Office of the Victorian Information Commissioner

Case Study: Security and Privacy of Online Forms

This case study outlines the information and security implications of when a Victorian Public Sector Organisation's (**agency**) online complaint form was not configured and/or tested correctly.

What happened

The agency had launched its complaint form, which was designed by a company from the e-Services State Purchase Contract panel, 2 years prior to the incident being identified. The agency required the form to comply with the Information Privacy Principles (**IPPs**) and the Victorian Protective Data Security Standards (**VPDSS**).

The incident involved the agency's online complaint form accidently leaking data from one complainant's completed form to a subsequent user's new form.

The incident was identified not through an active audit or detection program, but when an individual was presented with a pre-populated online complaint form. This pre-population inadvertently disclosed personal information from somebody else's complaint form, a disclosure which was inconsistent with the IPPs and public sector information obligations.

Consequently, the agency investigated and identified:

- approximately 40 other potential instances where this may have occurred in the previous 18 months
- personal and complaint information may have been disclosed to people outside of the agency
- the error occurred in 0.05 per cent of form submissions.

The agency assessed this as a serious breach due to:

- the profile of the agency given the services and functions it delivers
- sensitivity and significance of the information that was compromised
- potential impact on the individuals involved
- repeated and longstanding nature of the issue
- apparent failure of previous remediation steps
- potential impact on public trust in government agencies, especially online service delivery.

How it happened

The agency's investigation found that the main cause of the data leak was due to improper web form caching or session handling where the form intermittently stored data previously entered into the web browser. The agency found that when a user began a new complaint, information submitted from a previous session was sometimes displayed in the online form. However, this did not happen every time, making it difficult to identify, reproduce and fix the error. Additionally, while the agency had previously implemented measures to prevent this scenario, they proved ineffective.

How it was fixed

The agency engaged a new website support provider, who remediated the issue by ensuring the agency's online forms no longer retained or displayed information entered by previous users.

The agency has also implemented a range of other controls in line with the VPDSS to help it manage the complaint form, including:

- improving governance and management of the new contracted service provider, including increasing the monitoring and reporting requirements in the contract
- analysing web logs weekly to verify web form caching or token recycling of any kind is not occurring
- rigorously testing and scrutinising updates to the agency's website, supporting infrastructure and online forms' function and configuration through the agency's change approval process
- having daily and weekly automated vulnerability scans of the website performed by an external service provider, and monthly scans conducted by the Victorian Government Cyber Incident Response Service.

Based on the agency's self-assessment of the breach, its communication with OVIC about the breach, and the remediation actions it took, OVIC decided there was no need to take further regulatory action in this case.

Lessons for other public sector organisations

1. Prior to any project or initiative that involves public sector information, conduct a comprehensive:
    - Privacy Impact Assessment (where personal information is identified)[1]
    - Security Risk Assessment.[2]

[1] OVIC website, Privacy Impact Assessment
[2] Refer to Element 3.010 of the VPDSS

2. Conduct due diligence before selecting a contracted service provider and ensure any assessment in respect of public sector information collected, held, used, managed, disclosed or transferred by it for the agency, includes:
    - consideration of the value of the information
    - specification of the controls required to protect the information, commensurate with the information's value
    - documentation of roles and responsibilities
    - mechanisms to provide assurance that the contracted service provider is complying with the terms of the contract.
3. Ensure any proposed changes to online forms and functionality are thoroughly tested and scrutinised.
4. Ensure secure handling and storage of any data that has been captured, collected or recorded on behalf of, or by the agency. Communicate data storage and usage policies to stakeholders.
5. Implement a robust, independently reviewed and quality assured method for auditing and analysing website logs.
6. Undertake ongoing monitoring, review, reporting and management of risks relating to the project or initiative.
7. If your online forms raise any concerns, start by speaking with your Risk, Privacy, and/or Cyber security teams to confirm whether potential risks have already been considered and addressed through existing controls.

Further resources

Privacy resources for organisations https://ovic.vic.gov.au/privacy/resources-for-organisations/

Privacy Impact Assessment Guide https://ovic.vic.gov.au/privacy/resources-for-organisations/privacy-impact-assessment/

Victorian Protective Data Security Standards https://ovic.vic.gov.au/information-security/standards/

Practitioner Guide – Information Security Risk Management
https://ovic.vic.gov.au/resource/practitioner-guide-information-security-risk-management/

Victorian Government Design forms – digital guide https://www.vic.gov.au/design-forms