Office of the Victorian Information Commissioner

Investigation into Datatime Services Pty Ltd data breach

Under s8C(2)(e) of the Privacy and Data Protection Act 2014

6 May 2024

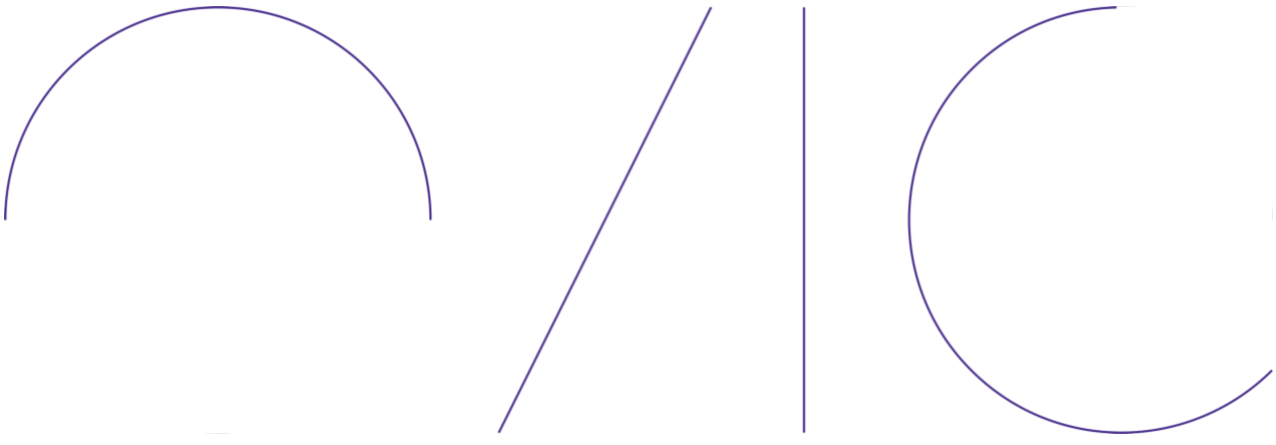

Table of Contents

Overview

In November 2022, Datatime Services Pty Ltd (**Datatime**) – a contracted service provider (**CSP**) to a number of Victorian public sector organisations (**organisations**) – suffered a data breach[1] in the form of a ransomware attack.

This meant that a malicious third party had unauthorised access to the personal information[2] of thousands of Victorians. OVIC decided to investigate under the *Privacy and Data Protection Act 2014* (Vic) (**PDP Act**) to determine whether Datatime had committed serious, flagrant or repeated contraventions of the Information Privacy Principles (**IPPs**) and whether it was appropriate to issue a compliance notice.

Ultimately, Datatime was voluntarily wound up in October 2023. This severely limited the amount of information OVIC could gather, and meant that it was not possible to formally determine compliance with the IPPs, or to decide whether to issue a compliance notice.

The Privacy and Data Protection Deputy Commissioner has nevertheless chosen to issue a report about the investigation, because the circumstances contain valuable lessons for both organisations and CSPs. This is especially so given the increasing prevalence of cyberattacks, including those involving third parties to government organisations.

Datatime and its services to Victorian government

1. At the time of the November 2022 data breach, Datatime was part of the PNORS Technology Group Pty Ltd group of companies (**PNORS**) – which also includes Netway Networks, Pacific Commerce, and Willdoo Business Management Solutions.

2. According to its archived website, Datatime was 'the Australian market leader in Document Scanning and Data Entry Services with a proven track record of successful project delivery to government, semi-government and corporate organisations'.[3] It had been operating for over 30 years.

[1] When relating to information privacy, OVIC considers that a 'data breach' occurs 'when personal information that is held by a public sector organisation (within the meaning of section 13 of the PDP Act) is subject to misuse or loss or to unauthorised access, modification or disclosure'. See https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/.

[2] Section 3 of the PDP Act defines 'personal information' as 'information or an opinion (including information or an opinion forming part of a database), that is recorded in any form and whether true or not, about an individual whose identity is apparent, or can reasonably be ascertained from the information or opinion but does not include information of a kind to which the *Health Records Act 2001* (Vic) applies'.

[3] https://web.archive.org/web/20230222084137/https://datatime.com.au/page/our-company.

Services to Victorian government

3. Datatime had longstanding arrangements for the provision of services to the Department of Education (**DE**) and Department of Families, Fairness and Housing (**DFFH**)[4].

4. Datatime undertook scanning and data capture of the School Entrant Health Questionnaire (**SEHQ**) from 2006 on behalf of DE. The SEHQ is completed by parents to record any concerns and observations about their child's health and well-being as they begin primary school in Victoria. It informs school nurses as part of the Primary School Nursing Program.

5. Datatime processed paper-based application forms for the Seniors, Companion, and Carer Card Programs since 2010 on behalf of DFFH. These cards provide a range of concessions and discounts to eligible people who are over 60 years old, who have a significant disability, or who are carers, respectively. Datatime was not involved in processing any online applications for these cards.

Datatime's obligations under the PDP Act

6. At the time of the November 2022 data breach, the following contractual arrangements were in place:

    - A 2019 contract between DE and Datatime for the preparation and processing of the Primary School Nursing Program SEHQ.
    - A 2021 contract between DFFH and Datatime for the processing, scanning and data entry of paper-based applications and associated forms for Seniors Card, Companion Card, and Carer Card.

7. Both contracts contained provisions stipulating that Datatime was bound to comply with the IPPs in relation to the activities it carried out under those contracts. Datatime was therefore a CSP within the definition set out at section 13(1)(j) of the PDP Act.

The data breach

8. On 3 November 2022, the Victorian Government's Cyber Incident Response Service (**CIRS**) advised OVIC of a ransomware attack on two companies in the PNORS group[5] - Datatime and Netway Networks.

[4] Datatime also carried out services for other organisations, but those services had either ceased by the time the data breach occurred, or did not involve Datatime holding personal information.

[5] While Datatime is the subject of this investigation, PNORS Technology Group coordinated the response to the data breach. This report therefore includes commentary on the actions of both companies. Netway Networks is not part of the investigation, as it did not hold personal information in relation to Victorian Government contracts at the time of the data breach.

9. The attack was carried out by a threat actor using *LockBit*. This is a Ransomware-as-a-service operation maintained by one cybercrime group which then sells access to its ransomware tools to other individuals or groups, allowing them to carry out attacks[6].

10. As explained below, the exact chain of events and methods used by the threat actor between the point of gaining access to affected networks and encrypting those networks has not been conclusively established.

11. However, it appears that the initial point of entry for the attack was a compromised Netway Networks server, with the threat actor then laterally moving across to gain access to the Datatime network. In attacks of this nature, threat actors will usually expand the reach of their unauthorised access by techniques such as system discovery, reconnaissance, password/credential hunting, and privilege escalation as they move around networks.[7]

12. Ultimately, the attack fully compromised the two companies, with the threat actor encrypting their networks. This denied any access to all information on those networks as well as interrupting business operations.

13. On 5 November 2022, the cybercriminal group released to PNORS, in a private communication, a sample of what was believed to be exfiltrated data and threatened to publish it unless a ransom was paid.

14. While the extent of any data exfiltrated by the threat actor has not been established, data exfiltration is a key feature of ransomware attacks of this nature[8]. Nonetheless, ongoing dark web monitoring has not found evidence of personal information being published by the threat actor.

What personal information was affected?

15. It was not possible to conclusively determine what personal information was impacted. However, given the threat actor's widespread access to the Datatime network, any personal information held by Datatime with respect to services it carried out for DE and DFFH is likely to have been subject to unauthorised access.

16. In relation to services carried out by Datatime for DFFH, it was therefore estimated that the number of individuals potentially affected by the data breach included:

    - Around 19,000 paper-based Seniors Card applicants from 2020 and 2021, plus an unknown number (up to 100,000) of paper-based Seniors Card applicants from 2012

[6] For more information on observed activity in LockBit ransomware incidents and recommended mitigations, see the Cybersecurity Advisory issued by a number of international organisations, available at: https://www.cyber.gov.au/about-us/advisories/understanding-ransomware-threat-actors-lockbit.

[7] See above, n.6.

[8] See above, n.6.

- 11,398 paper-based Companion Card applicants from 2021, plus a further 76,765 paper-based Companion Card applicants from 2003

- An unknown number (up to 11,500) paper-based Carer Card applicants from 2018, plus a further 59,700 paper-based Carer Card applicants from 2010.

17. In relation to services carried out by Datatime for DE, it undertook scanning and data capture of around 60,000 to 70,000 SEHQs each year, from 2006 to 2022. At the time of the data breach, Datatime held SEHQ data on its servers dating back to 2017.

18. Personal information contained in the Seniors, Companion and Carer card applications included name, date of birth, gender and address. Paper-based card applications contained signatures, while the Companion card application also included a photograph. The Carer card included eligibility fields such as whether the applicant receives Centrelink payments and the nature of the carer relationship. Additionally, although not subject to the PDP Act or OVIC's jurisdiction, the Companion card application collects health information[9] relating to the applicant's disability.

19. Personal information collected in the SEHQ included name; gender; date and place of birth; address; whether the child attended kindergarten; school attended; family relationships; languages spoken; whether an individual is a refugee or asylum seeker; information relating to parental background (date and place of birth, level of education); and whether a child lives in an out-of-home care placement under a child protection order. It also includes parents' evaluation of the developmental status of their child, the child's strengths and difficulties, and recent family events.

20. The SEHQ also collected health information including the types of health professionals seen; child and parental health conditions; and health related family issues.[10]

21. Given the types of personal information contained in the above datasets, the data breach created a range of risks for affected individuals, including identity theft, fraud, or other scams, as well as emotional distress.

OVIC's investigation

22. The Deputy Commissioner decided to investigate Datatime under section 8C(2)(e) of the PDP Act, to determine whether to issue a compliance notice. Under section 78 of the PDP Act, the Deputy Commissioner may serve a compliance notice on an organisation if satisfied that serious, flagrant, or repeated breaches of the IPPs have occurred. A compliance notice requires an organisation to take specified action within a specified period to ensure compliance with the IPPs.

[9] Health information is defined in section 3 of the *Health Records Act 2001* (Vic) and is regulated by the Health Complaints Commissioner. Health information is expressly excluded from the definition of 'personal information' in section 3 of the PDP Act.

[10] Given that the SEHQ is used to inform the School Nursing Program, it is open to interpret the information set out in paragraph 19 as health information under subsection (b) of that definition in that it may be considered 'other personal information collected to provide, or in providing, a health service'. However, the distinction was not material in the present circumstances.

23. The focus of OVIC's investigation was on two main themes – security measures that Datatime had in place to protect against the data breach, and Datatime's information retention and disposal practices. As such, the investigation related to the following IPPs:

> **IPP 4.1:** An organisation must take reasonable steps to protect the personal information it holds from misuse and loss and from unauthorised access, modification, or disclosure.
>
> **IPP 4.2:** An organisation must take reasonable steps to destroy or permanently de-identify personal information if it is no longer needed for any purpose.

24. OVIC notified Datatime of the commencement of the investigation and sought documents and information relating to the data breach.

25. However, Datatime's legal representative informed OVIC that Datatime was now under external administration, with the company's members having resolved to wind the company up voluntarily. Neither Datatime, nor its legal representative provided the requested documents or information.

26. OVIC then wrote to both PNORS and Datatime's external administrators, seeking the requested documents and information. Again, neither party provided the requested documents or information.

27. OVIC also wrote to the two organisations affected by the data breach – DE and DFFH. Both organisations responded by providing relevant documents (contracts and correspondence) and information about the data breach.

28. Given the above, OVIC was unable to gather sufficient information to determine whether Datatime had committed serious, flagrant, or repeated breaches of the IPPs or to decide whether to issue a compliance notice. In any case, there would be little benefit in issuing a compliance notice to an entity in the process of being wound up.

29. The Deputy Commissioner nevertheless decided to complete a report about the data breach and OVIC's investigation in accordance with section 111(3)(b) of the PDP Act, because the circumstances contain valuable observations and lessons that are relevant for both organisations and CSPs. This is especially so given the increasing prevalence of cyberattacks, including those involving CSPs to government organisations.

Observations about the data breach and the IPPs

Data security and IPP 4.1

30. From the information obtained by OVIC, it is clear that at the time of the data breach Datatime did not maintain sufficient network logging to allow for a conclusive understanding of the cause, nature and

extent of the ransomware attack. For example, firewall logs were overwritten every 24 hours. As such, forensic reports commissioned by consultants engaged by PNORS could not establish how exactly the data breach occurred nor what information was exfiltrated by the threat actor.

31. Nevertheless, from the information available, Datatime may not have taken reasonable steps to protect the personal information it held from a data breach of this nature because it appeared to have the following cybersecurity deficiencies:

    - Insufficient application control measures
    - Ineffective network segmentation
    - Insufficient restriction of administrative privileges
    - Absence of Multi-factor Authentication (**MFA**) across all user and administrative accounts for logging in to its network directly or via a Virtual Private Network (**VPN**)
    - Lack of complex passphrase rules for all Datatime accounts, or alternative methods such as passkeys
    - Ineffective firewall configuration to control incoming and outgoing network traffic
    - Lack of endpoint detection and prevention software on Datatime computers
    - Lack of incident detection and response by way of insufficient capture and monitoring of relevant logs.

32. As part of its remediation activities, Datatime took a range of steps to remedy these deficiencies. However, OVIC was unable to interrogate the efficacy of these steps, or Datatime's compliance with IPP 4.1 after the data breach.

Data retention and IPP 4.2

33. The information available to OVIC suggests that Datatime may not have taken reasonable steps to destroy or permanently de-identify personal information when it was is no longer needed for any purpose because:

    - PNORS advised DE that Datatime held SEHQ data on its servers dating back to 2017. DE formed the opinion that the retention of this data by Datatime was contrary to the terms of the service contracts between the parties. Subsequently, DE exchanged a series of letters with Datatime to ensure it securely deleted all SEHQ data from its servers.
    - DFFH data remained on Datatime's systems from 2003.

34. The destruction and de-identification of data appear to be concepts that were not well understood or managed by parties involved in the Datatime data breach. For example, Datatime was unclear about DE's expectations around IPP 4.2 and its intersection with the Public Records Act 1973.

35. There were ill-defined and seemingly conflicting terms outlined in the DE contract. Datatime appeared confused about the terms 'Records'[11] and 'Data'[12] and was therefore unclear about what information should be destroyed or de-identified, and when. The DE contract stated that, after termination or expiry, the Supplier must only dispose of Records in accordance with standards issued under the Public Records Act and must not dispose of any Records for at least seven years after termination of expiry of the Agreement. The Agreement also had a provision that any Data captured and/or stored needs to be securely destroyed following completion of the contract. Datatime believed that there was a tension between these two requirements.

36. For their part, the contracting organisations were unclear about whether and when Datatime had destroyed or de-identified the data associated with their services. Furthermore, Datatime was unable to provide this information to the contracting organisations in a timely manner as part of the incident response.

Lessons

37. Organisations and their CSPs hold considerable personal and sensitive information. Data breaches through cyberattacks can have significant impacts on the individuals who are affected by them. They can also damage public trust and disrupt business operations and service delivery.

38. The prevalence of cyberattacks is increasing. For example, cyber criminals try to access Victorian government networks every 45 seconds.[13] Protecting personal information requires that public sector organisations and their CSPs have appropriate measures in place to protect against cyberattacks.

39. To assess the adequacy of controls in relation to cybersecurity threats, organisations and CSPs should consult:

    - *Victorian Protective Data Security Standard 11* which states that 'an organisation establishes, implements and maintains Information Communications Technology (ICT) security controls'. This contains a range of elements and points to other primary sources to assist organisations to comply with the Standard.

[11] Records are defined in the Agreement as 'written records held, produced or created by the Supplier (or its Personnel) under or in the course of performing the Supplier's obligations under this Agreement'.

[12] Data is defined in the Agreement as 'any information, data, datasets or databases created by or on behalf of the Supplier in the course of providing the Services unless created for the Supplier's internal operational purposes'.

[13] https://www.vic.gov.au/prepare-cyber-incident

- The *Strategies to Mitigate Cyber Security Incidents* developed by the Australian Signals Directorate (**ASD**) to help organisations protect themselves against various cyber threats. The most effective of these strategies are referred to as the '*Essential Eight*'.

40. Organisations and CSPs should also be appropriately prepared to respond to cyberattacks when they occur as this can assist in limiting any harm. It is important to develop a cyber incident management plan and to practice using this.[14] The ASD describes that where an organisation is not prepared it:

> plays 'whack a mole', cleaning compromised computers, as well as blocking network access to internet infrastructure known to be controlled by adversaries, while the same adversaries simply compromise additional computers using different malware and different internet infrastructure to avoid detection.

41. For CSPs, preparing to respond to any data breach should involve always having a clear understanding of information holdings relating to government services – so that it can quickly report to organisations about what personal information has been affected by a breach. They should also have comprehensive communication plans for reporting a breach to relevant parties including outsourcing organisations, CIRS and OVIC.

42. Organisations should conduct appropriate due diligence in relation to a prospective CSP's information security posture – to assess it will be capable of appropriately handling personal information[15]. Where a CSP is engaged over a long period on a recurring basis, such assessments should be regularly repeated.

43. Depending on the nature and sensitivity of the information involved, conducting appropriate due diligence may involve seeking specific advice from a CSP on the cybersecurity resources and controls it has in place – such as by completing a self-assessment against the ASD's *Essential Eight*.

44. Where an organisation seeks specific advice from CSPs on cybersecurity or other information security measures, this could be incorporated into 'Request for tender (**RFT**) response' templates during procurement activities. In the present investigation, OVIC noted that DFFH's RFT response template asked tenderers to outline its processes to ensure compliance with information security requirements but left it up to tenderers as to how to answer this – leading to high-level responses from Datatime that did not capture the full range of controls that might be expected for effective risk management.

45. The data breach suffered by Datatime also illustrates the importance of appropriate destruction of personal information that is no longer needed for any purpose. Holding more personal information than is necessary increases the risk and seriousness of a data breach.

[14] It is important to note that cyberattacks are just one form of data breach that can affect personal information. For information on responding generally to data breaches (including developing a data breach response plan), see: https://ovic.vic.gov.au/privacy/resources-for-organisations/managing-the-privacy-impacts-of-a-data-breach/

[15] OVIC, Guidelines for outsourcing in the Victorian public sector – Accompanying guide, May 2017. Available at: https://ovic.vic.gov.au/privacy/resources-for-organisations/engaging-contracted-service-providers/

46. Any clauses in a State contract relating to information handling should be clear and unambiguous. It should be established between the organisation and the CSP that the meaning and effect of these clauses are clearly and consistently understood.

47. Organisations should actively monitor a CSP's (and their own) compliance with the IPPs and any contractual obligations relating to information handling. Depending on the privacy risks involved, this may include attestations, surveys, reports, site visits or audits. Contract provisions are not self-enforcing, and require some level of assurance that they are, in fact, being adhered to.

www.ovic.vic.gov.au