Review report

FishNet Secure breach investigation

1. Background

This report is prepared in response to item 8.4 of the Queensland Ombudsman's preliminary observations and proposed actions.

Table 1 Extract from Ombudsman's Preliminary Observations and Proposed actions, 8.4

No.	Observations	Proposed actions
8.4	FishNet Secure was inadvertently accessible in December 2018*. The department has identified the reasons for this and engaged PWC to review this incident. As at February 2020, this audit is yet to be finalised.	• Expedite completion of the audit. • Publish information to the industry about: - this incident and the actions taken by the department to address the problem and ensure security of the information contained in FishNet Secure - the actions the industry can take to improve security of their information in the department's systems.

*Issue was identified and resolved in January 2019.
Source: Ombudsman's Preliminary Observations and Proposed Actions - https://daf.engagementhub.com.au/projects/download/8309/ProjectDocument

FishNet Secure was inadvertently accessible from 18 December 2018 to 3 January 2019. The Department of Agriculture and Fisheries (DAF) identified the IT security issue on 3 January 2019 and the issue was immediately resolved.

The department engaged PriceWaterhouseCoopers (PwC) to investigate this incident based on information surrounding the breach. PwC provided a Digital Forensic Incident Response with six recommendations. Recommendations and other security measures have been undertaken by the department's technical team since the incident.

2. Overview of incident

2.1 What is FishNet Secure?

FishNet Secure is a web-based service that provides authority details to permanent or temporary holders of Queensland fishing authorities (permits, licences, and quotas).

An authority holder, can perform several functions online, including:

- temporary transfers of quota
- viewing of quota balances
- viewing reports relating to authorities
- viewing vessel tracking unit/s associated with authorities
- adding/moving vessel tracking units
- lodging updates for contact details.

2.2 What did the breach involve?

The breach involved the exploitation of a configuration error that allowed users to access FishNet accounts by entering a username (client ID) with any combination of characters as a password.

The department first became aware of this through a video which was released online by a user who had discovered and demonstrated unauthorised access in FishNet Secure. The release of the video led to others replicating the unauthorised access. The perpetrators either needed to know a client ID or guess a client ID to gain unauthorised access to FishNet Secure accounts as client IDs were/are not publicly available.

2.3 What was accessed during the breach and what action did the department take to inform clients?

Several FishNet Secure user accounts and personally identifiable information (PII) associated with those accounts were accessed. The department contacted all clients whose FishNet Secure accounts were accessed during the breach. Any client that believed there had been unauthorised access to their account were advised to contact the department for investigation.

All FishNet Secure accounts that conducted quota transactions during the breach were contacted immediately by the department. No fraudulent transfers of quota were identified.

2.4 What activities could the perpetrator undertake when they gained unauthorised access?

Upon unauthorised access to FishNet Secure accounts, the perpetrators could undertake the following actions. An analysis was conducted by the department to determine if they occurred.

- Unauthorised transfers of fishing quotas between accounts
    - *No fraudulent transfers of quota were identified.*
- Create and move vessel tracking units between boats held by the client
    - *No vessel tracking units were created or moved during the breach period.*
- Create a token for use on CatchLog eLogs system
    - *No eLogs tokens were created during the breach period*
- Scraping of data from FishNet accounts including PII to collect information about the users of the FishNet application.
    - *The department cannot confirm if information was copied and retained from the system during the breach. Clients are advised to report any information that indicates fraudulent activity based on their account information.*

2.5 What activities did the perpetrators undertake during the breach as indicated by PwC?

- Six IP addresses gained unauthorised access of 314 unique accounts.
- Of the 314 accounts, access to 44 accounts went beyond the successful sign in page.
- There were 26 accounts that visited the password change page. For noting:
    - Visiting this page is forced if the client does not have a FishNet secure login.
    - No passwords were changed. To change a password, the current password would need to be entered correctly first.
    - None of these accounts had active or suspended authorities.
- There were 36 accounts where personal details may have been acquired including full name, contact details (phone numbers, addresses) and licence details.

2.6 Could the perpetrators access my vessel tracking data through FishNet Secure?

No. Vessel tracking data is not stored on FishNet Secure. Vessel tracking data is stored on a platform managed by the Australian Fisheries Management Authority. FishNet Secure only allows for the management of vessel tracking devices and associations under authorities.

3. Actions taken and continuous improvement

3.1 Immediate Response

The following were immediate responses from the department on learning of the incident:

- FishNet Secure was immediately shut down to all users on 3 January 2019 to cease any further unauthorised access.
- The password of every account accessed during the period was reset.
- The 'Fisher PIN' of every account accessed during the period was reset.
- The functionality that enabled the incident in the first place was removed.

3.2 Recommendations made to the department and actions taken

As part of the PwC Investigation Report a number of recommended actions were made. Some of these were communicated to the department's technical team and actioned during the investigation. Following are the recommendations as per the report and actions taken by the department.

Recommendation 1: Third party risk management

As the service in question is provided by a third party, regular assurance over the controls the third party has in place is strongly recommended. Ensure the controls are mandated within the contract and perform appropriate levels of testing to gain confidence over their effectiveness.

- A formal User Acceptance Testing process has been developed and implemented.
- Developer code reviews implemented.

Recommendation 2: Change and release improvements

The implementation of a new, or the improvement of the existing Development Operations function could prevent such security incidents occurring in the future. The implementation of secure change windows, appropriate prototyping and testing and monitoring aligned to a Change and Risk Management model would ensure a similar situation in the future would occur during a well-staffed period and within a safe environment.

- A formal change and release process has been developed and implemented.

Recommendation 3: Policies and standards

Reinforced or new policies and standards will ensure no future system is implemented without controls or the appropriate processes in place. Activities could pivot around policy development, training, or auditing based on specific requirements.

- Rigorous manual testing of the platform is conducted prior to production release.
- FishNet is covered under the Business Continuity Plan.

Recommendation 4: Penetration testing

Regular penetration and vulnerability assessment against web facing applications will provide an extra layer of security against new and existing threats by ensuring that you discover them first.

- Penetration test was undertaken on FishNet in Feb 2019 to identify potential vulnerabilities. There were no critical vulnerabilities identified, all high and medium vulnerabilities have been addressed and re-tested.
- The penetration tests are proposed to be conducted annually or as required if there are major releases. Any vulnerabilities identified will be addressed and retested.

Recommendation 5: Log monitoring & aggregation

The integration and aggregation of log data from web facing applications into a new or existing security function would be recommended where possible. Automated and human monitoring is also recommended where resources permit.

- The detailed logging function was turned on. The information logged by FishNet was increased.

Recommendation 6: Further investigative steps

Police or legal counsel could provide additional advice on potential breaches of the criminal code specifically in relation to computer crime or other relevant Australian acts in accessing confidential DAF material knowingly.

- The incident was referred to Queensland Police Service. No additional advice was provided.

3.3 Further FishNet Secure security improvements

On the 18th of November 2021, FishNet Secure authentication has been migrated to Microsoft Azure AD B2C, which has increased security around logging into FishNet. This new process requires a unique email address to be registered, which must match the email address in our Register of Authority system.

Prior to implementation of Microsoft Azure AD B2C, a penetration test was performed.

Microsoft Azure AD B2C is capable of 2-factor authentication, but the option has not been configured in the system yet, as it will involve significant change management for industry to adopt.

The CatchLog eLogs API has been decommissioned in April 2022 to reduce the system vulnerability.

3.4 How can you prevent unauthorised access to your FishNet Secure account?

The following tips can assist industry in enhancing security of their FishNet Secure account:

- Ensure you are aware and understand the FishNet Terms and Conditions of Use.
- Do not share your FishNet Secure login details.
- Change your password regularly.
- Only access your FishNet Secure account through your own personal device.
- If you must access your FishNet Secure account through a device that you do not own or a shared device, ensure that it is logged out and that your login information has not been saved.
- If you believe there has been unauthorised access to your account/s, notify the department immediately.

4. Lessons learnt

The department acknowledges the need for information security, particularly regarding the access of FishNet Secure. The department engaged PwC to conduct a formal assessment of the incident and has taken necessary measures to increase security as recommended by the PwC report.

5. DAF Information Security Management System

DAF has implemented and actively maintains an Information Security Management System (ISMS) based on the international security standard ISO 27001. This is in accordance with the requirements outlined in the Queensland Government Information Security Policy IS18:2018.

The ISMS includes all information, system and technology assets identified in the department's information asset register and application asset register. The ISMS takes a systematic and repeatable risk-based approach to managing information, ensuring that steps are taken to minimise threats outside of the department's established risk appetite. This includes managing information security risks related to the confidentiality, integrity and availability of information entrusted to us.

In line with the ISMS, DAF conducts six-monthly risk assessment and monitoring of existing data security controls in FishNet Secure as part of the Whole of Government Information and Communication Technology planning process administered by the Queensland Government Customer and Digital Group. This enables risk mitigation activities to be identified and implemented. DAF also undertakes other regular ongoing improvement activities and assessments as part of its ISMS.

Date of document: June 2022