OPTUS 2022 CYBER ATTACK: SHINING A LIGHT ON THE INEVITABLE

What businesses need to know about the Optus 2022 cyber attack and lessons learned from the Service NSW 2020 Data Breach

By Michael Trovato, GAICD, MAISA, CISA, CISM, CDSPE;

Eugenia Caralt, MAISA, CISA, AFBCI; David Zhu, MAISA

October 2022

Cyber attacks are an imminent threat for all organisations

Vulnerable organisations

The Optus cyber attack in September 2022 [1] has once again displayed the vulnerability of Australian organisations to malicious actors and the dire consequences of: (i) privacy and data protection risks and issues; and (ii) insufficient legislative and regulatory frameworks.

Australian companies have been increasingly affected by cyber attacks in recent years, with a host of criminal actors targeting organisations that hold substantial amounts of personal information (PI).

The OAIC reported 464 notifiable data breaches from July–December 2021, an increase of 6% from the previous 6-month period [2]. The average cost of a data breach increased 2.6% from USD 4.24 million in 2021 to USD 4.35 million in 2022, totalling a 12.7% increase since 2020 [3].

There has also been a 15% increase in ransomware reported by the Australian Cyber Security Centre (ACSC) in FY21, including 500 reports of ransomware and a 47% increase of ransomware globally in July 2022 compared to June 2022 [4]. 23% of the Australian notifiable data breaches which resulted from cyber incidents were due to ransomware [4].

Many data breaches are occurring in the context of wider disruptions caused by COVID-19. As large portions of the professional workforce transitioned to work remotely, there has been a significant reliance on the use of personal devices and home networks to conduct work tasks, thereby increasing the security vulnerability for organisations.

Digital transformations and growing interconnectivity have also made many organisations financially valuable cyber targets.

The bad, the ugly, and the consequences

The Optus cyber attack has brought privacy and data protection concerns to the forefront after more than 2.1 million past and present Optus customers had their identification (ID) documents compromised, including driver licences, passports, and Medicare cards. [1]. Another 7.7 million customers did not have ID documents compromised but the attack still exposed information such as their name, email address, date of birth and phone number [1].

The significant number of affected individuals and sensitivity of the information involved means that Optus is dealing with a truly national personal information management disaster. The exposure of driver licences, passports, and Medicare cards is particularly concerning as it leaves individuals vulnerable to identity theft, which can cause serious psychological, emotional, financial, and reputational harm.

While the full extent of implications from the breach are still unclear for Optus customers and employees, one thing is for certain: Optus faces a highly damaged reputation, increased privacy and regulatory scrutiny, and costly lawsuits. Two major law firms, Slater & Gordon, and Maurice Blackburn, are already investigating a possible class action against Optus to seek compensation for people affected by the breach [5].

Reforms to privacy and security legislative frameworks are being implemented

Impactful regulatory action

Australia's privacy and security regimes have been in a state of flux and this is likely to continue. The Optus data breach has now triggered calls for regulatory reform to privacy and cyber security laws. Home Affairs Minister Clare O'Neil declared that the previous Coalition Government's recently passed cyber security reforms were 'absolutely useless' in relation to the Optus incident [6]. Attorney-General Mark Dreyfus also expressed that he was looking to reform privacy laws by the end of the year in response to the Optus incident [6].

Based on the Home Affairs Minister's recent statements, there will likely be a push towards greater regulatory scrutiny and harsher punishments for offending companies in a move that would align Australia more closely with the European Union's General Data Protection Regulation [7].

This comes amid ongoing reviews of the *Security of Critical Infrastructure Act 2018* (Cth) (SOCI Act), *Privacy Act 1988* (Cth) (Privacy Act), *Corporations Act 2001* (Cth) and Australian Consumer Law.

Given the yet-to-be-realised outcomes of the Optus data breach, key questions have arisen around how organisations should handle these types of situations. In many ways, the Optus incident draws parallels with the Service NSW (SNSW) data breach from March 2020. By looking at the SNSW data breach and its lessons learned, Optus and all other organisations can learn from its response. IIS assessed and advised the NSW Department of Customer Service (DCS) on SNSW's response and recovery, publishing a Post Incident Data Breach Report [8].

The Service NSW 2020 Data Breach: a valuable case study

About the breach

In March 2020, SNSW was the victim of a criminal cyber attack. Upon investigation, it was determined that 47 SNSW staff email accounts were compromised, and 730 GB of data was exfiltrated, comprising 3.8 million documents that relate to up to 186,000 customers.

The types of personal information compromised included sensitive data such as driver licences, birth certificates, passports, police checks, bank accounts, names, and email addresses which have the potential to result in significant customer impacts.

For staff or former staff, the types of personal information also included information gathered during recruitment and onboarding, including many cases their personal particulars and Tax File Number (TFN) as well as sensitive employment related items such as disciplinary and health matters.

IIS' overall opinion

At the outset, DCS/SNSW found itself in a position of adversity, with their resilience severely tested through a series of external crisis events while going through re-organisation as part of the 2019 Machinery of Government changes. Despite these challenges, DCS/SNSW responded in a way that demonstrated many attributes of a customer-focused and resilient organisation.

The mobilisation of resources and scale-up of front desk teams ensured that customer service levels were not impacted. However, IIS observed that the incident resulted in 'disruption' as internal initiatives across the DCS cluster had to be postponed. In focusing so strongly for many years on excellent customer service outcomes, SNSW was slow to address cyber vulnerabilities highlighted by the Essential Eight Strategies Audit in December 2018 and IT General Controls Audit in August 2019.

Nevertheless, SNSW mounted a significant effort to respond and recover from the data breach, by remediating the pre-exiting vulnerabilities while adapting to the challenges facing the organisation and incorporating lessons learned via other external crises such as floods, bushfires and COVID-19.

The Service NSW data breach: lessons learned

Key findings

Our key findings were:

Readiness: DCS/SNSW was not able to resist disruption to the business:

1. **DCS/SNSW was underprepared to respond** due to weaknesses across technology, processes and people and the lack of a pre-agreed and rehearsed incident assessment and response approach. DCS/SNSW did not have a 'ready to go', approved customer-tested breach response operating model.
2. **Leadership's understanding of cyber and privacy risk status and acceptance as part of DCS/SNSW's services to partnership agencies was low** and management's attestations and risk assessments were overly optimistic. Although a range of privacy and security controls to manage sensitive information were in place, there was a lack of understanding of the risks and operation of controls and what could go wrong.
3. **DCS/SNSW manages a lot of sensitive information, yet there was a low level of staff and leadership appreciation of the potential serious and long-term consequences** that a breach of such information may cause customers.

Response: DCS/SNSW displayed agility – both operational and strategic – in responding to the incident:

1. **Demonstrated itself to be a resilient organisation** with a 'one-in, all-in' mentality.
2. **Agile set-up of the response was a plus**, being change-ready due to experience and the culture of customer service and standing up new processes, DCS/SNSW displayed positivity, agility and commitment when responding to the breach.
3. **Strong sense of leadership ownership and accountability**, seeking expert advice but also making difficult decisions and owning them.
4. **Overall, the event generated moderate, low key media interest and the external communication strategy worked well**. The customer notification strategy followed a sound risk-based decision-making process and expert advice.
5. **The internal communication plan did not work as effectively** due to limited early personalised and broadcast communications, so employees did not fully absorb the messages.
6. **Strategic execution of customer strategy** – the approach taken was justified on an impact and effort basis and was aligned with regulatory guidance and best practice; the active support offered stands out as exemplar.

Organisations should treat data as both an asset and liability

Managing the data deluge

In the words of former Telstra chief executive David Thodey, the cyber attack on Optus 'could happen to anyone' and all organisations should be 'vigilant' about online security [9].

As cyber attackers have become increasingly efficient, adaptable, and sophisticated, it is impossible for any organisation to never experience a data breach. Rather than trying to remove an inevitable risk, organisations and governments should instead cooperate to **manage and minimise** risks.

The biggest source of privacy and security risks stem from the current data deluge which is occurring via the supercharged collection and processing of enormous amounts of information [10]. Indeed, the Optus incident has raised questions about the need to store government identifiers for several years. The Records and Information Management Practitioners Alliance (RIMPA), the peak body for records management, highlights that the Optus breach reflects a broader problem among all Australian organisations. 'As storage is cheap and because it is easy to keep, organisations are keeping that info for far longer than needed,' RIMPA boss Anna Cornish said [11].

The notion of data as an asset is well established as it is well-aligned with the board's responsibility to provide (among other things) strategic direction and work with the executive in driving organisational performance, including risk management and asset utilisation [10]. Organisations tend to keep data for the purposes of: (i) improving existing business functions; (ii) creating new value propositions; and (iii) underpinning new business models.

Directors should have intimate knowledge of their entity's desired outcomes, direction and operation, and potentially existential threats and opportunities created by the data deluge [10]. They must move away from 'siloed thinking' – for example, treating data as an IT concern. Instead, starting at the board level, they must ensure that data management is seen as a business-critical strategic issue. Directors should also ensure that organisational culture fosters a data and privacy aware culture that underpins all strategic and operational considerations [10].

Most importantly, organisations must contend with the fact that data can be a liability because of the risk of security breaches [12]. Directors and boards must realise that in return for holding data as an asset, they are responsible for the entity's liability, the consequences of which include regulatory action (such as fines and enforceable undertakings), class action lawsuits, financial loss (including loss of customers and stock market value) and reputation loss [12].

Balancing the pursuit of data as an asset and the protection of data as a liability cannot be achieved with only technical or legal solutions [13]. In pursuing data-driven opportunities, directors and boards must consider wider public expectations and seek acceptance for what they want to do. The relationship with the customer, the context in which it exists and the level of trust within that relationship are critical factors – they will determine whether a given use of personal information is considered delightful or creepy, acceptable, or unacceptable [13].

There needs to be stronger regulatory frameworks that provide more incentives and guidance for organisations

The need for stronger frameworks

The incentives for organisations that hold large amounts of personal information are still not aligned to consumers' best interests or the wider national interests of Australia [14]. In May, the Australian Securities and Investments Commission successfully challenged an Australian financial services firm in the federal court over the adequacy of the firm's cybersecurity risk management. The firm was ordered to pay $750,000 [14].

This was an important first in Australia. However, it raises the questions about the strength and consistency of our framework for ensuring there are consequences for cyber attacks [14].

The SOCI Act and Privacy Act are arguably not strong enough in their administration and do not provide the necessary controls that tell organisations how to protect their information.

Time to act

Organisations are well advised to stay updated on the outcomes of the Optus data breach and its impact on the Government's roadmap of reforms around privacy, data, and security.

Now is a good time for all Australian companies to be reminded of their privacy, cyber security, and other business and regulatory obligations and the need to review their data security and retention processes to ensure they are fit for purpose and compliant with regulatory and business obligations. Review your cybersecurity playbooks and data breach response procedures, rehearse them, and ensure your response team has the resources required for a possible long hold.

If organisations treat data as both an asset and liability and adequately implement the lessons learned from the SNSW data breach, this will have a positive effect on risk reduction. It would be an unenviable position for Boards and Executives to be in should any penny-pinching or risk discounting result in the need to consider paying a ransom to an attacker.

Please contact IIS Partners (contact@iispartners.com) if you would like to know more about how we can assist in uplifting your cyber security posture to address your risk and compliance obligations.

Key Questions for Boards and Executives

Boards and executives:

- Do we know what our key information assets are, especially with respect to personal information?
- Have we applied appropriate controls to provide for privacy and data protection of those assets and related risks?
- Do we fully understand the liabilities of a data breach to those assets?
- Is there an understanding of the organisation's cyber and privacy risks, operation of controls and what could go wrong?
- Have we conducted an external privacy and security assessments and internal audits to determine that our privacy and security controls are fit for purpose and comply with the law, best practice, and customer expectation?
- Have we conducted assessments for third-party service providers that have access to the organisation's personal information?
- Does our organisation have weaknesses across technology, processes and/or people that would inhibit our response to a cyber attack?
- Is there a pre-agreed and rehearsed cyber incident assessment, response and recovery approach?
- Is there an aligned and rehearsed data breach response and recovery approach?
- Do staff and leadership understand the potential serious and long-term consequences that a data breach may cause customers and employees, including more vulnerable individuals?
- Do we have a plan for the reconstruction of these assets, should all be lost due to a ransomware attack or other catastrophic physical or cyber security incident?

Bibliography

[1] ABC News, 'Optus reveals more than 2 million customers had personal ID numbers compromised in cyber attack,' ABC News, 3 October 2022. [Online]. Available: https://www.abc.net.au/news/2022-10-03/optus-data-breach-cyber-attack-deloitte-review-audit/101496190. [Accessed 4 October 2022].

[2] OAIC, 'Notifiable Data Breaches Report: July–December 2021,' OAIC, 22 February 2022. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/notifiable-data-breaches-statistics/notifiable-data-breaches-report-july-december-2021. [Accessed 4 October 2022].

[3] IBM, 'How much does a data breach cost in 2022?,' IBM, 1 August 2022. [Online]. Available: https://www.ibm.com/au-en/security/data-breach. [Accessed 4 October 2022].

[4] Australian Cyber Security Centre, 'Annual Cyber Threat Report 1 July 2020 to 30 June 2021,' 15 September 2021. [Online]. Available: https://www.cyber.gov.au/acsc/view-all-content/reports-and-statistics/acsc-annual-cyber-threat-report-2020-21. [Accessed 5 October 2022].

[5] M. Atherton and E. Sanchez-Lasaballett, 'A class action against Optus could easily be Australia's biggest: here's what is involved,' The Conversation, 5 October 2022. [Online]. Available: https://theconversation.com/a-class-action-against-optus-could-easily-be-australias-biggest-heres-what-is-involved-191515. [Accessed 5 October 2022].

[6] S. Basford Canales, 'Optus data hack: Why some want to beef up Australia's data privacy laws,' The Canberra Times, 4 October 2022. [Online]. Available: https://www.canberratimes.com.au/story/7927069/optus-data-hack-why-australias-data-privacy-laws-could-get-beefed-up/?cs=14263. [Accessed 4 October 2022].

[7] J. Mathews, J. North, M. do Rozario and J. Wallace , 'The Optus data breach: a timely reminder of your statutory cyber obligations,' Corrs Chambers Westgarth, 30 September 2022. [Online]. Available: https://www.corrs.com.au/insights/the-optus-data-breach-a-timely-reminder-of-your-statutory-cyber-obligations. [Accessed 4 October 2022].

[8] IIS Partners, 'SNSW Data Breach – Post Incident Report,' 16 December 2020. [Online]. Available: https://static1.squarespace.com/static/6110c420ee0a8f06d4fdf25b/t/612765fa2186e97aaa4483c4/1629971975737/DCS%2BSNSW%2BData%2BBreach%2BPIR%2BReport%2B16122020%2BFinal.pdf. [Accessed 3 October 2022].

[9] J. Kehoe, 'Optus hack 'could happen to anyone' ex-Telstra boss warns,' The Australian Financial Review, 28 September 2022. [Online]. Available: https://www.afr.com/companies/telecommunications/optus-hack-could-happen-to-anyone-ex-telstra-boss-warns-20220928-p5blrg. [Accessed 4 October 2022].

[10] M. Crompton and M. Trovato, 'The New Governance of Data and Privacy,' pp. 7-8, Australian Institute of Company Directors, 27 November 2018.

[11] L. Baird, 'Optus chief calls for a 'united front', says attacks premature,' The Australian Financial Review, 3 October 2022. [Online]. Available: https://www.afr.com/companies/telecommunications/optus-calls-in-deloitte-for-cyber-review-20221003-p5bmor. [Accessed 4 October 2022].

[12] M. Crompton and M. Trovato, 'The New Governance of Data and Privacy,' pp. 13, Australian Institute of Company Directors, 27 November 2018.

[13] M. Crompton and M. Trovato, 'The New Governance of Data and Privacy,' pp. 17-18, Australian Institute of Company Directors, 27 November 2018.

[14] F. Hanson, 'Criminal or state actor, there are major lessons in the Optus cyber breach,' The Strategist, 23 September 2022. [Online]. Available: https://www.aspistrategist.org.au/criminal-or-state-actor-there-are-major-lessons-in-the-optus-cyber-breach/. [Accessed 2 October 2022].

IIS Partners

INFORMATION INTEGRITY SOLUTIONS PTY LTD
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
E: contact@iispartners.com
www.iispartners.com
ABN 78 107 611 898
ACN 107 611 898