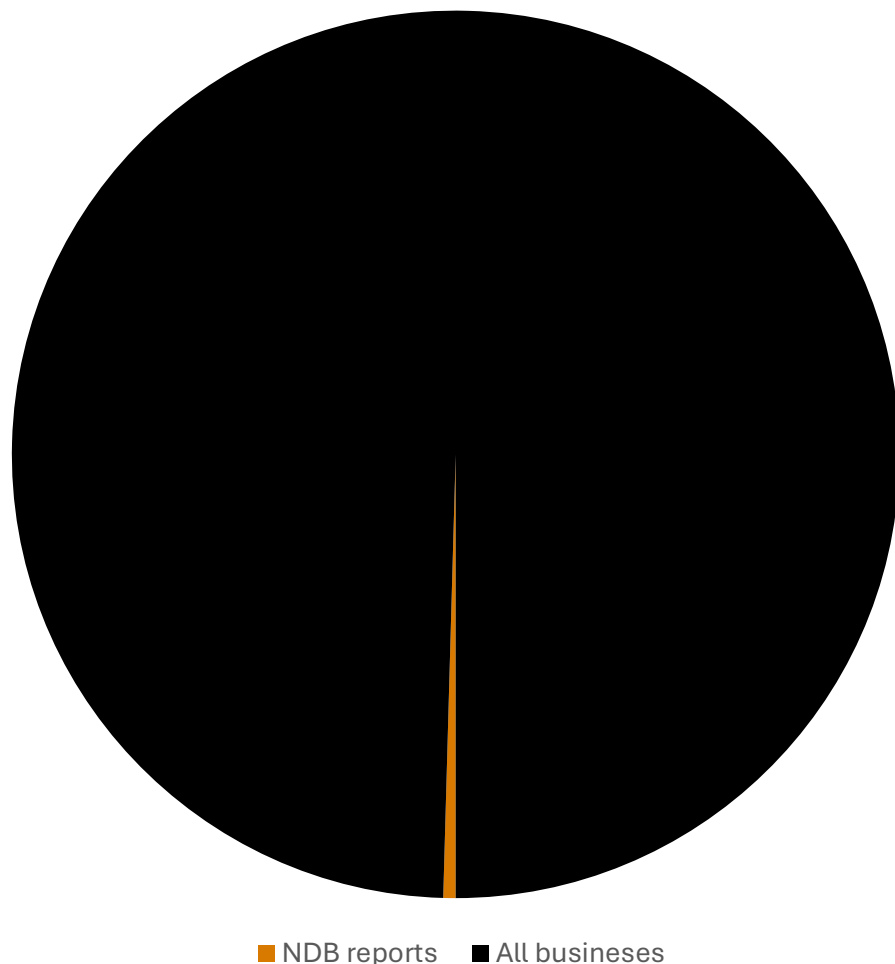


Chronic underreporting

We estimate that approximately 200,000 organisations are required to report notifiable data breaches to the OAIC. This includes any businesses in Australia with a turnover of \$3m or more, as well as any organisations that routinely collect sensitive data eg. hospitals, retailers, marketing agencies.¹

Yet an average of just 900 reports are submitted each year – a third of which come from the finance and healthcare sector alone.

We estimate that just 0.04% of large businesses submitted an NDB report to the OAIC last year. This figure feels incredibly low when you consider a recent survey that found that 41% of businesses experienced a breach in 2023.



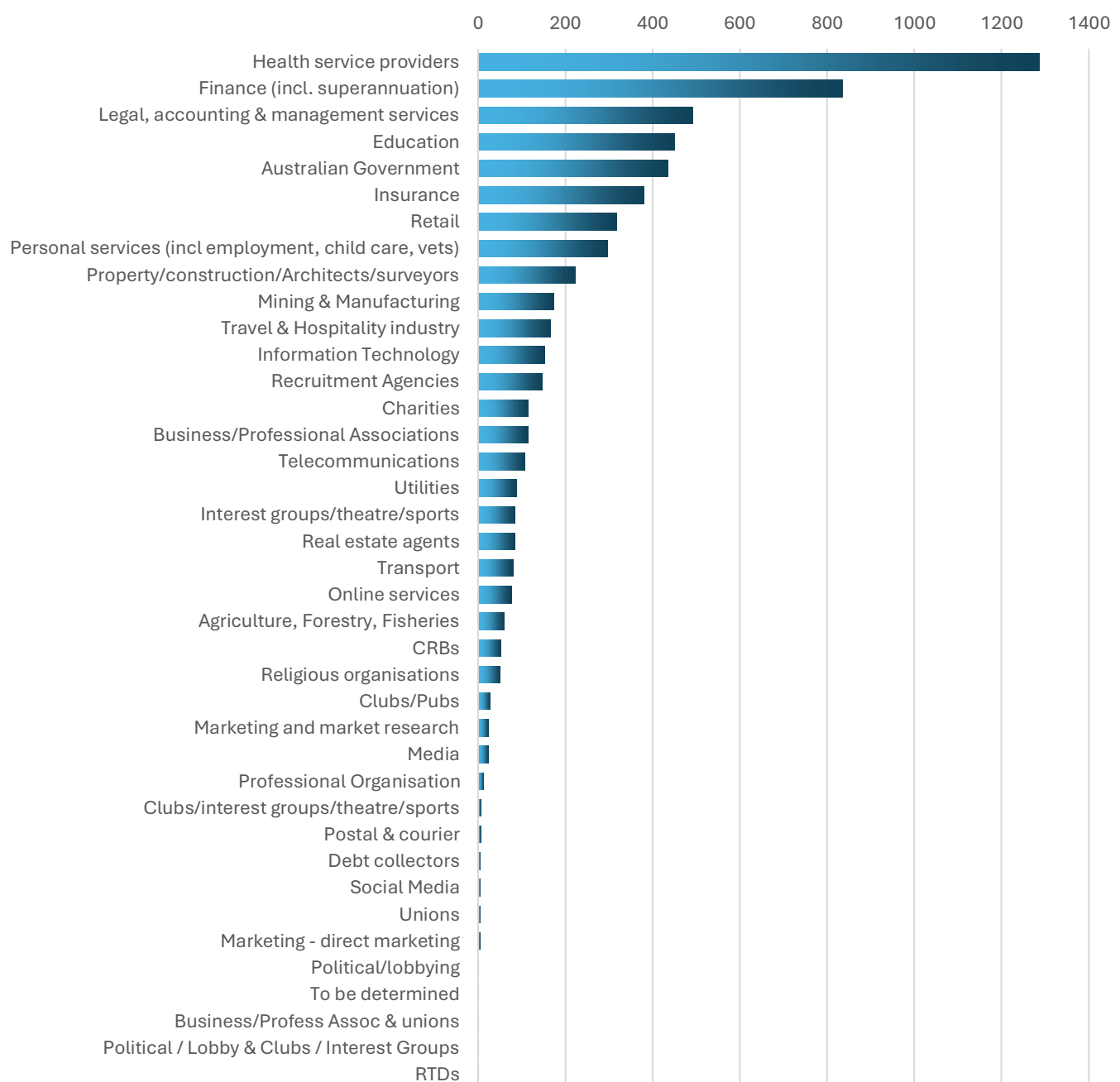
¹ There are 90,000 Australian businesses with a turnover of \$5m+ and 117,000 with a \$2m-\$5m turnover
<https://www.asbfeo.gov.au/small-business-data-portal/number-small-businesses-australia>

Industry breakdown

Industry by industry, a few interesting trends that emerge. There are more than 2,000 data breaches reported by healthcare and finance organisations combined, significantly more than any other sector, and nearly a third of all NDB reports since 2018.

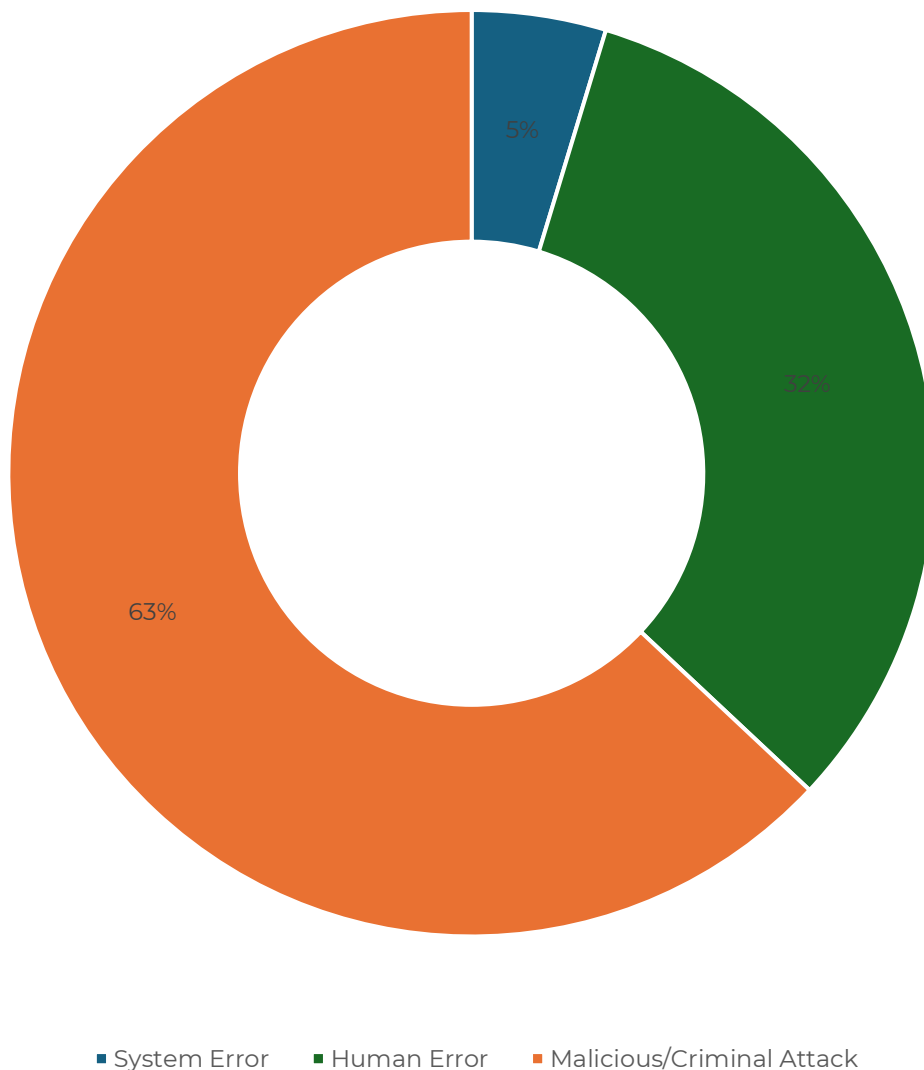
The big question is whether these industries are more frequently targeted, or more prone to breaches because they are insecure. Or, most likely, these heavily regulated industries are more inclined to submit NDB reports to the AOIC as part of their due diligence. I think it's safe to assume that there are hundreds, if not thousands of data breaches that should be reported to the AOIC in other industries but are not. For instance, it's hard to believe that, among every retailer in Australia that handles sensitive data (eg. payment and contact info), only 300 data breaches have occurred since 2018.

Notifications received 2018-2024



Among all cyber-attacks reported to the OAIC since 2018 that have resulted in a serious data breach, nearly two thirds (63%) were attributed to malicious / criminal attacks, rather than user or system error. Yet this fluctuates significantly by industry and year.

Breaches from 2018 - 2024

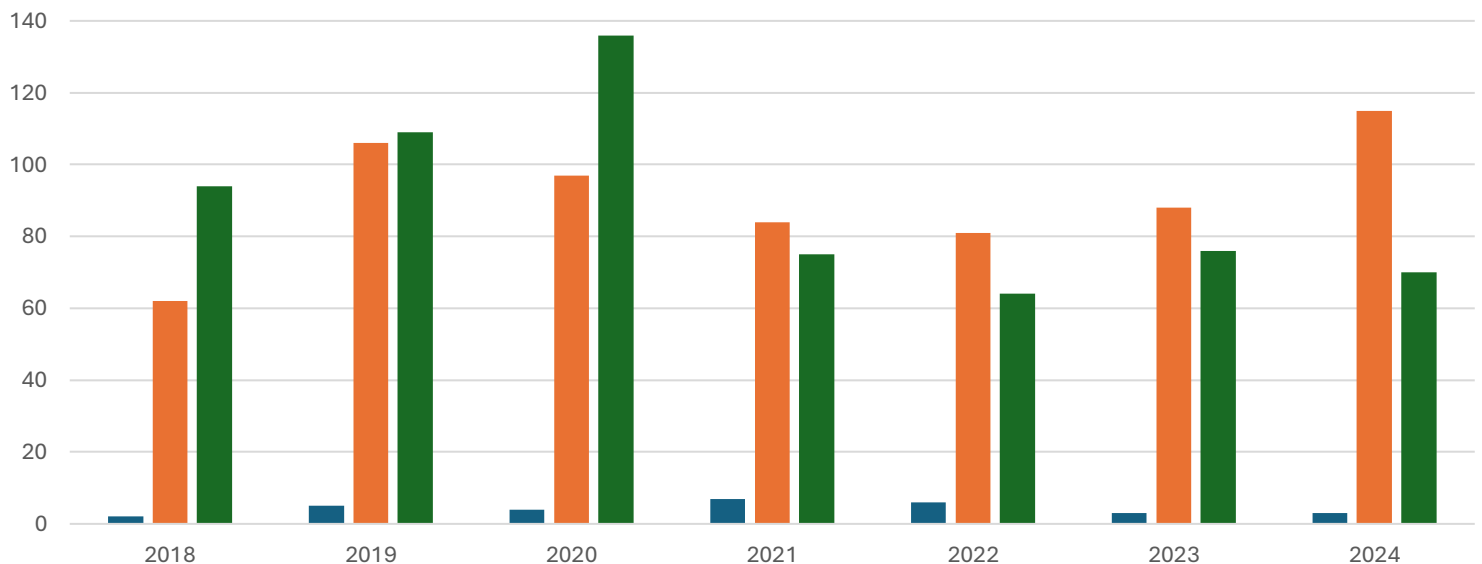


Humans, the weakest link in healthcare

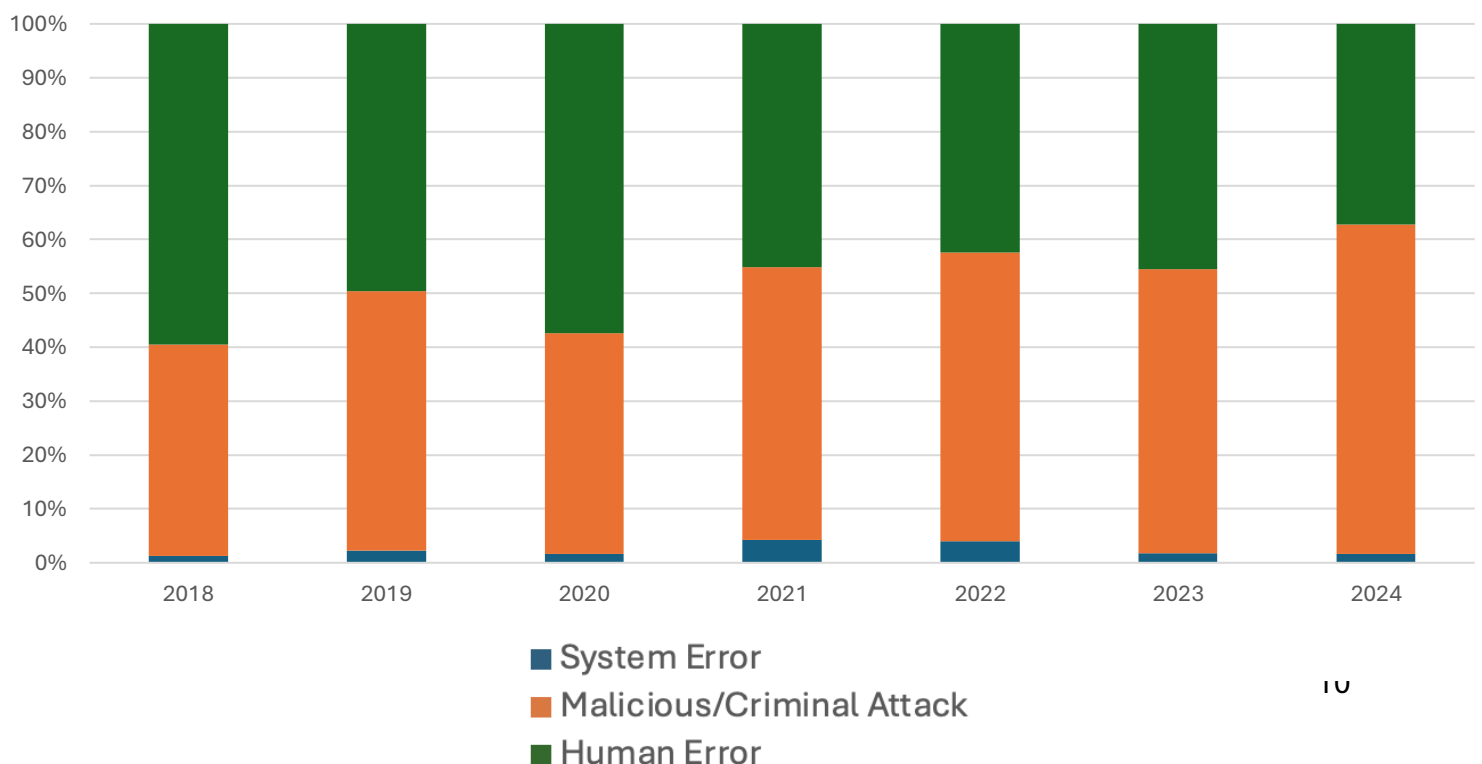
In healthcare, the most active sector for reports submitted to the OAIC, the cause of breach is much more likely to be user error (compared to the average of all NDB reports submitted by all industries). There was understandably a huge surge in user error related breaches in 2020 during the height of the COVID pandemic when hospitals were overrun.

There was a slight uptick in IT errors relating to breaches in 2021 and 2022 but, on the whole, a very small percentage of healthcare breaches are the result of tech. For security teams in healthcare, the focus must be on user education and implementing processes that mitigate common human mistakes.

Healthcare breaches (total reports)



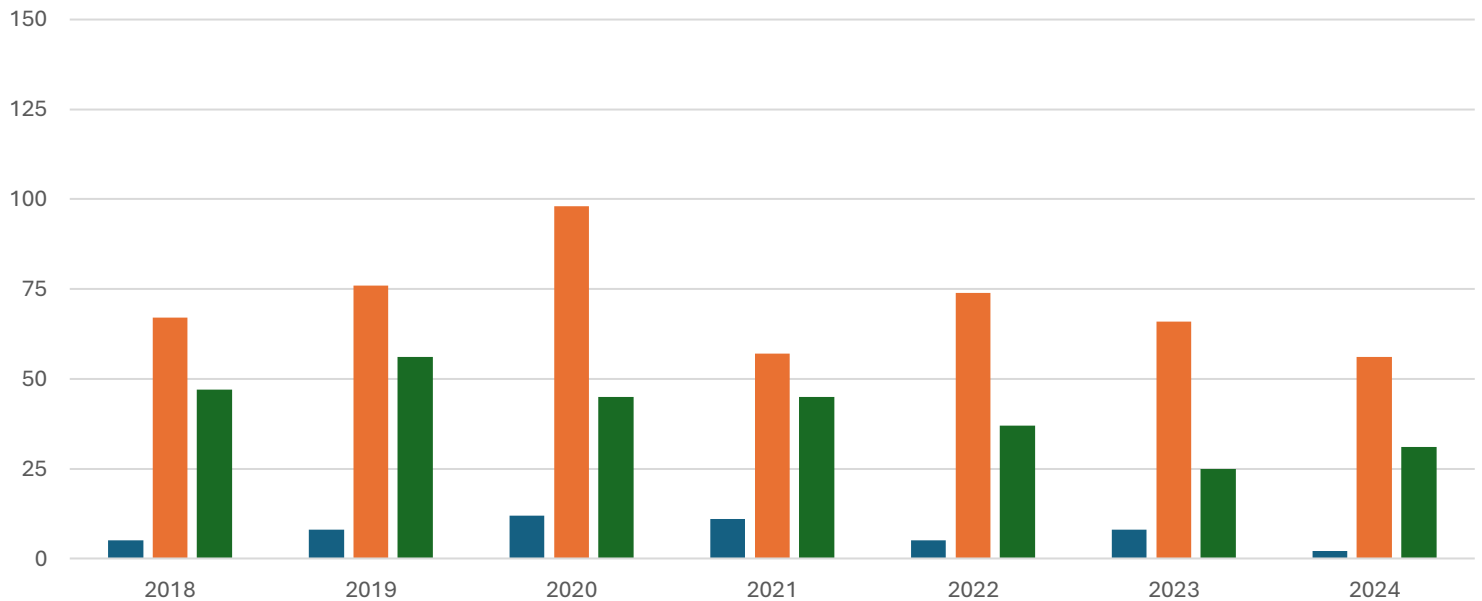
Healthcare breaches (percentage)



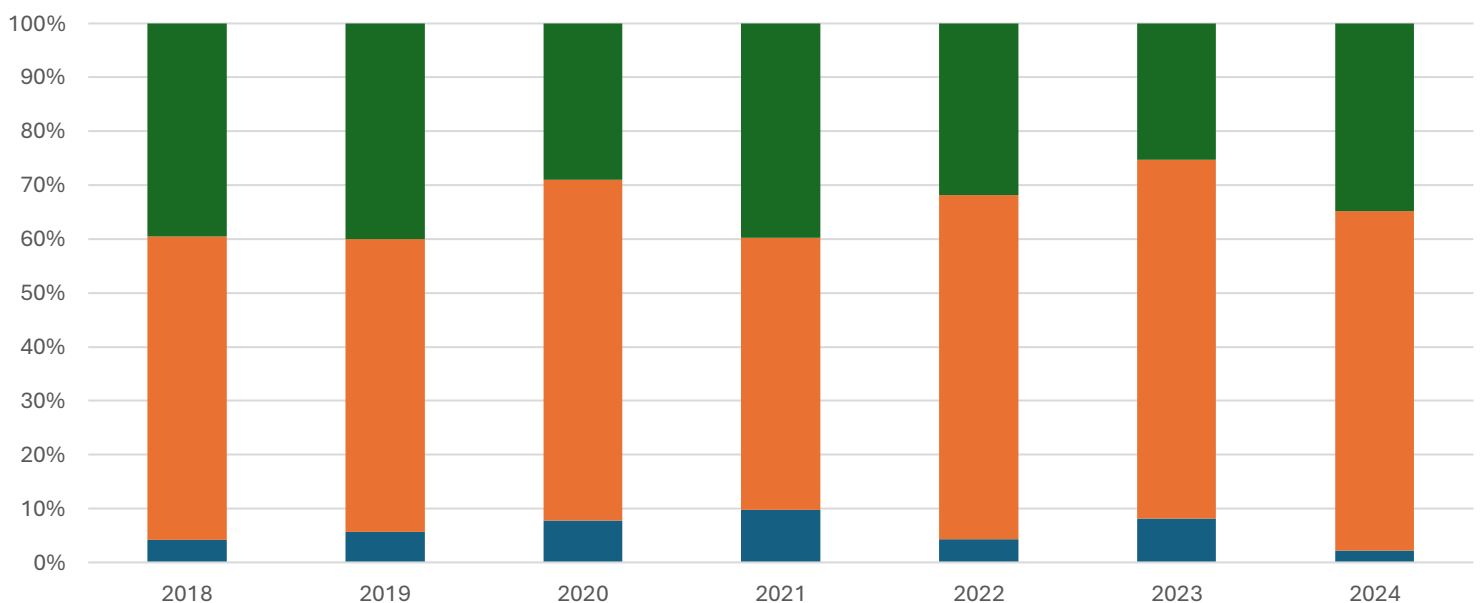
Finance and insurance are a top target for criminals

Finance is another heavily regulated industry that frequently reports breaches to the OAIC. It's notable how many breaches impacting finance and insurance companies are the result of criminal attack, because these institutions are such a lucrative target. Finance is also disproportionately impacted by IT and system errors. Across all industries, system errors only account for 5% of NDB reports. For the finance sector, this number is twice as high (10%) in 2021, and above average in other years too.

Finance (total breaches)



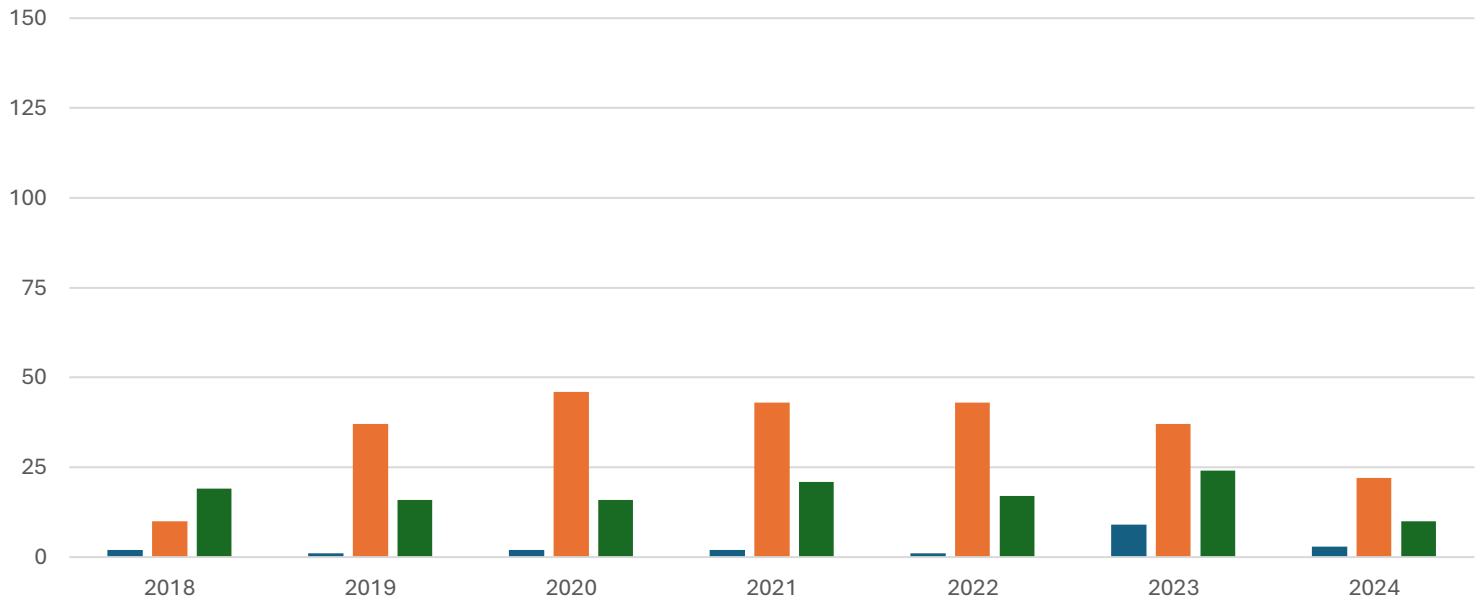
Finance breaches (percentage)



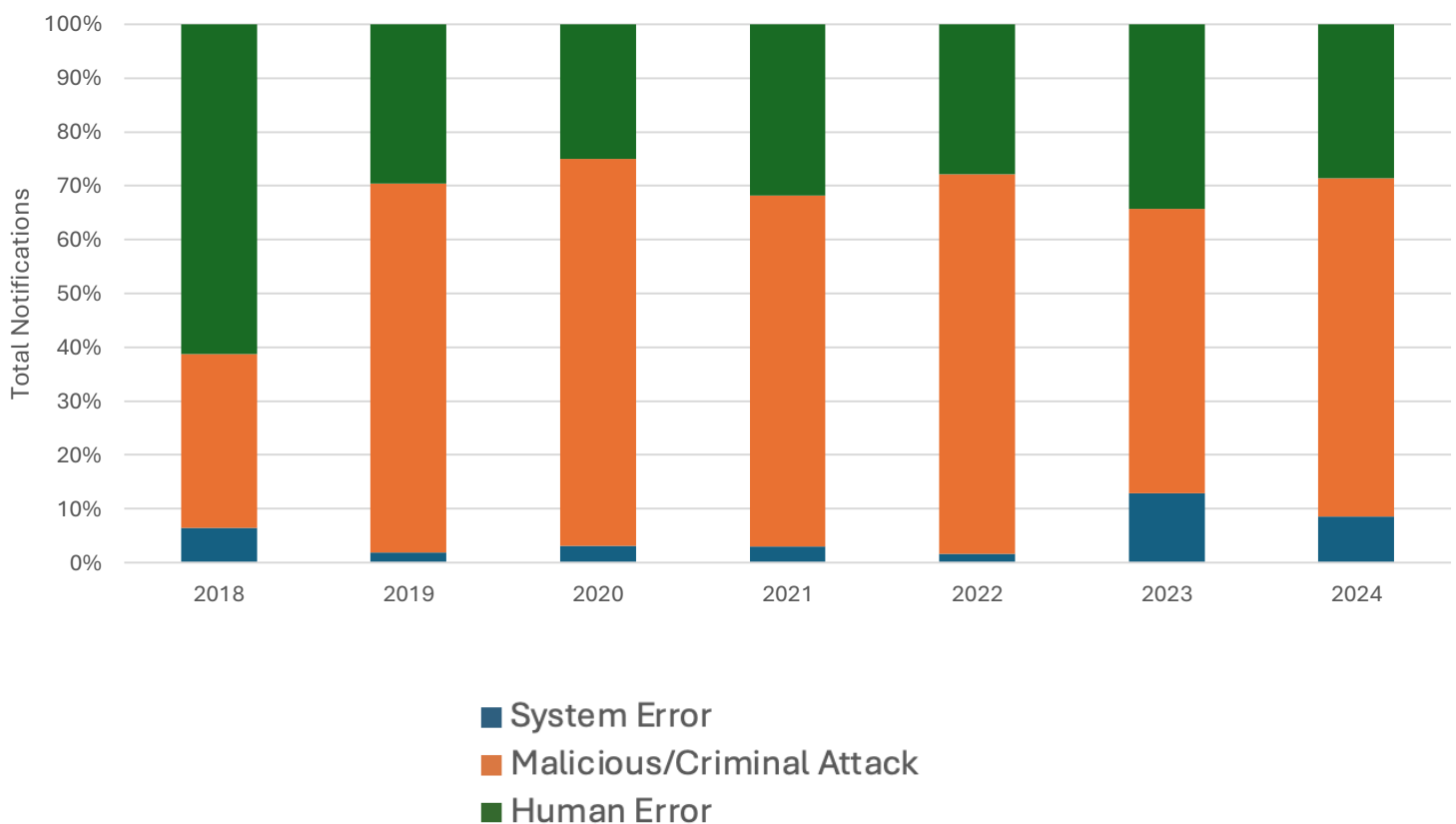
■ System Error
■ Malicious/Criminal Attack
■ Human Error

Insurance is extremely similar. It is dominated by cybercriminal / malicious attacks, but there are years where IT / System errors increase from one or two per year, up to 9. N.B insurance offers a smaller sample size than finance.

Insurance



Cyberattacks in the Insurance Sector

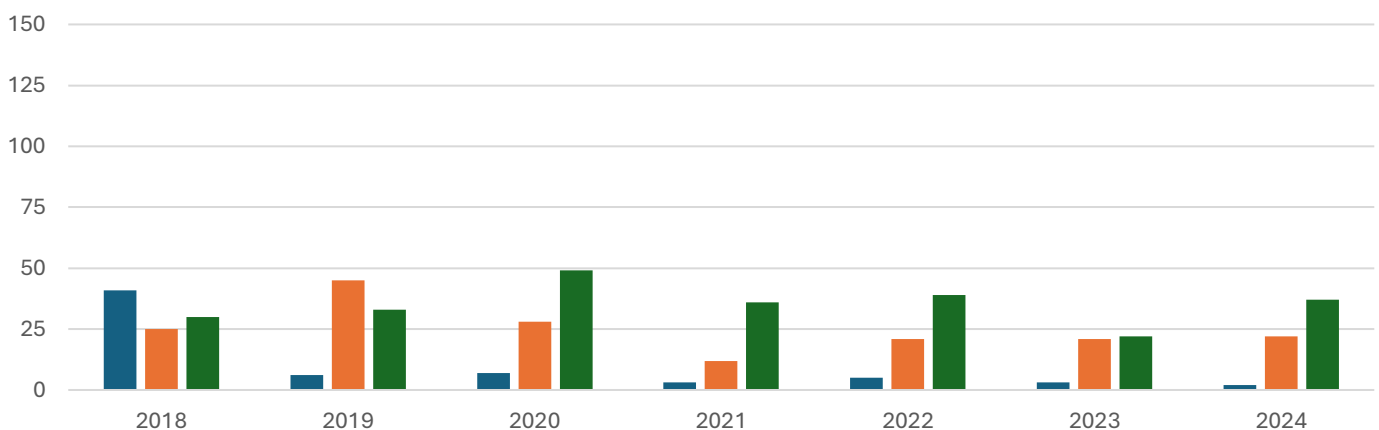


Education and the perils of supply chain risks

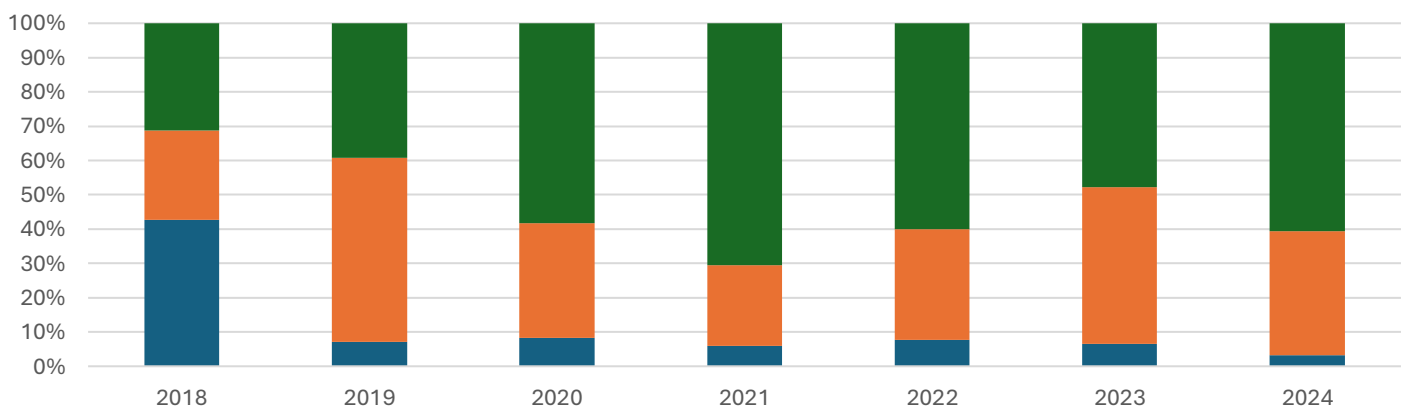
The source of data breach breakdown in the education sector is extremely similar to healthcare. It is dominated by user error, as the cause of 70% of breaches in a single year (2021) – more than double the national all industry average (32%). Another outlier is the huge surge in IT errors resulting data breaches in 2018. At 40%, this figure is 8x higher than the all industry average (5%). This is likely the result of the ProctorU breach that exposed email addresses from several universities in Australia, including the University of Sydney, the University of New South Wales, and the University of Melbourne. This underscores the urgent need for security teams to vet technology partners carefully and take extra steps to mitigate the impact of their vulnerabilities/breaches.

It is worth noting that data breaches impacting the education sector are in decline. In 2023, the last full year of available data, there were half as many data breaches caused by user error compared to 2020.

Education (total breaches)



Education (percentage of breaches)



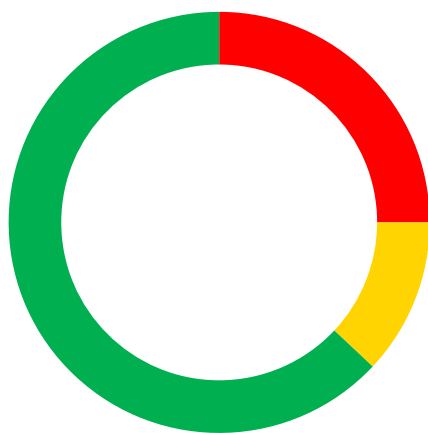
■ System Error
■ Malicious/Criminal Attack
■ Human Error

A spotlight on Government failings

Looking at all 6,000 NBD reports submitted since 2018, it's clear which industries are struggling most when responding to data breach incidents.

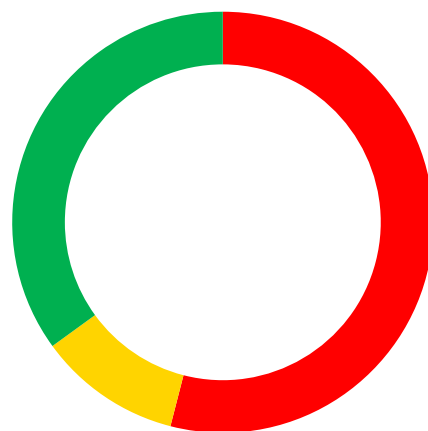
Across all industries, only 25% of data breaches are identified 30 days after an incident or later. This figure is significantly higher in the public sector. 53% of data breaches involving Government organisations went unidentified for 30 days or longer.

All reports all industries



■ Late identification
■ Average identification
■ Early identification

All Government reports

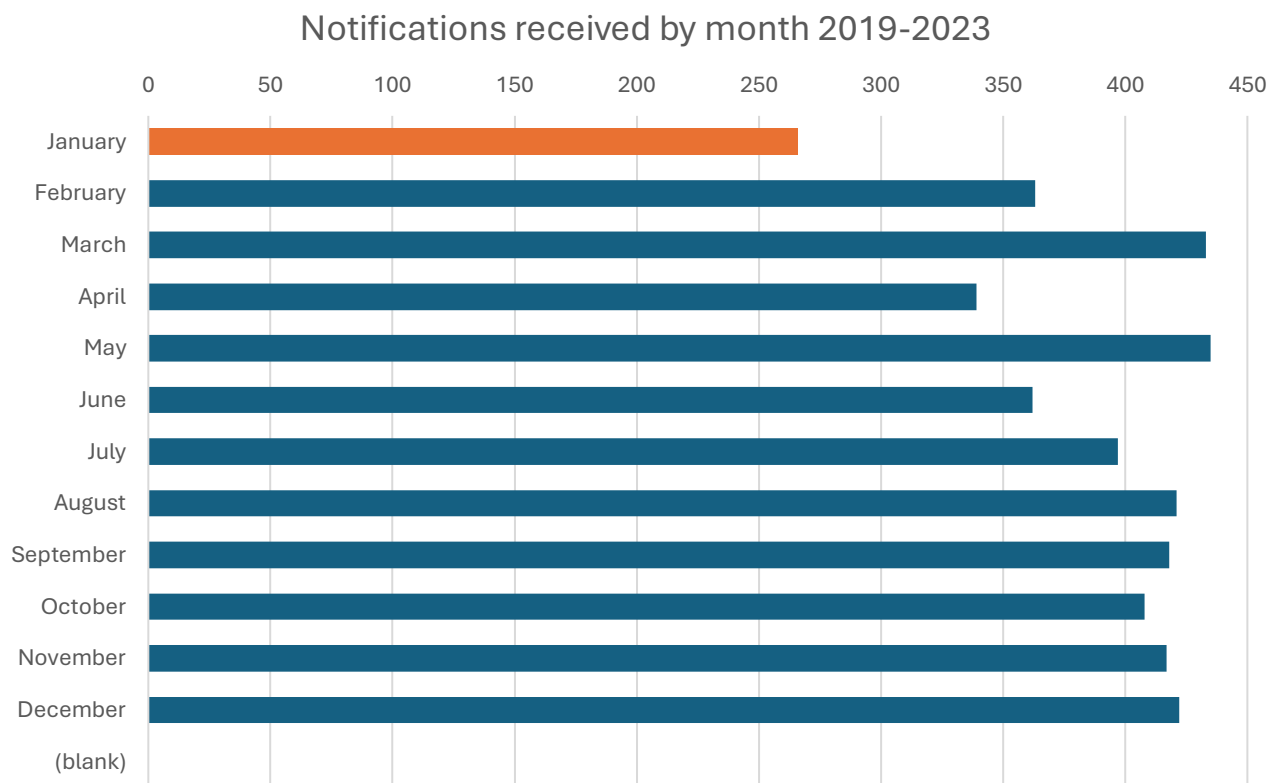


■ Late identification
■ Average identification
■ Early identification

Indeed, all three of the ACT Government's NBD reports submitted since 2018 have been identified late.

Fewer breaches in January

A slump in data breaches reported to the OAIC during the Australian summer months is an interesting quirk in the data. Breaches are down by a third in January, and remain lower than average in February.



This may sound counter-intuitive for security teams, who regard the summer break as among their busiest periods.

A worrying but highly likely possibility is that cybercrime does not reduce in the summer, but businesses are simply missing data breaches. Breaches may be underreported in the summer because they are simply not discovered. When organisations and members of their security teams go on holiday, they are understaffed and under resourced. As a result, they identify fewer breaches.

Businesses must not be complacent during summer, and should carefully consider their security resources and staffing during the summer months.

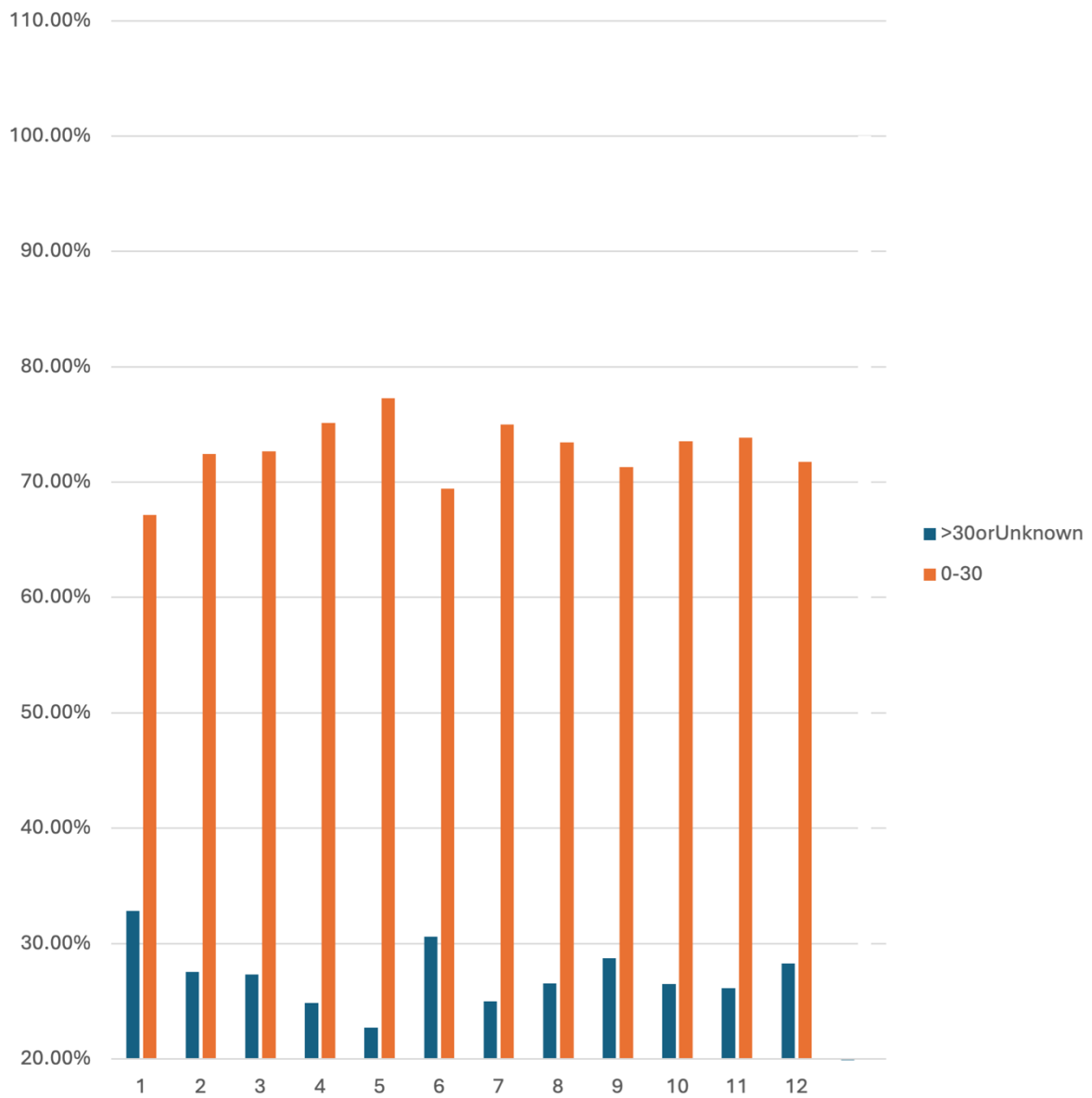
The idea that Australian security teams are under-resourced in the summer months is underscored by data breach reporting times.

After a data breach is identified, the OAIC allows 30 days to assess whether it could cause harm, and if an NDB report needs to be filed. Yet many reports (27%) are submitted late.

January is the slowest month for reporting breaches, with more than 32% of breaches being reported to the OAIC more than 30 days after they occur.

Once again, this could be a staffing issue. The IT or security personnel tasked with assessing whether a breach warrants an NDB report may be away, the process may be pushed back, or missed entirely.

Breaches reported after 30 days or more



Conclusion

“It’s a sobering thought that every data breach report filed to the OAIC is from a large, tightly regulated and seemingly highly functioning business. Most would have been compliant with their industry standards, would have budgeted for good security, and probably thought themselves secure. But it’s an important reminder that compliant does not equal secure. Good security is an ongoing process that cannot be fixed through single point in time compliance checks.

“Mega data breaches have become the norm in Australia, because attackers are routinely breaching companies of every size across every industry. There’s no such thing as too big to fail in the security landscape.

“Security always comes down to having adequate resources and applying the right technology and processes in the right areas. Big businesses and small businesses alike can fall victim to a breach if employees are not properly educated, or the company fails to enact effective credential policies.

“99.9% of Australian businesses do not have the skills and resources to run a Security Operations Centre in house. Instead, they must find a trusted security partner to ensure they can mitigate and identify breaches to limit the potential impact of cybercriminal attacks. Likewise, if the worst should happen, a good security partner can help businesses report breaches in time and in detail to the OAIC. This can save them from heavy fines and reputational damage among customers/partners.”



About us

Started almost 2 decades ago in Sydney in 2006, we began delivering a number of security programs of work including a large PCI DSS program for Energy Australia and since then, have grown to one of Australia's most trusted and respected Cyber Security firms.

In 2020, we became a member of the NSW Government Cybersecurity Taskforce. We are also a member of the Australian Cyber Security Centre.

Today, we service over 100 mid-tier and ASX-listed companies, providing them with comprehensive cyber security solutions tailored to their individual needs.



Corporate Office - Australia
C/o Macquarie DeepTech
Incubator
Level 1, 3 Innovation Road
Macquarie University, NSW,
2109



Our Services

StickmanCyber As A Service
Governance, Risk and Compliance
Virtual CISO
Threat Monitoring, Detection and Response
Proactive Cybersecurity

Quick Links

Start an Assessment
Blogs
Webinars
About StickmanCyber
Terms of use
Privacy Policy

Contact

☎ 1800 785 626
✉ sales@stickmancyber.com
✉ media@stickmancyber.com
✉ hr@stickmancyber.com

