Cyber:

Not for the faint-hearted…

The What:

Woollahra Council was impacted by a cyber-incident on 15 December 2023.

On this day, Council discovered that its third-party library system was experiencing an incident involving unauthorised access by a third party.

A Threat Actor exploited a software vulnerability to access the Monitor system of approximately 30 Councils and Universities in NSW, including Woollahra.

Upon discovery, Council notified Cyber Security NSW (CNSW) of the incident and immediately isolated the affected library system to prevent further unauthorised access.

The server in question was in Council's 'demilitarised zone', operating on a segregated network to internal servers; therefore limiting broader environmental exposure.

Are you serious?

Once detected, urgent investigations commenced, with the system being taken offline immediately from public use.

This meant that there was a loss of key library functions such as:

- Public computer access.
- Printing, copying, scanning.
- Facility reservation i.e. for Library rooms.
- Online payment for overdue fees.

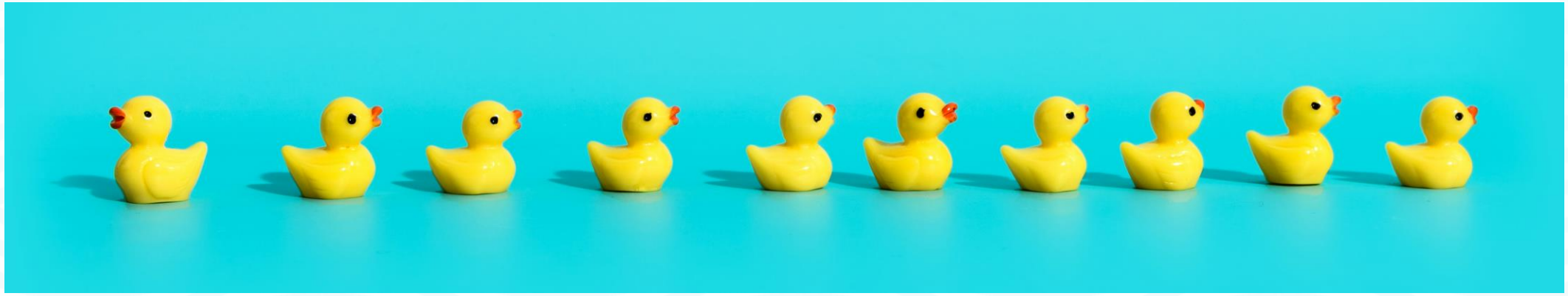
Getting our ducks in a row…

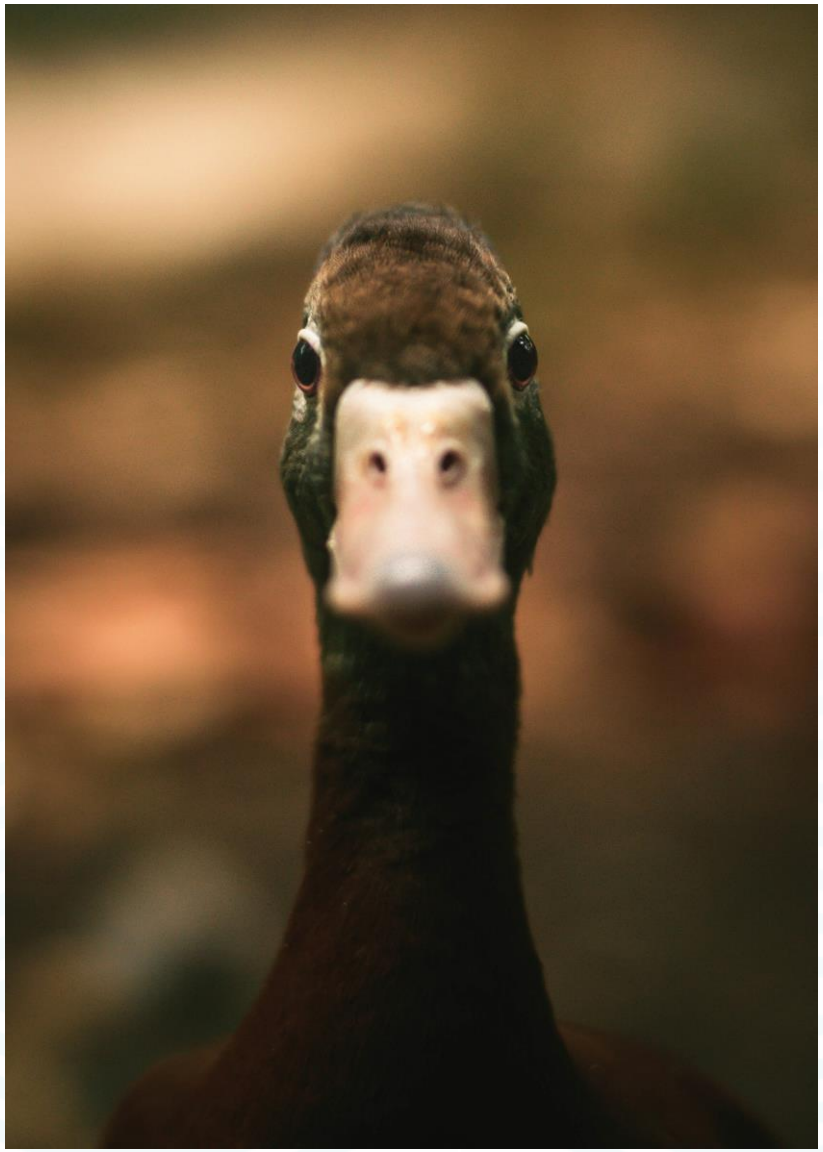
In less than 24 hours, the following response actions had taken place, noting that this list is not exhaustive:

- The two servers were network-isolated.
- All relevant firewall rules were revoked.
- Monitor BM were advised of likely breach.
- All relevant passwords (local and domain) were changed.
- Council's I&DT team and the Sophos Managed Detection & Response (MDR) team were actively investigating.
- A report to Cyber Security NSW (CSNSW) was completed.
- An Australian Cyber Security Centre (ACSC) report was also submitted.
- Council's insurance broker was informed of the incident.

More ducks…

- Following our notification to CSNSW, CSNSW sent an alert to all government entities about the potential data breach.
- Council registered the breach on the Chubb Cyber Alert online system and Council engaged appropriate legal representation.
- Council notified the Information & Privacy Commissioner (IPC) on a precautionary basis of the incident.
- Data analysis work continued in relation to determining the number of library users that might be impacted by the incident and what specific data might have been impacted.





…even more ducks…

Once the system loss was evident we:

- Equipped the library customer service staff with consistent information to provide to customers.
- Provided manual workarounds to impacted business processes, where possible.
- Provided General Manager messaging to the library staff to bolster morale and for consistency of messaging.
- Continued to investigate impacts and possible remediation until the public Monitor functions were restored on 10 January 2024.

What did the data tell us?

Data mapping indicated that there may have been unauthorised access to the records of **37,105** people, across the following types of information:

- Contact and personal information (name, email addresses, mobile numbers, phone numbers, postal addresses);

- Encrypted passwords; and

- Partial credit card details (either the partial or full credit card number only)...noting that Monitor only ever saved partial card details.

Not leaving our customers out in the cold…

- On 19 December 2023, the General Manager made the decision to notify customers of the incident.

- This decision was made following discussions internally, with our legal advisors and others.

- This was a decision taken in the interests of community trust and our belief in the protection of a person's right to the privacy and confidentiality of their details in any of our systems and / or third party systems.

Avoiding panic:

Notifying people when there is no clear breach of personal information, can result in people panicking.

This could easily have been the case when you consider the timing of all of this i.e. the sending of notifications in the days before Christmas, so not ideal !!

Of course there was little control over the timing of the incident, therefore, in the interests of community trust in Council, the decision was made to notify all concerned.

How did we notify?

In the days following the incident, we were connected with the team at ID Support NSW, an arm of the NSW Dept. Customer Service.

Notifications of such incidents are bread and butter for ID Support NSW…and they were incredible to deal with.

Not only did ID Support NSW assist us in massaging the data relating to potentially impacted customers, they were also able to run the entire notification process on behalf of Council.

How did ID Support NSW assist?

- ID Support NSW provided a range of communication templates that we were able to work with to ensure that the notification Council wanted to get out was correct and appropriately informative…all at no cost to Council.
- ID Support NSW ran the entire notification process, which included electronic & hard copy distribution of the agreed comms; all done through a range of tools at their disposal.
- Importantly, ID Support NSW operate a 1800 number and a call centre for such incidents, where potentially impacted customers can call to seek advice on how to protect their identity. This 1800 number was included on the comms to our customers, not a Council phone number.

The legal bits and the IPC…

- Council has a range of obligations under the provisions of the revised *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) and in regard to a cyber-incident, the Mandatory Notification of Data Breach scheme (MNDB Scheme).
- Under the MNDB Scheme, Council has an obligation to investigate whether a cyber-incident amounts to an 'eligible data breach' and requires notification.

information and privacy commission
new south wales

- Council has 30 days (subject to any extension) to complete its assessment as to whether the incident amounts to an eligible data breach.
- Such an assessment must be made on the basis of information available at the time, with the ability to revisit this assessment should further forensic findings impact the Council's preliminary findings.
- This does not mean Council has to notify the IPC or affected individuals within 30 days…rather it must complete its assessment within that time and subsequently notify potentially affected individuals and the IPC 'as soon as practicable' after if it forms the view that there has been an eligible data breach.

What is an eligible data breach?

Under s59D of the PPIP Act, an eligible data breach will occur when:

There is unauthorised access to, or unauthorised disclosure of, personal information held by a public sector agency or there is a loss of personal information held by a public sector agency in circumstances that are likely to result in unauthorised access to, or unauthorised disclosure of, the information (Unauthorised Access Test); and

A reasonable person would conclude that the access or disclosure of the information would be likely to result in serious harm to any of the individuals to whom the information relates (Serious Harm Test).

The MNDB Scheme applies to breaches of personal information.

Was it an eligible data breach?

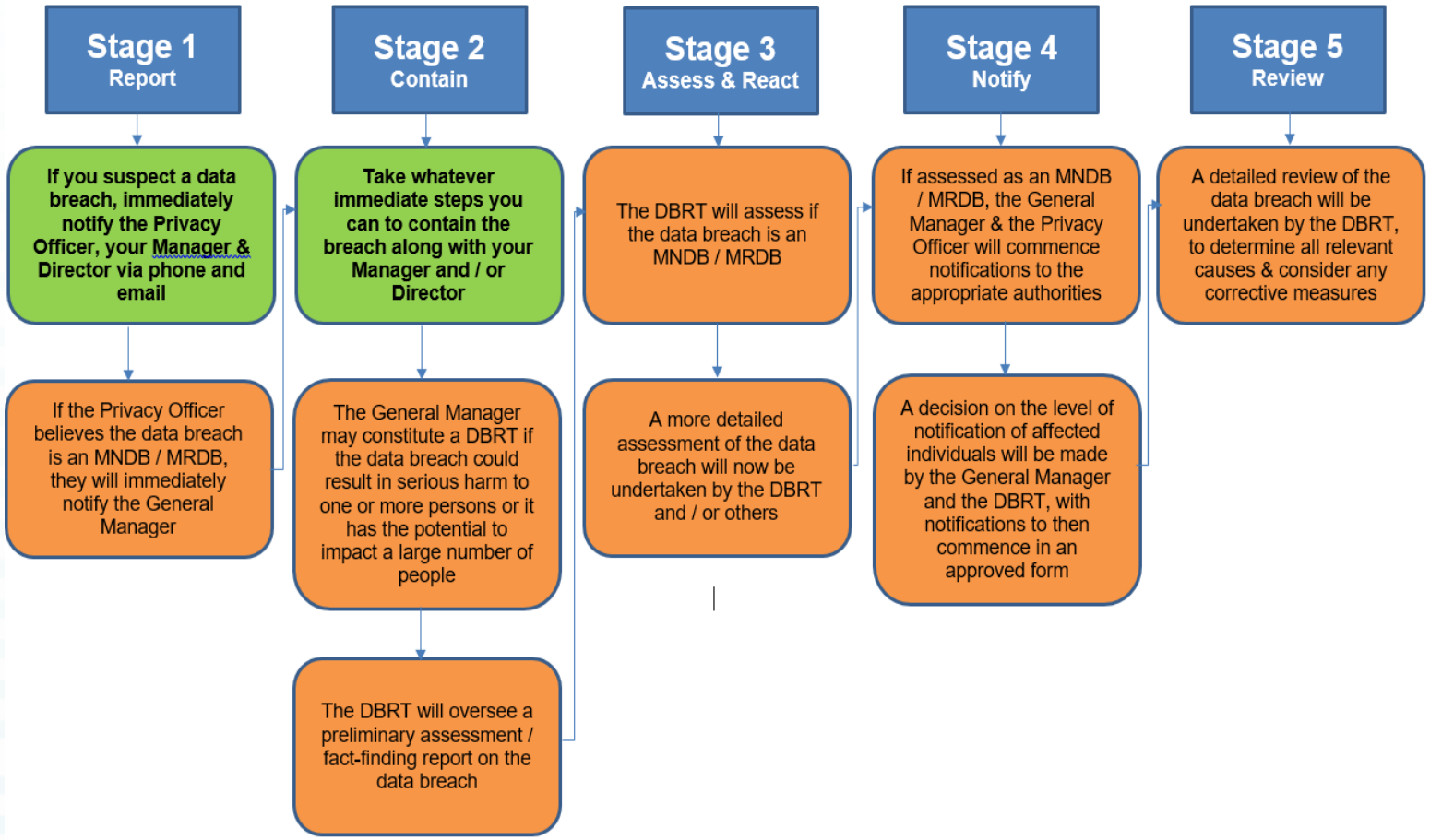
It was assessed that due to the nature of the impacted data, it was unlikely to meet the serious harm test i.e. that the information disclosed would be unlikely to result in serious harm to any of the individuals to whom the information related…therefore, as *Head of Agency*, the GM determined that the incident was not an eligible data breach.

Following approval of one extension of time for the assessment of this incident, on 31 January 2024, Council advised the IPC that it had completed its assessment of the data breach and concluded that the breach did not amount to an eligible data breach.

The IPC acknowledged this and in mid-March 2024, the IPC informed Council that this notification was now closed and thanked Council for *'…its immediate actions to identify the impacted persons and provide notification of the data breach on a precautionary basis*.'

Being prepared:

- Is your Data Breach Policy & Response Plan (DBPRP) current and easily accessible to staff and the community?
- Does your DBPRP have a quick-find guide that quickly directs staff to what to do if they suspect a data breach?
- Is your DBPRP contact list current?
- Is your crisis communications plan current and is it embedded in your DBPRP?
- Is the interplay between your DBPRP and your Business Continuity Plan clear?



Lessons learnt:

- Don’t be too cock-sure of yourself…seek assistance from others and ask lots of questions.
- There are agencies out there that can assist you, such as Cyber Security NSW and ID Support NSW.
- Stay up to date with all legislative and other changes from agencies like the IPC and Cyber Security NSW.
- Have appropriate specialist legal representation in place and ready to be activated if required.
- Find out what 3rd party contracts you have in place and gain an understanding of what those contracts state re the obligations of the contractor around security of Council-held information that they may have access to, have been provided with, or hold on behalf of Council.
- Remember that you are dealing with people, not machines…so potentially, emotions can run high.

How prepared were we for such a data breach?

What had we already done?

- Implemented Managed Detection & Response (MDR) for Endpoints & Servers, which is why Woollahra was the first entity to detect this breach.
- Incorporation of Cyber Security Risks into Council's Enterprise Risk Management Processes.
- Annual Penetration Testing.
- Adoption of Australian Government Services (Australian Protective DNS) and Cyber Security NSW services (Attack Surface Monitoring).
- Increased Cyber Security budget.

Active:

- Recruitment of one IT staff member with Cyber experience and specific Cyber Security responsibilities in their duties.
- Adoption of Third Party Risk Management system for software vendors.
- Gap Analysis of the Cyber Security Guidelines for Local Government.

Planned:

- Internal Audit review of our Cyber Security.
- External Assessment of ACSC Essential Eight Compliance.
- Development of a Cyber Security Strategy, in tandem and with the outcomes of the above activities.

Questions?