Department of Customer Service

Cybersecurity – Post-hearing responses

Questions taken on notice

Mr DAVID SHOEBRIDGE: You make it sound as though there is going to be a pool of insurance to cover the loss and damage. But, Mr Rees, that pool of insurance money just comes from another pot of public money, doesn't it? What is the size of the claim?

Mr REES: I can either take the question on notice or we can direct it to icare. I am not qualified to speak to how icare will fund the insurance claim.

Mr DAVID SHOEBRIDGE: Perhaps you might take it on notice then, Mr Rees.

Mr REES: Sure.

Answer

Service NSW is covered for its legal liabilities under the Statement of Cover (SoC) by NSW Treasury Managed Fund (TMF), a NSW Government self-insurance scheme. The TMF covers Service NSW for various losses, liabilities or damage including cover for cyber risks. The TMF is managed by icare.

A claim has been submitted by Service NSW to icare regarding the cyber incident in 2020. The claim is currently active.

Service NSW is unable to comment on the insurance arrangements underpinning the TMF.

The Hon. ADAM SEARLE: Just to be clear, I think you used the words "formally notified the Minister". Was there any informal indication to the Minister or his office or any member of his staff earlier that there may have been a data breach? If so, what time period roughly would that have occurred in?

Mr REES: I think we had informal conversations with the Minister's office prior to that, but at that time I do not believe we understood the magnitude of that. The point at which we understood the magnitude of the incident was the point at which we formally briefed the Minister.

The Hon. ADAM SEARLE: When did those informal discussions take place, roughly?

Mr REES: I will need to take that on notice.

Answer

The Department of Customer Service first alerted Minister Dominello's office to the breach and potential customer impacts on **Tuesday 5 May**.

This conversation immediately followed receipt of a report from Crowdstrike, a forensic security firm engaged to conduct a preliminary analysis of the incident, into the estimated scope of the breach, and the commencement of a preliminary plan by Allens, an internal commercial law firm engaged to provide legal advice and forensic investigation, to analyse the 47 inboxes on **4 May**.

Minister Dominello's office was contacted on **12 May** ahead of the formal briefing the next day.

Once the magnitude of the breach was realised, a formal Privacy Briefing was held at **10am on 13 May** attended by the Minister, DCS Secretary Emma Hogan, SNSW CEO Damon Rees, DCS Chief Operating Officer Stephen Brady, and GCISO Greg Wells and other senior staff. Information Integrity Solutions (IIS), our privacy advisors, were also in attendance.

A follow-up briefing was given to Minister Dominello on **18 May**, by Mr Rees.

The Hon. ADAM SEARLE: How many of the citizens whose data was compromised in March 2020 have sought compensatory payments and how many have received them? Separate to that, what other measures has your agency put in place to otherwise address the breaches or the compromising of that citizen data? If you do not have the information to hand I am happy for you to take it on notice.

Mr REES: I will take the question on notice to come back with the specifics. The number of people that have requested compensation or reimbursement is low—it is in the hundreds—but I will come back to you with the exact answer.

Answer

As at 17 February 2021:

Requests for compensation

- There have been 94 requests for compensation from citizens whose data was compromised
- Of these, 6 (six) are current or former Service NSW staff
- Of the 94 requests for compensation, 26 have been remunerated.

Requests for reimbursement

- In addition to the compensation requests, there have been 83 requests for reimbursement of costs from citizens whose data was compromised
- Of these, 8 (eight) are current or former Service NSW staff
- Of the 83 requests for reimbursement of costs, 57 have been remunerated.

Definitions of compensation and reimbursement

Requests for compensation/reimbursement are requests from customers:

- whose personal information was disclosed due to the data breach incident, and
- have received notification stating their personal information has been compromised
- who are seeking financial payments from Service NSW for loss and/or damage as a result of the data breach, above the replacement of NSW Government identity documents exposed in the breach.

Compensation refers to claims for psychological harm as a result of the data breach. This includes generalised claims for pain and suffering as well as claims based on a specific psychological harm or psychiatric harm. Specific claims need to be substantiated and evidenced with medical reports.

Reimbursement refers to claims for quantifiable out of pocket expenses (including lost income) incurred by the customer as a result of the data breach. For example, the cost of replacing a passport or reimbursement for lost wages or income.

Service NSW is replacing NSW Government issued documents such as driver licences, boat licences, citizenship papers, birth certificates free of charge for those impacted by the breach.

What other measures has your agency put in place to otherwise address the breaches or the compromising of that citizen data?

Service NSW has established a suite of privacy and security-related improvements, in concert with the Department of Customer Service, to deliver on our public commitment to make significant and enduring changes to the way we do business.

The main initiatives include the Service NSW Cybersecurity Uplift and Remediation Program, and the Service NSW Privacy Program. The Service NSW Privacy Program will address the eight recommendations made by the NSW Audit Offices' *Handling of Personal Information* report, which Service NSW has accepted in full. The Program has commenced work across all areas of Service NSW to deliver significant reforms in ambitious timeframes. This includes an urgent focus on options for implementing secure methods of transferring, and storing, personal information, replacing the need for Service NSW to rely on email; and reviewing the privacy provisions detailed in our Partner Agency agreements.

Current update in relation to controls that have been implemented within Service NSW

In addition to the above, Service NSW has implemented – as of June 2020 - an Email Management initiative applied to 2,300 frontline staff emails accounts which automatically archives all emails older

than 60 days. Emails that have been identified and tagged as containing sensitive information, are automatically archived after 5 days. This has resulted in 92% less data being held in these emails accounts and moved more than 300,000 emails for archiving within the first two weeks. This represents a significant reduction in risk to personal information but is a small part of the broader reforms and strengthening to protect customer privacy.

Mr DAVID SHOEBRIDGE: Would it be fair to say that if you were designing a system that wanted to protect people's privacy and have as many layers of cybersecurity as possible, you would not start with emails?

Mr CHAPMAN: Which is why agencies across New South Wales were actually, in fact, using Accellion as an alternative to email.

Mr DAVID SHOEBRIDGE: But the agency sitting right next to you now, Service NSW, continues to send large amounts of data by email. Are you aware of that?

Mr CHAPMAN: That is a matter for Service NSW's practices.

Mr DAVID SHOEBRIDGE: Well, I am going to ask you, first of all, Mr Chapman, if you are aware of that.

Mr CHAPMAN: I would have to take that on notice. I am not aware of the current update in relation to controls that may or may not have been implemented within Service NSW.

Answer

Please refer to the response above.

Mr DAVID SHOEBRIDGE: But the privacy risks of sending data by email has been explained to your agency and recognised by your agency since 2015. You say it is not a rapid fix, but you have been on notice about these data risks, particularly sending information through emails that do not have MFA, since 2015. That is true, isn't it?

Mr REES: I would need to take on notice when concerns were first raised in that space.

Mr DAVID SHOEBRIDGE: Well, the Auditor-General says since at least 2015. I assume the Auditor-General is accurate.

Mr REES: I will need to take the question on notice.

Answer

Multifactor Authentication (MFA) is a measure that Service NSW has planned to apply in two different ways: internally, to add assurance that only Service NSW staff are accessing our internal systems; and externally for customers, to add assurance that a customer can only access their own MyServiceNSW Account.

On 25 April 2020, Service NSW implemented MFA internally, to mitigate attacks of the type that caused the data breach last year, along with a number of other security enhancements to protect customer data.

A number of Privacy Impact Assessments have been conducted since 2015 to ensure personal information of its clients, staff and others held or accessed by Service NSW or its authorised representatives is respected and protected.

Implementing MFA as an option for customers' MyService Accounts has been on the MyService Account roadmap for some time and is on track to be delivered by the date recommended by the Audit Office.

Customers are able to access personalised NSW Government services that are offered via Service NSW, by adding them to their MyServiceNSW account. This is part of a process called 'linking'. To link a service, a customer must first provide documentation that verifies and confirms their identity, for example via the national Document Verification Service.

For noting – a program to enable multi-factor authentication (MFA) on emails was initiated in FY19/20, but progress was paused due to organisational transformation. This included a planned transition in February 2020 to the DCS Microsoft O365 platform, which integrated with the MFA Service. This was

deferred due to the NSW Bushfire Emergency response being provided by Service NSW and the at-the-time need to extend 24/7 customer support to impacted communities.

Mr DAVID SHOEBRIDGE: Is the Auditor-General accurate when it says that you did not have—and as at December 2018, so far as I understand, still did not have—reviewable logs of access history for Salesforce?

Mr REES: That is correct.

Mr DAVID SHOEBRIDGE: Are they available now?

Mr REES: I need to take that on notice.

Answer

We now do have reviewable access logs for salesforce and can see when staff have accessed information.

We are further enhancing this to meet the audit office's recommendations of delineating role-based access controls, and regular access monitoring and access reviews.

Mr DAVID SHOEBRIDGE: Has it been fixed since December and now?

Mr REES: We have remediated a range of risks around our use of Salesforce. I will need to take on notice the status of that particular item.

Answer

Yes, the logs are now available.

Mr DAVID SHOEBRIDGE: Is it used to store information gathered from the COVID-19 app?

Mr REES: It is not used to store the contact tracing information that we gather.

Mr DAVID SHOEBRIDGE: What is?

Mr REES: That data that we gather through the COVID check-in is stored in a completely different system.

Mr DAVID SHOEBRIDGE: What system?

Mr REES: I will need to take on notice the actual technology

Answer

The Check-in event information (Person ID, Business / Venue ID, Date/Time of Check-In) is stored in ServiceNSW's secure virtual cloud hosted in Australia (AWS).

For customers who don't have a MyServiceNSW Account, any personal details provided during Covid Safe Check-in is stored in secure virtual cloud hosted in Australia (AWS).

MyServiceNSW Account customers do not need to provide personal details, and only check-in information is stored in secure virtual cloud hosted in Australia (AWS).

All Covid-check in data is encrypted and stored securely. Data is deleted after 28 days.

Mr DAVID SHOEBRIDGE: What firm? What company? Is it outsourced?

Mr REES: I will take that question on notice.

Answer

Service NSW manages all databases that collect and store Covid Safe Check-in information.

The data is stored in Service NSW's Secure Private cloud in AWS (Amazon Web Services) using modern event streaming and relational database technology.

Mr DAVID SHOEBRIDGE: Are you aware that the privacy documentation for Service NSW does not include details or information about the exemptions under the health legislation, which is what is used to share information on the COVID-19 app with NSW Health?

Mr REES: The sharing of contact tracing information from the COVID check-in to Health is covered under the privacy consent statement for that service with customers.

Mr DAVID SHOEBRIDGE: Can you provide a copy of that privacy consent statement to the Committee?

Mr REES: I will take that on notice.

Answer

COVID Safe Check-in – Privacy Collection Statement

This Privacy Collection Statement is to advise you of the personal information Service NSW will collect from you as a result of either your use of the COVID-19 Safe Check-in tool via the Service NSW app or using the Service NSW Web Check-in.

Any personal information Service NSW collects from you in your use of the other features of the Service NSW app or otherwise in your dealings with Service NSW will be handled by Service NSW in accordance with the Service NSW Privacy policy.

Service NSW COVID-19 Safe Check-in tool and web check-in

The Public Health (COVID-19 Restrictions on Gathering and Movement) Order (No 7), as amended by the Minister for Health and Medical Research from time to time ('the Order') requires people who enter certain premises to register their contact details electronically either with Service NSW, or with the occupier of the premises, unless otherwise specified in the Order. The information has to be kept for a period of 28 days and will be provided to the Chief Health Officer, if requested, for contact tracing purposes.

Under the Order, from 1 January 2021, hospitality venues and hairdressing salons must require persons entering those premises to electronically register their details with Service NSW through the COVID-19 Safe Check-in tool or the Service NSW web check-in. Occupiers of hospitality venues and hairdressing salons are not permitted to use any alternative electronic registration process unless it is not possible to do so because of unexpected circumstances which are explained later in this Privacy Collection Statement.

The tool is a contactless way to support businesses to be COVID Safe by providing a safe and easy solution to help track and manage customer check-ins in a seamless and secure way.

The COVID-19 Safe Check-in tool or the web check-in enables you to 'sign in' to a participating venue in NSW. While it is not compulsory under the Order, the NSW Government encourages you to also use the COVID-19 Safe Check-in tool to 'check out' of the premises when you leave.

In order to use the COVID-19 Safe Check-in tool via the Service NSW app you will need to either have a MyServiceNSW Account or register to use the tool as a 'guest' using the link provided via the Service NSW app.

If you access the COVID-19 Safe Check-in tool using your MyService NSW Account, the contact details you have provided to Service NSW in connection with your MyServiceNSW Account will be used by Service NSW for the purpose described in this Privacy Collection Statement. This is in addition to the way Service NSW handles your personal information as described in the Service NSW Privacy policy.

If you access the COVID-19 Safe Check-in tool by registering to use the tool as a 'guest', Service NSW will collect your Personal Information for the purposes described in this Privacy Collection Statement.

Service NSW COVID-19 Web Check-in

In order to enable people who do not have the Service NSW app to 'sign in' to premises as required under the Order, Service NSW provides the COVID-19 Web Check-in.

The COVID-19 Web Check-in is a webform which will be completed by a staff member at the premises you are visiting on your behalf to register your attendance.

In order to use the COVID-19 Web Check-in you will need to provide your Personal Information to the staff member at the premises you are visiting.

If you use the COVID-19 Web Check-in, Service NSW will collect your Personal Information for the purposes described in this Privacy Collection Statement.

Personal information

Service NSW is collecting your personal information for the purposes of registering your attendance at a venue in accordance with the Order and to otherwise help protect the health and welfare of members of the public during the COVID-19 pandemic, including so that you can be contacted by NSW Health in the event that another person at that venue is a confirmed or suspected case of COVID-19 and so that Service NSW can send advisory notifications and advice to you, on behalf of NSW Health, if you might be at increased risk of becoming infected.

By using either the COVID-19 Safe Check-in tool via the Service NSW app or the COVID-19 Web Check-in, Service NSW will create a record of your attendance at the venue.

If you access the COVID-19 Safe Check-in tool using your MyService NSW Account, Service NSW will retrieve your contact details (including your name, email address and mobile phone number) from your MyServiceNSW Account. If you have not registered a contact phone number with Service NSW, then Service NSW will also collect this information when you use the COVID-19 Safe Check-in tool.

If you register to use the COVID-19 Safe Check-in tool via the Service NSW app as a 'guest', Service NSW will collect your contact details (including your name and mobile phone number).

If you use the COVID-19 Web Check-in, Service NSW will collect your contact details (including your name and either phone number or email address).

While the Order does not require the collection of both an email address **and** a mobile phone number, Service NSW considers that both forms of contact information are reasonably necessary to protect the health and welfare of members of the public during the COVID-19 pandemic

When you scan the QR code made available to you at the venue or use the COVID-19 Web Check-in, Service NSW will collect the following additional information:

- details of the premises you are attending, and
- time and date of your attendance

This additional information will, together with your contact details, comprise the record of your attendance at the venue.

Service NSW will hold the record of your attendance for a period of 28 days from the date it was collected and will handle such personal information in accordance with the Order.

If requested by the Chief Health Officer, the record of your attendance will be disclosed by Service NSW to the Chief Health Officer for the Chief Health Officer to use in the manner contemplated by the Order.

Upon the expiry of this 28-day period:

- if you accessed the COVID-19 Safe Check-in tool using your MyService NSW Account, Service NSW will permanently delete the additional information that was collected (i.e. details of the premises attended, time and date of attendance). Your contact details in your MyServiceNSW Account will not be changed or deleted; and
- if you registered to use the COVID-19 Safe Check-in tool as a 'guest' or used the COVID-19 Web Check-in at a Service NSW Service Centre, Service NSW will permanently delete the record of your attendance.

Any information transferred to the Chief Health Officer may be retained for more than 28 days in accordance with the Order.

If you do not provide your personal information to Service NSW in the manner described within this Privacy Collection Statement you will not be able to register your attendance at the premises via the Service NSW app or COVID-19 Web Check-in, and you may be required to sign in using the alternative means provided by the occupier of the premises.

The Order requires you to register your contact details electronically, unless it is not possible to do so because of unexpected circumstances. In that case, you still have to provide your contact details to the venue, and the venue has to register them electronically within the timeframe permitted by the Order.

Registering another person's details

You can register contact details for another person if that person is unable to complete their own electronic registration because of age, disability or an inability to understand the electronic registration device. For example, if a child enters a venue with you, you can complete the child's registration.

Notifications

Unless you choose to opt-out, SNSW will send advisory notifications and advice to you if you might be at increased risk of becoming infected. For example, we may send you a message about the action we advise you to take because there is a hotspot near where you live or near a business you have visited. SNSW will send these messages on behalf of NSW Health. You may receive them by email, SMS, or other means of contact that you have provided to us.

If you want to opt-out of receiving these notifications, go to settings - preferences and notifications.

Additional information

You may ask for access to the personal information we hold about you at any time and request to update, correct or amend your personal information using the contact details set out in the Service NSW Privacy policy.

However, once you register your attendance at a venue using the COVID-19 Safe Check-in tool or COVID-19 Web Check-in at a Service NSW Service Centre you will not be able to update or amend the details of your attendance.

If you are concerned about an alleged breach of privacy law or any other regulation, please contact Service NSW using the details set out in the Service NSW Privacy policy.

For further information about how we protect your privacy, to make a privacy complaint or to seek to amend the personal information we hold about you, please see the Service NSW Privacy policy.

Mr DAVID SHOEBRIDGE: Has Cyber Security NSW double-checked the cybersecurity levels for that COVID-19 information that is being gathered by Service NSW under their app?

Mr CHAPMAN: I would have to check, Mr Shoebridge, about the exact involvement of Cyber Security NSW.

Answer

The Covid Safe Check-in app has undergone multiple external reviews. These include a Privacy Impact Assessment, multiple Penetration tests, Secure by design activities, and internal reviews.

An independent Privacy Impact Assessment was conducted on the Covid Safe Check-in by The Lockstep Group: https://www.service.nsw.gov.au/privacy-impact-assessment-covid-safe-check

The CHAIR: Has the Department of Customer Service taken the actions recommended by the Auditor-General, to be taken by July last year, to improve the security of the Registry of Births, Deaths and Marriages?

Mr WELLS: I cannot speak to the specifics of the Department of Customer Service. While we are in and part of the Department of Customer Service, we have got a whole-of-government view and a whole-of-sector role in terms of uplifting that capability, so I might need to take that on notice and come back to you.

Answer

Please see appendix A on the following page

The Hon. ADAM SEARLE: The audit report into the integrity of the births, deaths and marriages registry found that births, deaths and marriages has no direct oversight of the database and is very much reliant on third party assurance, a private company holding and maintaining that data. What is

being done to address that and how many and what percentage of State agencies are also, as it were, hostage to private providers holding customer data, that is public data, given to them by State agencies?

Mr WELLS: Maybe I would start with, in order to provide the services to government those suppliers must be on something called the ICT Services Scheme. It is the way we procure services. In order to get on those panels they need to satisfy—

The Hon. ADAM SEARLE: Just pausing, that was not the question. The question was, what percentage of government agencies have the data they get from customers held by the companies?

Mr WELLS: We do not have the statistics. I can take that on notice.

The Hon. ADAM SEARLE: Please do.

Answer

A RACI matrix was developed on July 2020 to formalise the responsibilities between the Registry of Birth, Death and Marriages and the Department of Communities and Justice in relation to the management of database security.
The database is in a secure data centre in Sydney administered by internal DCJ staff through a managed service provider.

The Department of Customer Service is unable to confirm how many government agencies across NSW Government have their data held by private companies. This information is held and managed by the individual agencies or clusters.

In the Department of Customer Service it is estimated close to 100% of agencies have their data held by private companies (cloud service providers, data centres etc). All private companies holding NSW Government data are bound by a contract which specifies how the data is stored and processed in order to protect the confidentiality, availability and integrity of the data.

Appendix A: Responses to recommendations in the Auditor General's report *Integrity of data in the Births, Deaths and Marriages Register*

No.	Recommendation	Response
1.	As a matter of urgency, the Department of Customer Service (DCS) should ensure that the Registry of Births Deaths and Marriages (the Registry) works with the Department of Communities and Justice (DCJ) to ensure that passwords for users authorised to access the databases and servers comply with the DCJ's policy on password settings. **Response:** Accepted. The DCJ Chief Information Security Officer is facilitating the implementation of the DCS Password Policy to ensure compliance for all authorised users. It will be completed by 30 April 2020.	Completed and in place.
2.	By July 2020, the Department of Customer Service should ensure that the Registry of Births Death and Marriages routinely monitors: privileged user activity in the Register, other user activity in the Register, including activity outside normal office hours, reporting software user activity. **Response:** Accepted. The Registrar has commenced regular Privileged Access User Activity Audits and After-Hours Access Audits through the internal Audit Program.	Completed and in place.
3.	By July 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages restricts the ability of LifeLink users to export and distribute information from the Register outside of legitimate actions required for their role. **Response:** Accepted. Information protection arrangements are being put in place to restrict the extraction, printing and emailing of LifeLink information outside of the LifeLink system by July 2020.	This was investigated and found that the ability to extract, print and email information from LifeLink is required for Registry staff to perform their regular duties. However, information protection arrangements are in place to mitigate risk through regular user audits of activity, restrictions on access based on user role, and audits of access out of hours.
4.	By July 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages updates the Service Partnership Agreement with Service NSW to include monitoring of Service NSW Staff activity in the Register. **Response:** Accepted. Work is underway to update the Service Partnership Agreement. Action to be completed by end of July 2020.	SPA updated.
5.	By July 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages performs regular fraud detection audits for eRegistry users. **Response:** Accepted. Regular Fraud detection audits for eRegistry uses have commenced.	Assurance Reviews are performed regularly.
6.	By July 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and	Completed.

	Marriages works with the Department of Communities and Justice to ensure that there are regular access reviews of users of the databases and servers that sit behind the Register, there is regular monitoring of activity of users who have access to the databases and servers that sit behind the Register, there are regular audits to provide independent assurance that database security controls operate effectively. **Response:** Accepted. An access review process is being developed jointly by the Registry, DCJ and DCS. In addition, the new database security controls will be implemented, with an external audit undertaken to independently confirm the effectiveness of security control. Action to be completed by end of July 2020.	
7.	By July 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages clarifies and formalises responsibilities with the Department of Communities and Justice in relation to the management of database security. **Response:** Accepted. RACImatrix is developed and roles and responsibilities have been clearly identified. Action complete.	RACI in place to address concerns of audit.
8.	By December 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages undertakes a risk-based analysis of the impact of gaps in the controls to prevent unauthorised user activity on the historical integrity of data in the Register. **Response:** Accepted. The Registry will undertake risk analyses within the required time frame and determine an action plan required to mitigate the risks identified through the analysis. Action to be completed by end of December 2020.	Risks identified analysed and included on risk register
9.	By December 2020, the Department of Customer Service should ensure that the Registry of Birth, Death and Marriages implements remediating action stemming from recommendation eight. **Response:** Accepted. The Registry will implement the action plan that is determined from response to recommendation 8. Actin to be completed by end of December 2020.	Remediating action implemented to prevent staff who have departed the Registry from accessing the Register. Regular audits and checks against establishment.

PORTFOLIO COMMITTEE NO. 1 – PREMIER AND FINANCE

INQUIRY INTO CYBERSECURITY

Supplementary Question to the Department of Customer Service

Question 1. What is the status of the NSW Government's update to its Cyber Security Strategy? Please provide details as the committee understands that this was due for release in late 2020.

Answer 1: The NSW Government's Cyber Security Strategy is currently under development and is set to be released in the first half of 2021.