Optus 2022 Cyber Breach

Benjamin Janssens

Independent Researcher

**Executive Summary**

Intellithreat

This report addresses the data breach made public by Optus on Thursday, 22 September 2022. I have found a theme that Optus seems to be at fault due to negligence of data handling and accessibility. The Australian Broadcasting Centre (ABC) stated that “A senior figure inside Optus”[[1]](#endnote-1) revealed an unsecured API was the cause of the breach.(Greene, 2022) This breach was on an enormous scale effecting 9.8 million Australians initially,[[2]](#endnote-2)(APRA, 2022) over one in three of the population and this number is expected to be higher.

This left authorities scrambling on how to respond, Optus suggested key financial institutions Moneysmart.com and OAIC.com to help monitor identity fraud.[[3]](#endnote-3)(Optus, 2022) Optus is appointing professional services firm Deloitte to conduct an independent external review of the recent cyberattack. The findings of this report have not yet been made publicly available.[[4]](#endnote-4)(Optus, 2022) The Office of the Australian Information Commissioner (OAIC) and The Australian Communications and Media Authority (ACMA) conducted a joint investigation into whether Optus had been negligent in its practices, the finding of this investigation haven’t been made public yet.[[5]](#endnote-5)(OAIC, 2022)

The OAIC has created a framework in accordance with the Privacy act 1998, stating the best practices for an organization to adopt after a data breach. This can be found on their website.[[6]](#endnote-6)(OAIC, 2019) Treating sensitive data as a vulnerability opposed to an asset was a key takeaway by Commissioner Angelene Falk. (ABC, 2023) This seems to be a reoccurring message being made by leading security experts. A global survey conducted in 2023 by PwC found” Consumers are acting on their concerns. Half said they don’t share any more personal data than necessary (49%), and 32% opt out of receiving emails”[[7]](#endnote-7)(PwC, 2023)

**Introduction**

This research paper will outline the findings and recommendations made in relevance to the 2022 Optus Cyber Attack. This report aims to use exclusively Primary sources that are backed up by quantitative and qualitative data, with the exception of one anonymous source.

This report will highlight the approach Optus had to dealing with the breach and how the government assisted in this. This report aims to outline the response the government had and the implications they are taking in arise to modern complications around data management and protection, and what this might look like.

**Investigations / Methodology**

Correlational Research will be used in accordance with Intellithreats research policy. Qualitative data has been collected from a variety of primary sources such as Optus and the ACMA. This data has been cross referenced with any available resources from other government agencies. Quantitative data has been looked at from the same sources and a marketing survey. Opinion based statements and statements without sources have been avoided. Documentation has been stored appropriately and is accessible to Intellithreat intranet as per company policy.

**Findings**

Optus has shown an inherent lack of cyber security awareness. Displayed by the sheer size of the hack, that is, the amount of data that moved through the network undetected, and the methods the hacker used has been scrutinized by the cyber security Minister, the Australian Federal Police (AFP) and the ABC to name a few.[[8]](#endnote-8)(ABC, 2022) The Disproportionate figures show that nearly 10 million Optus customers lost their ID documents while many of those individuals are not active Optus Customers. The Telecommunications (Interception and Access) Act 1979 requires telecommunications companies to retain a required set of telecommunications data for at least 2 years[[9]](#endnote-9),(Dept. of Home Affairs, 2023) Optus claims that they are bound to hold this information for 6 years**[[10]](#endnote-10)**(Bogle, 2022). this is a strong indication into why so many former customers were affected. What they failed to mention is the Australian Transaction Reports and Analysis Centre(AUSTRACK) requires businesses to adhere to Know Your Customer (KYC) procedures, which states “As a reporting entity you must apply customer identification procedures to all your customers”.[[11]](#endnote-11)(AUSTRAC, 2022) This gives AUSTRACK a database to help investigations into money laundering or terrorism. Forms of Identification such as: Name, address and transactional records should be adequate, there is no need to store information such as birth certificates, passports and drivers licenses outside of the telecoms act (1979).

Data breaches are becoming more apparent, Commissioner Angelene Falk stated “The stark figures track the period between July and December 2022 and reveal a 67 per cent rise in the number of attacks from the first half of the year, which only saw 24 large-scale attacks compared to 40 in the back half.”[[12]](#endnote-12)(Tran, 2023) While there is no indefinite answer to these statistics, re occurring reports of insufficient security measures around data that isn’t necessary to retain, seems to be a common theme. PwC, a financial institution with over 300,000 staff, conducted a global market survey which discovered “Consumers are acting on their concerns. Half said they don’t share any more personal data than necessary (49%), and 32% opt out of receiving emails”[[13]](#endnote-13)(PwC, 2023). This personally resonates with me, and I am less inclined to use a service such as an app required to sign into a jobsite, or signing up to a store membership. Companies seem to think it’s acceptable to ask for personal information from customers in exchange for receiving a service. This practice is something that companies need to determine what is crucial information and what is not necessary.

Optus has claimed they were victims of a sophisticated hack that could have happened to any major company. The ABC refuted stating that *“A senior figure inside Optus”[[14]](#endnote-14)* who was acting anonymously, revealed an unsecured API was the cause of the breach. The *senior figure* said “"It's still under investigation. However, this breach, like most, appears to come down to human error," the Optus insider told the ABC. "They wanted to make integrating systems easier, to satisfy two-factor authentication regulations from the industry watchdog, the Australian Communications and Media Authority (ACMA). The process allegedly involved opening up the Optus customer identity database to other systems via what's known as an Application Programming Interface, with the assumption that the API would only be used by authorised company systems. "Eventually one of the networks it was exposed to was a test network which happened to have internet access." It's claimed this allowed access to the Optus network from outside the company.”” (Greene, 2022)[[15]](#endnote-15)

Although Optus has denied these claims and said it was a sophisticated hack, SQL injections and API entry points are a reoccurring precursor to companies reporting data breaches. These methods of attacking companies by compromising the development side of business often proves successful for threat actors as a work environment may make staff feel there is a segregation between an end product that needs protecting and the skeleton that is built up to arrive at that end product. While the password to gain initial access to the intranet may be difficult, companies, more specifically, individuals, opt for the quicker more efficient option of a weaker password for checkpoints inside the network that is easy to remember. This exponentially hinders security effectiveness and allows threat actors to “easily walk around the building” once they get in the front door.

Deloitte was employed by Optus to commence a third-party audit of their security policies and if they had breached any legislation.[[16]](#endnote-16)(Optus, 2022) This was an attempt by Optus to seem transparent in doing what they could to be accountable. The findings of this report have not yet been made public. They suggested in the interim that customers seek the services of companies like moneysmart.com and OAIC.com to help them monitor Fraudulent use of their credentials.[[17]](#endnote-17)(Optus, 2022)

OAIC and the ACMA commenced a joint investigation into whether Optus has been negligent in their data handling and what steps could be taken to mitigate this in the future[[18]](#endnote-18).(OAIC, 2022) This report is yet to be released. The OAIC recommends all businesses refer to its data breach preparation and response guidelines when navigating through a cyber crisis[[19]](#endnote-19).(OAIC, 2022)

The ACMA stated “The Department of Home Affairs has established a Commonwealth Credential Protection Register to help stop compromised identities from being used fraudulently.”(ACMA, 2022) a register would prevent compromised identity credentials from being fraudulently used by diverting all credentials through the Document Verification Service. “The Document Verification Service is used by government agencies and businesses, such as banks, to verify an individual’s identity online. This will prevent credentials that are included on the register from being used fraudulently. However, this means rightful owners will not be able to use them online. New credentials issued following the data breach will work as normal.”[[20]](#endnote-20) (ACMA, 2022)

I believe this approach the government had is what is necessary in today’s day and age. An agency with the power to freeze Australian issued identification when it has been flagged as stolen and then work with big enterprises to establish a form of framework to implement this permanently. This would eliminate the ability for threat actors outside of Australia to use these documents without going to a physical Australian location. Whilst I believe Government shouldn’t intervene in supporting businesses, as businesses don’t share profits when they are successful, I do believe this form of protection for Australian citizens is in the governments best interests.

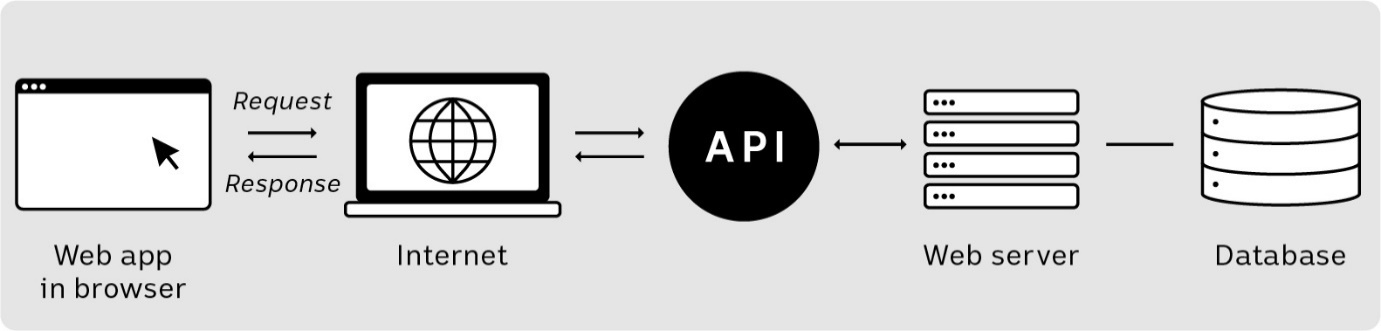
**Conclusions**

Data security and retention is a tricky issue. Meta data is viewed as an asset to companies as they can tailor products to fit your needs. It gives companies an advantage because they already have an idea of who you are, and this saves the business time in meeting your needs. Optus stored this data in accordance too standard industry telecomm policy, which isn’t as tight as it could be, but they failed to protect the avenues that were open and gave access to these files, which is inherently difficult as it is ever evolving with technology. The Telecommunications Act 1979 requires telecommunications companies to retain a particular set of telecommunications data for at least 2 years, Companies should adjust their security and privacy policies to ensure that any sensitive information is deleted after this threshold. The ACMA and OAIC stepped up to the issue swiftly by creating a temporary register to store stolen credentials and deny access to the documents until new documents are verified. Although this temporarily meant victims couldn’t use their ID online until steps had been taken to verify their identity. I think a centralized service should be developed and be accessible to citizens and businesses to better manage these circumstances. The Australian Cyber Security Centre could work with The Australian Competition and Consumer Commission to help develop these frameworks.

**Recommendations**

My recommendations would be for companies to update security policies and guidelines to ensure nothing but absolute essential data is retained and everything else is safely disposed of. The access to networks and databases containing this critical data should be heavily regulated and calculated prior to adaptation. No single network should have administration like privileges that are accessible via WAN connections, They should be exclusively zero trust networks that have access to these kinds of documents. The amendments made to Telecommunications Regulations 2021 and the register the department of home affairs created is the direction the industry needs to head in. Government shopfronts such as The Road Transport Authority could have a service that allows Identification and stolen credentials to be put on pause when a citizen discovers they have been misused.

**Attachments**



 Application Programming Interfaces enable different applications to talk to each other.(ABC News: Emma Machan) - <https://www.abc.net.au/news/2022-09-23/optus-rejects-claim-hack-likely-result-of-human-error/101468846> (Machan. 2022)

**References**

1. <https://www.abc.net.au/news/2022-09-23/optus-rejects-claim-hack-likely-result-of-human-error/101468846> (Greene. AG. 2022. Optus rejects insider claims of 'human error' as possible factor in hack affecting millions of Australians: ABC) [↑](#endnote-ref-1)
2. <https://www.apra.gov.au/news-and-publications/optus-data-breach-an-update-for-apra-regulated-entities> (APRA. 2022. Optus data breach: an update for APRA regulated entities: APRA) [↑](#endnote-ref-2)
3. [**https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack**](https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack)(Optus. 2022. Optus notifies customers of cyberattack compromising customer information: Optus) [↑](#endnote-ref-3)
4. <https://www.optus.com.au/about/media-centre/media-releases/2022/10/optus-commissions-independent-external-review-of-cyberattack> (Optus. 2022. Optus commissions independent external review of cyberattack: Optus) [↑](#endnote-ref-4)
5. <https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-optus-over-data-breach> (OAIC. 2022. OAIC opens investigation into Optus over data breach: OAIC) [↑](#endnote-ref-5)
6. <https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/preventing-preparing-for-and-responding-to-data-breaches/data-breach-preparation-and-response> (OAIC. 2019. Data breach preparation and response: OAIC) [↑](#endnote-ref-6)
7. [Global Consumer Insights Survey 2023: Frictionless retail and other new shopping trends | PwC](https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey-feb-2023.html)(PwC. 2023. February 2023 Global Consumer Insights Pulse Survey: Consumers seek frictionless experiences in a world of disruptions: PwC) [↑](#endnote-ref-7)
8. <https://www.abc.net.au/news/2022-09-26/home-affairs-minister-blames-optus-for-cyber-attack-hack/101474636> (Evans. JE. 2022. Home Affairs Minister Clare O'Neil says Optus ‘left the window open’ for cyber criminals to conduct simple hack: ABC) [↑](#endnote-ref-8)
9. <https://www.homeaffairs.gov.au/about-us/our-portfolios/national-security/lawful-access-telecommunications/data-retention-obligations> (Depart of Home Affairs. 2023. Data retention obligations: Depart of Home Affairs) [↑](#endnote-ref-9)
10. <https://www.abc.net.au/news/science/2022-10-02/why-is-optus-keeping-customer-data-for-so-long/101491200> (Bogle. AB. 2022. Past Optus customers have had their data exposed — why did the company still have it?: ABC) [↑](#endnote-ref-10)
11. <https://www.austrac.gov.au/business/core-guidance/customer-identification-and-verification/customer-identification-know-your-customer-kyc> (AUSTRAC. 2022. Customer identification: Know your customer (KYC): AUSTRAC) [↑](#endnote-ref-11)
12. <https://www.abc.net.au/news/2023-03-01/data-breaches-revealed-by-australian-information-commissioner/102039710> (Tran. DT. 2023. Data breaches affecting millions of Australians are on the rise, Information Commissioner says: ABC) [↑](#endnote-ref-12)
13. [Global Consumer Insights Survey 2023: Frictionless retail and other new shopping trends | PwC](https://www.pwc.com/gx/en/industries/consumer-markets/consumer-insights-survey-feb-2023.html) (PwC. 2023. February 2023 Global Consumer Insights Pulse Survey: Consumers seek frictionless experiences in a world of disruptions: PwC) [↑](#endnote-ref-13)
14. <https://www.abc.net.au/news/2022-09-23/optus-rejects-claim-hack-likely-result-of-human-error/101468846> (Greene. AG. 2022. Optus rejects insider claims of 'human error' as possible factor in hack affecting millions of Australians: ABC) [↑](#endnote-ref-14)
15. <https://www.abc.net.au/news/2022-09-23/optus-rejects-claim-hack-likely-result-of-human-error/101468846> (Greene. AG. 2022. Optus rejects insider claims of 'human error' as possible factor in hack affecting millions of Australians: ABC) [↑](#endnote-ref-15)
16. <https://www.optus.com.au/about/media-centre/media-releases/2022/10/optus-commissions-independent-external-review-of-cyberattack> (Optus. 2022. Optus commissions independent external review of cyberattack: Optus) [↑](#endnote-ref-16)
17. <https://www.optus.com.au/about/media-centre/media-releases/2022/09/optus-notifies-customers-of-cyberattack> (Optus. 2022. Optus notifies customers of cyberattack compromising customer information: Optus) [↑](#endnote-ref-17)
18. <https://www.oaic.gov.au/newsroom/oaic-opens-investigation-into-optus-over-data-breach> (OAIC. 2022. OAIC opens investigation into Optus over data breach: OAIC) [↑](#endnote-ref-18)
19. <https://www.oaic.gov.au/newsroom/advice-on-optus-data-breach> (OAIC. 2022. Advice on Optus data breach: OAIC) [↑](#endnote-ref-19)
20. <https://www.acma.gov.au/optus-data-breach> (ACMA. 2023. Optus data breach: ACMA) [↑](#endnote-ref-20)