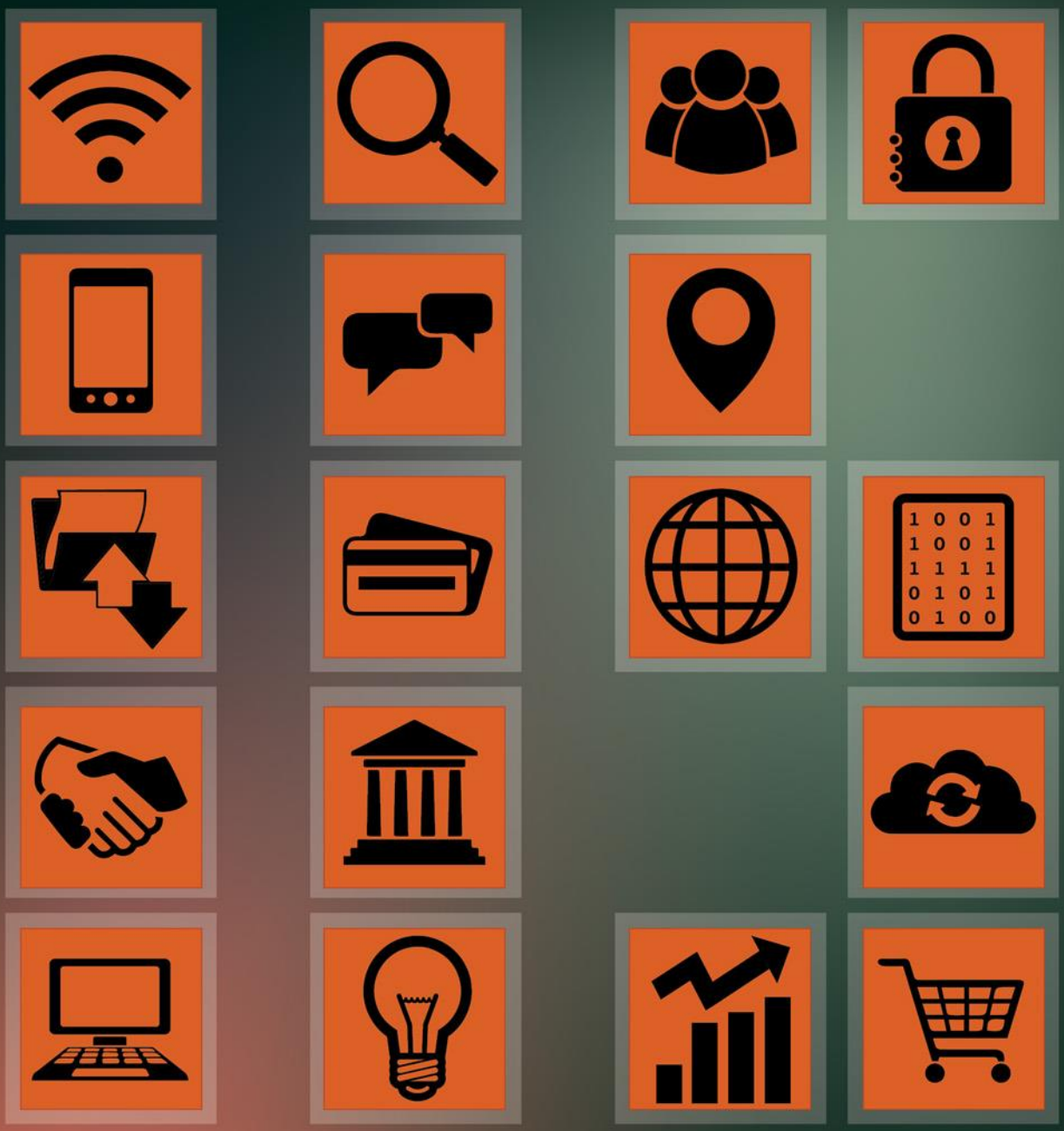


SNSW Data Breach – Post Incident Report

For: NSW Department of Customer Service

Date: 16 December 2020 – FINAL

OFFICIAL: Sensitive NSW Government

INFORMATION INTEGRITY SOLUTIONS

managing the **privacy** of **individuals** is **complex** and we can help you get it **right**

Table of Contents

Glossary

Abbreviation or term	Expansion or definition
ACSC	Australian Cyber Security Centre
Allens	Allens Linklaters
AP List	Affected Person List
ASD	Australian Signals Directorate
ATO	Australian Tax Office
BAU	Business as usual
BCM	Business continuity management
BDM	Births, Deaths and Marriages
CEO	Chief executive officer
CISO	Chief information security officer
CITAF	Cyber Incident Task Force
COO	Chief operating officer
CPRG Group	Cyber and Privacy Resilience Governance Group
CRM	Customer Relationship Management
CRN	Centrelink Reference Number
CSAT	Customer satisfaction
DAC	Data and Analytic Centre
Data breach	A data breach is unauthorised access to or unauthorised disclosure of personal information, or a loss of personal information an entity holds
DCS	NSW Department of Customer Service
DIY	Do it yourself
DOFM	Do it for me
GovConnect NSW	GovConnect NSW a provider of outsourced shared services including: Business process services (BPO) in the functional areas of finance and accounting, human resources and payroll, and SAP systems and Information Technology services (ITO) in the functional areas of information technology and service desk. The Accellion file sharing platform is a service available via GovConnect.
GRP	Governance Risk and Performance
Hypercare Team	Privacy customer service team
IoC	Indicators of compromise
IPC	Information and Privacy Commission
IPPs	Information Privacy Principles in the PPIP Act
ISMS	Information Security Management Systems
LOE	Level of Effort
MFA	Multi Factor Authentication

Abbreviation or term	Expansion or definition
NDB	Notifiable data breach
OAIC	Office of the Australian Information Commissioner
Personal information	Information or an opinion (including forming part of a database and whether or not recorded in a material form) about an individual whose identity is apparent or can reasonably be ascertained from the information or opinion. Relevant exceptions include information about an individual who has been dead for more than 30 years, and information about an individual contained in a publicly available publication. (PPIP Act, s 4)
Personally Identifiable Information (PII)	PII originates from the legal context in the United States and refers to specific pieces of information that can distinguish or trace an individual's identity, such as name, social security number, and date and place of birth. PII is sometimes conflated with 'personal information' by entities within Australia. IIS notes the latter term has a wider scope as it applies to *any* information that could, alone or combined with other readily available information, reasonably identify an individual.
PID	Public Interest Direction
PMO	Project Management Office
POI	Proof of Identity
PPIP Act	*Privacy and Personal Information Protection Act 1998* (NSW)
SDA	Sensitive data assessment
SME	Subject matter expert
SNSW	Service New South Wales
SNSW DBRP	SNSW Data Breach Response Plan
SOC	State Owned Corporations
TFN	Tax file numbers
TfNSW	Transport for NSW
The Group	Cyber and Privacy Resilience Governance Group
WFH	Working from home

1. Executive summary

1.1 Introduction

The NSW Department of Customer Service (DCS) asked Information Integrity Solutions Pty Ltd (IIS) to provide expert independent advice to its Cyber Incident Task Force (CITAF) that has been stood up to respond to a major data breach. At the time of writing this report, notifications were still in process.

About the breach

In March, Service NSW (SNSW) was the victim of a criminal cyber-attack. Upon investigation, it was determined that 47 SNSW staff email accounts were compromised and 730 GB of data was exfiltrated, comprising 3.8 million documents that relate to up to 186,000 customers.

The types of personal information compromised included sensitive data such as driving licences, birth certificates, passports, police checks, bank accounts, names, and email addresses which have the potential to result in significant customer impacts.

For staff or former staff, the types of personal information also included information gathered during recruitment and onboarding including many cases their personal particulars and TFN numbers as well as sensitive employment related items such as disciplinary and health matters.

About the report

In addition to providing advisory services during the breach response, DCS asked IIS to write this Post Incident Data Breach Report. The Report is an independent review of how DCS and SNSW in particular have managed the response to the cyber incident (see Section 2 for more information).

This report is not intended to be a formal root cause analysis of the cyber incident, nor an assessment of the cyber incident response procedural documentation. However, in order to assist CITAF and issue this report, IIS obtained a high-level understanding of readiness status prior to the event.

This report is primarily concerned with privacy (in particular, the aspect that relates to incident response pertaining to a large breach of personal information), which in turn is impacted by cyber security.

IIS would like to thank DCS/SNSW management and staff members for their collaboration and support during the development of this report.

1.2 IIS overall opinion

At the outset, DCS/SNSW found itself in a position of adversity, with their resilience being severely tested through a series of external crisis events while going through re-organisation as part of the 2019 Machinery of Government changes. Despite these challenges, DCS/SNSW responded in a way that demonstrated many attributes of a customer-focused and resilient organisation.

The mobilisation of resources and scale-up of front desk teams ensured that customer service levels were not impacted. However, IIS observed that the incident resulted in ‘disruption’ as internal

initiatives across the DCS cluster had to be postponed. In focusing so strongly for many years on excellent customer service outcomes, SNSW was slow to address cyber vulnerabilities highlighted by the Essential Eight Strategies Audit in December 2018 and IT General Controls Audit in August 2019.

Nevertheless, SNSW has mounted a significant effort to respond and recover from the data breach, by remediating the pre-exiting vulnerabilities while adapting to the challenges facing the organisation and incorporating lessons learned via other external crises such as floods, bushfires and COVID-19.

Finally, through this experience DCS/SNSW jointly have demonstrated the ability to reshape itself through innovation and agility, while producing learnings that can be shared across the Whole of NSW Government.

IIS assessed and advised on the response and recovery based on NSW law, policies and procedures as well as best practice in the wider Australian and global context.

Our key findings are:

Readiness: DCS/SNSW was not able to resist disruption to the business:

1. **DCS/SNSW was underprepared to respond** to an incident of this scale due to weaknesses across technology, processes and people and the lack of a pre-agreed and rehearsed incident assessment and response approach. Moreover, DCS/SNSW did not have a 'ready to go', approved customer-tested breach response operating model.
2. **Leadership's understanding of cyber and privacy risk status and acceptance as part of DCS/SNSW's services to partnership agencies was low** and management's attestations and risk assessments were overly optimistic. Although a range of privacy and security controls to manage sensitive information were in place, there was a lack of understanding of the risks and operation of controls and what could go wrong.
3. **DCS/SNSW manages a lot of sensitive information, yet there was a low level of staff and leadership appreciation of the potential serious and long-term consequences** that a breach of such information may cause customers.

Response: DCS/SNSW has displayed agility – both operational and strategic – in responding to this incident:

1. **Demonstrated itself to be a resilient organisation** with a 'one-in, all-in' mentality. The team has overcome many challenges and the team is largely on track to meet its goals and success measures for the incident response.
2. **Agile set-up of the response was a plus**, being change-ready due to experience and the culture of customer service and standing up new processes, DCS/SNSW displayed positivity, agility and commitment when responding to the breach.
3. **Strong sense of leadership ownership and accountability** during the response, seeking expert advice but also making difficult decisions and owning them.
4. **Overall, the event generated moderate, low key media interest and the external communication strategy worked well**. The customer notification strategy followed a sound risk-based decision-making process and expert advice. However, in hindsight (especially in

light of the unexpected length of time to complete a very complex analysis prior to the notification phase), there are aspects that could be improved for future responses.

5. **The internal communication plan did not work as effectively** due to limited early personalised and broadcast communications, so employees did not fully absorb the messages; management has already recorded the lessons learned from this.
6. **Strategic execution of customer strategy** – the approach taken was justified on an impact and effort basis and was aligned with regulatory guidance and best practice; the active support offered stands out as exemplar.

IIS notes that although the system appears to be working for the individuals who actively engaged with SNSW, the strategy assumed that most customers, on receipt of the notification letter, would act individually to assess and mitigate their risk. While customers were inevitably displeased to learn their information has been compromised and many were particularly unhappy with the length of time that it took to be notified , those that made contact appeared to be impressed by the quality of support and could appreciate the work done across agencies to mitigate the risk.

Key insights and metrics show:

- The channels have performed well in terms of supporting volumes, although volumes may become larger than anticipated; monitoring and forecasting volumes remain important and challenging.
- The Customer Satisfaction (CSAT) performance of Hypercare has been excellent.
- The IDCARE experience and support has been well received.
- SNSW delivered best practice customer experience for the majority of those it supported (otherwise unknown for non-responders).

Future focus: With a ‘do not let a crisis go to waste’ attitude:

- DCS/SNSW has made a conscious effort to learn and share its learning for a more resilient NSW Government
- DCS/SNW has established a program of work to uplift cybersecurity and privacy (known as Project Trust), including a DRF-funded program focused specifically on SNSW Cyber Remediation and Uplift.

IIS has made 26 actions with the following priority ratings:

- **Current –** address within the next **three months** / as part of current data breach response.
- **BAU/Project –** address within the next **six to nine months** as part of business-as-usual process or within a project, like Project Trust.
- **Playbook** – include in a Playbook to guide NSW Government teams so they can prepare, respond, prioritize actions and engage the right people during a data breach response. To be developed and socialised in the next **three to six months** (Note: these actions go beyond the specifics of this incident and DCS/SNSW’s response).

- **Consideration** – Further considerations to enhance: (i) cyber and privacy resilience posture; or (ii) customer service and capability.

No.	Priority	Action
1	**Current & Playbook**	Secure dedicated response team
2	**Playbook**	Document changes to response team composition and roles
3	**Current**	Plan for healing and recovering
4	**BAU/Project**	Monitor staff attrition and morale levels
5	**BAU/Project & Playbook**	Consolidate stakeholders' relationships
6	**Current & Playbook**	Check point on data handing procedures
7	**BAU/Project**	Review DCS and SNSW crisis triggers and touch points
8	**BAU/Project**	Review and update SNSW Business Continuity and Data Breach Response Plans
9	**BAU/Project & Playbook**	Enhance Communication Data Breach response
10	**BAU/Project**	Secure specific media training to leaders
11	**Playbook**	Prioritise internal communications
12	**BAU/Project**	Review incident and data breach escalation procedures
13	**Playbook**	Re-visit harm assessment when extent of breach is confirmed
14	**BAU/Project & Playbook**	Plan needs and requirements to complete forensic analysis
15	**Playbook**	Consider alternatives to primary strategy (contingency)
16	**BAU/Project & Playbook**	Assess customer risk exposure continuously
17	**BAU/Project**	Review core breach response operating model and capabilities
18	**Consideration & Playbook**	Holistic reporting showing customer effort and journey progress

No.	Priority	Action
19	**Consideration & Playbook**	Collate all available customer insights from front line staff
20	**Consideration & Playbook**	Collate insights about effectiveness of letter and plan to conduct extra research/testing
21	**Consideration & Playbook**	Plan framework for tracking end-to-end customer experience and associated improvement plan during incident response
22	**Consideration & Playbook**	Review issue of compensation for effort and associated language
23	**Consideration & Playbook**	Capture journey insights, pain-points and improvement opportunities
24	**Consideration & Playbook**	Review flexible systems architecture and service design options to facilitate future responses
25	**Consideration & Playbook**	Formally consider broader customer research scope (i.e., beyond those who contact SNSW)
26	**Consideration & Playbook**	Review effort, cost, value added and outcomes by segment

***Note**: On 11 November 2020 while the draft version of this report was being finalised, DCS/SNSW informed IIS that they discovered further issues with the forensic analysis of the data. As a result, the total number of individuals impacted by the data breach is now significantly lower than the original number. DCS/SNSW has identified that notifications have been sent to individuals that were not impacted by the cyber incident, while also discovering that the number of impacted staff is higher.*

This confirms again the risk of working with email as a means of sensitive personal information data sharing with customers and between government agencies and the challenges of understanding and actioning unstructured data in email files. Nevertheless, DCS/SNSW has further demonstrated resilience and has rapidly initiated remediation.

While this report is based on the original number of impacted individuals, this does not change our findings and conclusions.

2. About the report

2.1 Scope and purpose

DCS engaged IIS in May 2020 to provide independent expert privacy assessment services as follows:

- **Incident Management Response** – Immediate, active and adaptive expert independent advice to support the decisions of the DCS/SNSW Incident Management Team.
- **Post Incident Data Breach Review** – Independent review of how DCS/SNSW has managed the data breach incident from its discovery.

During the **Incident Management Response,** IIS provided advice to support the DCS/SNSW Incident Management Team as follows:

- Daily check-ins for the first four months with all CITAF streams
- Privacy matters decision-making across the CITAF streams
- CEO, Deputy Secretary and Secretary requests, issues and risks
- Cyber and Privacy Resilience Governance Group attendance and advice
- Customer, media, comms, stakeholder and partner engagement issues, risks and strategies
- PMO team after daily checkpoints and actions
- Daily CITAF progress reports during the 'hot phase' of directional decision-making.

IIS notes that the PMO was appreciative of the privacy assessment support we provided during CITAF stream meetings and bilateral conversations, which were open, transparent and constructive.

IIS maintained independence throughout the **Incident Management Response** and **Post Incident Data Breach Review** phases by:

- Identifying and discussing the assessment activities with DCS prior to, during and after the engagement.
- Actively managing conflict of interest in the delivery of assessment services from the following:
    - Self-review threat – acting in a significant capacity in the delivery of the assessment services where IIS has provided a significant role in the design and implementation of processes/systems and internal controls.
        - IIS did not design or implement processes/systems of internal controls
        - IIS provided assessment and advice only.
    - Self-interest threat – a financial interest or other interest will inappropriately influence IIS or team members judgement.

- IIS has monitored issues and risks with doing additional services, like the Privacy Impact Assessment for the S41 PID, and agreed they were aligned services, and not impactful from a value perspective vs. the breach services
- Direct active supervision of IIS staff by two IIS partners
- Determining professional fees for any additional services were not in excess of fees for the breach assessment services.

- Familiarity threat – objectivity may be compromised due to proximity and or tenure of NSW Government relationships.
  - Although IIS has a history of providing privacy services for NSW Government, these services have been for a variety of departments and agencies and primarily in delivering privacy impact assessments for individual business processes across a broad range of clients
  - In addition, all relationships were essentially new for the Engagement Director and Principal Consultant, located in Melbourne, so our perspectives were fresh.

The following guiding principles were agreed by DCS and IIS in order to avoid conflicts of interest:

- Open communication between DCS and IIS in relation to any issues or risks
- Timely identification and reporting of potential conflicts to DCS
- A mutual commitment to resolve conflicts in the best interest of NSW government.

IIS's independent expert advisory services are not just about assessing the response with respect to compliance but also distilling key learnings than can help build resilience across NSW Government to prevent, detect and respond to data breaches and to improve practice after such events.

This report is not intended to be a formal root cause analysis of the cyber incident, nor an assessment of the cyber incident response procedural documentation.

2.2 Deliverables

Phase 1: Incident Management Response

- Provide immediate, active and adaptive expert independent advice on privacy, cyber security, organisational resilience, risk management and customer support to the following CITAF workstreams:
  - Incident Discovery and Impact Analysis
  - Stakeholders Engagement and Media Communication
  - IT Security Response and Remediation
  - Customer Engagement and Support
  - Business Processes and Change Management
  - Privacy, Legal and Compliance

- Project Office (PMO).

- Attend daily stand-ups as required by the PMO from 14 May until 9 October.
- Participate in project risk working sessions with stream and team leaders facilitated by DCS Group Risk and Performance (GRP).
- Attend and contribute to Cyber and Privacy Resilience Governance Group (the Group), with Malcolm Crompton serving as an independent privacy advisor (since 28 May and ongoing).

Phase 2: Post Incident Data Breach Review

- Prepare a report that:
  - Maps the actions completed by the different streams' teams since the discovery of the incident until the Incident Management Team is stood down.
  - Highlights actions taken by DCS/SNSW in response to the breach, identifying both positives and areas of improvement against various guidelines (including the OAIC data breach response guidelines, IPC data breach guidance for NSW Agencies and the NSW Cyber Security Policy).
  - Assesses the incident management against DCS/SNSW customer objectives, support procedures, and customer support best practice (i.e., the 'customer journey').
  - Summarises the lessons learned from the breach response daily engagement, workshop discussions, stakeholder interviews and documentation reviewed.
  - Recommends actions to enhance privacy and security compliance, risk management, customer outcomes and organisational resilience.

2.3 Methodology

IIS takes a practical and strategic approach to its reviews and worked closely with CITAF and DCS/SNSW leadership at all stages.

IIS's approach to the post data breach review has entailed reviewing documents, interviewing key stakeholders, facilitating lessons learned workshops and conducting high-level data breach benchmark research. Further information in relation to methodology can be found at Appendix A.

2.4 How to read the report

Section 3 of the report is descriptive and provides contextual information about SNSW and the cyber incident and resulting data breach.

Sections 4 to 6 set out IIS's findings on the data breach response:

- *PART A – Response team and governance and other key participants*
  Reviews the operational, governance, escalation and communication arrangements that were set up in response to the data breach.

- *PART B – Adherence to regulator guidance and SNSW data breach response plan*
  Assesses extent to which DCS/SNSW's response followed the steps prescribed by regulator guidance and its own data breach response plan.
- *PART C – Adherence to customer service best practices*
  Assesses extent to which DCS/SNSW's response aligned with its commitments to customer service and best practice.

Section 7 sets out a brief benchmark conducted by IIS of the DCS/SNSW response against other recent data breaches of comparable scale and scope.

Due to the volume of material reviewed and interviews conducted, not all of the content could be presented in the main body of the report. IIS has included a series of appendices with more information about the report methodology, context to the breach and further detailed findings:

- Approach and methodology (Appendix A)
- Further context to SNSW and the breach (Appendix B)
- Further detail on key participants to the data breach response (Appendix C)
- Examples of media articles relating to the cyber incident (Appendix D)
- Detailed analysis of customer support and experience (Appendix E)
- Record of CITAF lessons learned (Appendix F)

3. Background

3.1 Privacy and cyber security

DCS/SNSW operations, by and large, revolve around managing on behalf of partners a vast amount of personal information (including sensitive information) that, if not protected with strong security measures and handled appropriately, may have significant impacts on people's lives (e.g., risk of identity takeover).

At the outset, it is useful to establish the differences with, and relationship between, cyber security and privacy as both are considered in this review. It is important to ensure a clear and consistent understanding across agencies to prevent misallocation of responsibilities or inadequate protections being implemented.

The fields of privacy and cyber security have been converging. IIS defines the two terms as follows:

- Privacy – Is concerned with the collection, use, disclosure, retention and protection of personal information in accordance with certain principles (which may be found in law) as well as broader notions of what is considered appropriate and expected by citizens.
- Cyber security – Is concerned with the protection of IT systems, networks and information (including personal information) from malicious attacks.

Maintaining good cyber security is a necessary but only one component of maintaining privacy. Using a bank vault analogy, cyber security relates to the bolt, doors, access codes and surveillance systems that are part of the construction of the vault, whereas privacy relates to what is stored within the vault. An entity can have the world's best cyber security practices to protect its personal information, but still should not have collected it in the first place or should not have used it in a way that contravenes the use limitations in privacy law or its customer's expectations.

Nevertheless, in our increasingly connected and digital world, it is important to have both – that is, ensuring that personal information is collected and handled properly while also ensuring that the networks and systems that hold the information is protected.

This review is primarily concerned with privacy (in particular, the aspect that relates to incident response pertaining to a large breach of personal information), which in turn is influenced by cyber security practice.

3.2 SNSW functions and customer services

SNSW is an NSW Government executive agency that delivers improved one-stop-shop services for customers, partner agencies and businesses, making it easier for customers to access government services online, over the phone or face-to-face through SNSW Centres across NSW. SNSW is the single service provider for transactional services.

SNSW offers a broad range of NSW government agency services on behalf of lead NSW government agencies. These services include: registration of births, deaths and marriages; drivers' licenses and registration of vehicles; education services; and registration of businesses to name a few examples.

SNSW front-line personnel handle a vast amount of personal information (some highly sensitive) on behalf of the government partner agencies and their customers.

As the shop-front for all of NSW government, SNSW's priority is to ensure that customers receive the best services and support as it strives to be a distinctive leader in the provision of government services.[1] SNSW is customer-centred and seeks to innovate in not only the kinds of services that it provides but the way that they are delivered – namely, to be accessible through a choice of channels and that delivers a positive and enjoyable customer experience.

This is in line with and informed by the NSW Government's *Beyond Digital*[2] NSW Customer and Digital Strategy. The vision behind the strategy is 'delivering smart, simple and seamless personalised services available from anywhere.' SNSW operates with the following Customer Commitments that come from the Digital Strategy: (i) easy to engage; (ii) act with empathy; (iii) respect my time; (iv) explain what to expect; (v) resolve the situation; and (vi) engage the community.

SNSW's culture of innovating quickly and delivering digital services is built upon an agile project methodology. The agency is supported by a leading project management team and necessary resources/tools with extensive experience to stand up the necessary task force to deliver products and services. Such internal capability was put to good use as part of the cyber-incident and data breach response.

The 2019 Machinery of Government changes led to SNSW corporate support functions (such as legal, people & culture, privacy, risk) being centralised into DCS. Every corporate service area underwent structural change to integrate corporate services roles from SNSW and other entities into the equivalent functions in DCS. Since then, the GRP team members have been working to support SNSW's governance and risk needs as SNSW has tackled the dual challenge of delivering new programs as well as providing services to support citizens impacted by natural disasters and the COVID-19 pandemic.

3.3 Cyber and data breach incident

In March, SNSW was the victim of a criminal cyber-attack. Initially, this was reported to SNSW Cyber Security team after a high volume of spam emails were delivered into a range of users within SNSW. The incident was identified as a phishing attempt. The email was purged from staff mailboxes and newsflashes posted to all staff via the contact service desk to reset their password if they clicked the link in the message body. A subsequent event was discovered on 14 April when over 2,000 internal SNSW employees received an email from an internal employee's email address. SNSW Cyber Security Team identified this as a Business Email Compromise (BEC) and reported the event to DCS CISO and Cyber Security NSW.

[1] https://www.service.nsw.gov.au/system/files/2020-01/25660_AnnRpt_18-19_FINAL_ACCESS.pdf

[2] https://www.digital.nsw.gov.au/article/beyond-digital-our-new-nsw-customer-digital-strategy

SNSW and DCS engaged an independent cyber forensics firm, 'Crowdstrike' to investigate the incident. During the investigation Cowdstrike produced a technical report containing evidence of suspicious login activity from the user's mailbox used in the BEC and another 47 staff accounts. Through further analysis, on 21 April, Crowdstrike determined that 47 staff email accounts were accessed, and mailboxes synchronised to a remote server via the IMAP protocol.

SNSW enforced password resets of the compromised accounts and engaged DCS Governance and Risk and Cyber Security NSW to report a data breach to IDCARE, the NSW Information and Privacy Commission (IPC) and the federal Office of the Australian Information Commissioner (OAIC).

On 26 April, DCS migrated the SNSW email domain and staff email to the DCS Microsoft Office 365 Tenant. SNSW and DCS implemented a range of controls to contain the incident, including enabling and enforcing Multi-Factor Authentication (MFA), upgrading the DCS Microsoft Office 365 instance to 'E5' licensing for advanced security features including active Risky Login Blocking and disabling Legacy Authentication protocols. SNSW and DCS then engaged an independent forensic IT investigation to assess how many customers have been affected by the breach through analysis of the mailbox contents.

The following categories of information were compromised in the data breach:

- Financial details (e.g., bank account details, payment cardholder number, transaction history, credit report)
- Tax File Numbers (TFN)
- Identity information (including Centrelink Reference Number (CRN), passport, driver license, birth certificate)
- Contact information (including home address, phone number, email address)
- Health information (including medical forms, patient notes, medical certificates)
- Other sensitive information (including sexual orientation, political opinion, religious views, racial origin, etc.)
- Staff/HR information (including sensitive employment information such as disciplinary matters and health information).

Some further statistics on the breach include:

- 730 GB of data exfiltrated
- 3.8 million documents compromised
- Up to 186,000 customers whose personal information was breached
- 10 government agencies impacted (six in NSW and four Federal)
- At least three key IT systems had to be designed and deployed in response to the breach (NUIX platform, SNSW Salesforce, IDCARE portal)
- A total headcount of internal and external totalling 422 people were working either full-time or part-time on the response and remediation of the cyber-attack – 70 were directly involved

in the taskforce core team; most of the others worked on data forensic analysis and Hypercare customer support

- Notification is expected to be completed eight months after the first attack
- As Service NSW's response to this breach was ongoing at the time of this review, the full cost of its response was not known. However, it is expected to be excess of $30 million.

At the time of writing, NSW Police has reported that there has not been evidence of SNSW data circulating on the Dark Web and there has not been any significant increase in scam activity (such as someone pretending to be SNSW). IDCARE reported that it was only aware of 26 cases of reported data misuse, but it is far from clear whether the reports arose from misuse of data from the SNSW breach or elsewhere. However, it is also known that cyber-crime syndicates will collect information from different sources to piece them together and exploit them over time. SNSW may not know the extent of data misuse stemming from the breach for some time, if ever.

For further information related to SNSW and the data breach context, refer to Appendix B.

4. PART A – Response team, governance and other key participants

4.1 Response Team: Cyber Incident Task Force

In response to the identification of the cyber incident, a *special purpose team* called CITAF was established to quickly carry out the necessary response actions to reduce the potential impact of the data breach and to:

- Undertake forensic analysis of cyber incident and customer impact (**completed**)
- Provide the necessary care and support for any impacted customers (**ongoing**)
- Meet agency obligations under legislations (**ongoing**).

CITAF decided to follow the four key steps of the OAIC's guide to managing data breaches[3] (the 'OAIC guidelines') – Contain, Assess, Notify, Review – and also reviewed NSW IPC guidance[4] (as for most purposes DCS/SNSW is regulated by the NSW IPC and the PPIP Act.

The scope, command and control, governance and deliverables were documented and formally agreed.

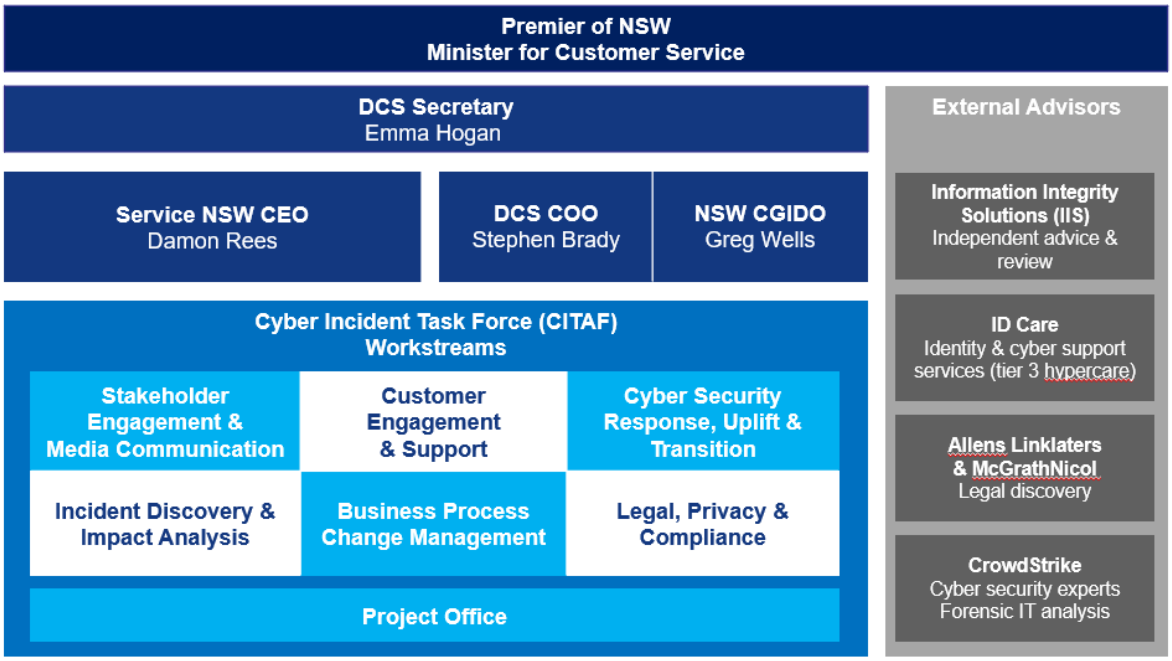


Figure 1: Composition of CITAF (provided by PMO)

[3] https://www.oaic.gov.au/assets/privacy/guidance-and-advice/data-breach-preparation-and-response.pdf

[4] https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies

IIS observed that:

- As required by the OAIC guidelines, each stream had the roles and responsibilities established and documented as soon as the response team was stood up (see Appendix C for more detail). The core CITAF workstreams were also supported by further internal DCS/SNSW working groups or sub-groups (such as People & Culture) and external cyber forensic, legal and privacy advisors.
- The key deliverables of the taskforce were agreed (see Appendix C for reference). Among them are sharing lessons learned and develop a Cyber and Privacy Response Playbook that aims to guide NSW Government teams so they can prepare, respond, prioritize actions and engage the right people during a data breach response. The Playbook will collate the learnings accumulated from previous cyber and privacy incidents, as well as critical considerations raised by work stream leads. Finally, the Playbook will provide a structured, high-level approach to support the different work streams that need to be engaged when responding to future data breaches, regardless if they result from a cyber security incident, ICT misconfiguration, human error, or other means[5]
- The CITAF core team and all Hypercare team members completed privacy training facilitated by IDCARE, which provided guidance to the response team in relation to what to expect in relation to the customer journey and customers' emotional state.
- A decision making and action log[6] was managed by the PMO and a central repository was made available for data sharing across team members. An event register and document register were also managed and made available to CITAF.
- CITAF was agile in the on-boarding of external support third party providers at the early stages of the response and coordination with critical agencies such as NSW Police, the Australian Tax Office (ATO), NSW Register of Births, Deaths and Marriages (BDM) and Transport for NSW (TfNSW).
- There was a process to workshop possible options and solutions. Decisions were documented and briefing notes approved.
- Project risk management sessions were held (including risk-discovery and deep dives), facilitated by GRP team. The Project Risk Register was handed from GRP to the project team in September 2020. Significant risks were reported to CITAF command and control lead as part of the decision-making process and ongoing monitoring. Specific risk assessments were completed as part of the working groups to assist decision making and approval of briefing notes. Stream leaders relied too often on the PMO office to lead or follow up on actions agreed.

[5] This definition comes from PMO office.

[6] IIS did not review the final decision/action log status at the time of writing this report. IIS reviewed the initial version created by PMO.

- The extent of the data breach was not known for a period of time (while investigation and forensic analysis were being completed). Resources deployed for the response were based on the information available at a point in time.

IIS findings:

Initial CITAF composition did not include People & Culture, the business unit that has played a significant role in completing the risks assessment and notification of employees. Furthermore, CITAF did not document changes to its composition, roles and responsibilities.

The effort required to respond to the breach was evolving. Resources were increased during the response as the extent of the breach and complexity was being discovered.

IIS considers that once established, the CITAF was a good response model and helpful in coordinating the breach response.

In discussions with CITAF team members, on several occasions they raised the issue that some areas had to 'fight' to get extra headcounts or that the people had to work long days and weekends continuously for too long. The CITAF was further challenged as it took a long time to fully assess and understand the scale and complexity of the work required and personnel involved in the response also had to perform their BAU roles. Teams were overstretched and overworked for a long period of time, including working long hours and weekends. As a result, some staff members had to take sick leave. Staff moral and fatigue levels were not formally monitored during the length of the response despite the risk was highlighted in the Project Risk register.

The length of the response had a significant toll during the project. Organisational resilience best practices depend on the human factor of the response team and this is challenged by the physical and mental fatigue of events like this with such a long tail.

Action 1: Secure dedicated response team

Agree on a protocol to secure dedicated response team for future events of similar nature and scale (in particular if novel to the organisation). Provide guidance to when staff should be drawn out of BAU roles, provide them with necessary training and enable them to move quickly to a dedicated response team.

Priority: Current & Playbook

Action 2: Document changes to response team composition and roles

2.1 Include People & Culture as part of response team governance structure. Revisit team composition once the full extent of the cyber incident and data breach has been confirmed.

Action 2: Document changes to response team composition and roles

2.2 Document and communicate changes to participants if/when there are changes to the composition of the response team and working group.

Priority: Playbook

Action 3: Plan for healing and recovering

Allow the CITAF team and support functions to take additional time off (as indicated by Shane Fitzsimmons (Resilience NSW), after the event you need to allow for the team to heal and recover).

Priority: Current

Action 4: Monitor staff attrition and morale levels

4.1 People & Culture to monitor reasons for sick leave overall and attrition in the coming months to further understand the potential knock-on effect that the cyber incident and data breach had on staff working as part of CITAF or staff whose personal information has been breached.

4.2 Report on this to assist with further insights into the data breach scale.

Priority: BAU/Project

Action 5: Consolidate stakeholders' relationships

5.1 Invest in future response services: Consolidate stakeholders' relationships and establish expert networks that could be re-activated quickly in the event of future incidents. This could include forensic analysis partners, mailing house, etc.

5.2 Through the SNSW Partnership group, set up a cross-agency data breach response group to leverage lessons learned, consolidate future response to incidents and participate in cyber incident and data breach desktop and simulation exercises.

Priority: BAU/Project & Playbook

IIS also noticed failures with handling project documentation correctly as per SNSW policy. After several months we still observed project documents not properly classified as per the NSW document classification guidelines,[7] documents being exchanged with external advisors using unsecured

[7] https://data.nsw.gov.au/information-classification-labelling-and-handling-guidelines

methods (email and unencrypted) and staff unaware of secure data transfer methods in place (GovConnect NSW).

Action 6: Check point on data handling procedures

6.1 Train/debrief data breach response team on documentation classification procedures and methods of data exchange. Undertake spot check reviews to ensure that policies and procedures are being followed.

Priority: Current

6.2 Emphasise the need for the data response team to be familiar with data handling procedures and secure methods to exchange documents with third parties.

Priority: Playbook

4.2 Data breach governance – Cyber and Privacy Resilience Governance Group

The Cyber and Privacy Resilience Governance Group (the CPRG Group) was established in May 2020. The CPRG Group is chaired by the DCS Secretary and co-chaired by the DCS COO. The key purposes of the group are to:

1. Provide executive-level leadership and oversight of response and recovery activities related to the cyber security incident and the data breach.
2. Lead the development and implementation of an ongoing DCS Cyber and Privacy Incident Recovery Framework.
3. Build resilience against major cyber security and privacy breach incidents across the DCS cluster and the NSW Government sector more generally to significantly reduce the risk of future incidents.

The work and focus of the group are being delivered in three key phases under the name of Project Trust:

- Phase 1 – Immediate response and recovery priorities – May to August 2020 (completed)
- Phase 2 – Establishment of Ongoing Resilience Framework/Pathway – July 2020 to June 2021 (ongoing)
- Phase 3 – Lookback, review and evaluation – (TBC).

In addition to the delivery focus noted above for each phase, the CPRG Group drives the overarching goal of building and strengthening resilience across the DCS cluster. At the time of writing this report a total of nine meetings have been held.

IIS findings:

IIS considers that the CPRG Group was a good governance model for overseeing the response, challenging the options presented, testing decisions and looking forward to future improvements.

IIS has observed that the CPRG Group played a key role during the last seven months to raise cyber security and privacy awareness across DCS/SNSW leadership team. This included highlighting the extent and scale of the threat that the type of compromised data may represent, such as identity takeover. IIS understands that as part of Project Trust, a specific workstream has been created to raise cyber and privacy awareness across DCS. IIS commends this initiative and encourages DCS to continue working with Cyber Security NSW to raise leadership awareness across the cluster.

4.3 Other participants to the response

Details of other participants to the response can be found in Appendix C. Key federal and NSW agencies that supported DCS/SNSW efforts were Services Australia, NSW Firearms Registry, BDM, the Cybercrime Squad within NSW Police, NSW Office of the Children's Guardian, TfNSW, NSW Data Analytics Centre (DAC) and iCare.

4.4 Decision-making triggers

The DCS Cluster Crisis Controller role sits within the remit of the COO. As part of the data breach response a special purpose response group was invoked (the CITAF). It is important to note that the Crisis Controller was involved in the decision making around the formation of CITAF as the primary response group.

The Crisis Controller did not trigger or declare a crisis. IIS was informed that 'crisis' within the DCS Crisis Management Framework may be triggered only for business disruption events related to power outages, IT/Technology failure, building unavailability, loss, etc.

On the other hand, IIS notes that SNSW has its own Business Continuity Framework and Crisis Communication Plan that classifies privacy or security breaches that affect potential personal safety and wellbeing of customers as a 'Major Crisis'. However, these documents were dated to 2013. When inquiring about the testing and rehearsal regime, IIS was informed that no testing and rehearsal of a data breach response was completed prior to the event. In discussions with CITAF team members, there were inconsistencies with how the incident was classified.

When responding to events or incidents, the 'label' matters in terms of activating certain response pathways as well as to ensure that all response members are on the same page. IIS considers that in light of this incident, now is a good opportunity for DCS and SNSW to revisit or recommit to existing plans for updating relevant documents and ensuring that they are aligned to the extent possible.

Regardless of the definition of 'crisis', IIS observes that as a matter of practice:

- The cyber incident and data breach resulted in disruption for the internal operation within parts of DCS Corporate Services, SNSW and affected agencies, along with significant costs

to the NSW Government. The consequences of the breach to SNSW brand and reputation are still unknown.

- Significant resources were stood up and applied to the project, from multiple DCS and SNSW streams – this made up for DCS/SNSW's initial low level of readiness to respond to a breach of this size and complexity.

Action 7: Review DCS and SNSW crisis triggers and touch points

7.1 Consider adding major data breaches into the DCS Crisis Management Framework taking into account the particularities of each agency. Harmonise across the cluster where possible.

7.2 Ensure ISMS, Incident Management and Crisis Management Frameworks between DCS and SNSW are aligned and interconnected.

Priority: **BAU/Project**

Action 8: Review and update SNSW Business Continuity and Data Breach Response Plans

8.1 Review and update the BCM Framework, Business Continuity Plans and Data Breach Response Plans, taking into account lessons learned during 2019-2020 real events.

8.2 Implement a regular testing/rehearsing and training regime.

8.3 Consider a centralised major breach response function for Whole of NSW Government.

Priority: **BAU/Project**

4.5 Cyber incident and data breach communication strategy and delivery

A team was established to manage the breach response communications aspects comprising: Communications/Media (Comms (both internal and external), messaging, media management, PR, social etc.), engagement (partnerships, stakeholder etc), and GRP (escalations, complaints and compensation requests).

The team developed and is executing a data breach communication plan, which includes:

- External and internal communications roll out – phases and key messages (three key phases)
- Communication approval pathways, phases, and activities
- Stakeholder groups and who is responsible for liaising with external stakeholders

- Risks (i.e., media leaks, brand damage, confusion, staff morale, weakened partnership trust) and risk mitigation plans as well as success measures
- Schedule of what communications will be released and when, as well as a range of key 'artefacts' such as a media release, fact sheets, holding statements and Q&As
- Coordination of internal communications such as briefings series for people's leaders, leadership site visits, internal awareness campaigns (i.e., essential mentions) and live chats on workplace and Q&A with SNSW CEO
- A single source of truth and consistent narrative when responding to official correspondence
- CEO and subject matter experts were made available for media debriefs.

DCS/SNSW was responsive and numerous additional partnership debriefings have been hosted as well as debriefs with cyber security stakeholders such as the Australian Cyber Security Centre (ASCS) and NSW cluster CISOs.

External communication strategy and associated risks:

The SNSW CEO envisaged at the beginning of the response that implementing the right communication strategy for impacted customers was going to be complex. The strategy must balance the need for timeliness against creating additional risk by going out too soon when the full picture (both overall and for each individual) was unknown, with the potential for creating additional anxiety or increasing the risk of scammers. The priority was placed on customer safety and protecting customers and employees from further harm. Following professional advice, CITAF agreed that notification would only happen when "accurate and complete information" was available about the specific documents breached for every customer. The aim was to reduce customer anxiety, confusion and risk of excessive call volumes. The communication strategy was aligned with the notification strategy. As such the communication strategy during the initial months was aimed at keeping public communication about the event general and the 'noise levels' around the data breach quite low with the aim of avoiding excessive media attention until notification letters have been released to reduce the risk of scammers and ensure the Hypercare team was ready to provide the right level of customer support. A series of media releases and web updates were made and media enquiries fielded.

See Appendix D for links to media articles relating to the cyber incident and data breach.

IIS findings:

Overall media coverage was relatively low key and limited. There have been some harsh press headlines, but the lack of consumer harm event stories surfacing has largely minimised the coverage.

By that measure, the external messaging was successful. SNSW acknowledged its mistakes and was humble, transparent and consistent, and its messaging was easy to read. The simple message of 'we will inform people individually when the data is available' appeared to work. SNSW also took the opportunity to provide guidance to customers on proactive steps to protect themselves along the journey. This included website updates and initial guidance on 14 May and followed up on 7 September with a video clip. However, IIS considers that the guidance to customers on taking proactive steps to protect themselves was light in content and could have been emphasised at every update along the way.

Nonetheless, the communication team believes they have been fortunate. They were deeply concerned about the customer impact and risk and thus equally concerned that despatch of notifications has been slower than preferred. They also were concerned about alarming more customers than absolutely necessary. They believe SNSW has been fortunate insofar as there has not been a major harm event which would have triggered large scale media or consumer response. Media cycles in this case would have driven more significant demand on the call centre and/or more customer dissatisfaction.

IIS also observed that:

- In the early weeks and months of the breach BAU resources were gradually drawn in to support the breach response. It was only after some time that a Director of Comms and Strategic Projects was brought in to 'help pull the strings together'. The BAU/operational nature of the business and the existing significant pre-breach BAU workloads meant the team was stretched. Managing a communication response like this is effectively a large-scale comms project and requires an (non-BAU) operating model with additional resources, roles and a budget that is triggered early as the major data breach crisis is confirmed.
- There was limited attention to cybersecurity specialist media and proactive preparation for potential questions to be asked on the subject.

Action 9: Enhance Communication Data Breach response

9.1 Conduct a full debrief and collate lessons learned just on media.

Priority: BAU/Project

9.2 Create a suite of media templates, IP tools and governance models to support the team in managing future data breaches (recognising that they need to be adapted and not 'copy and pasted' for re-use).

9.3 Define alternative models for different communications objectives and event scenarios and develop aligned operating models for different types and size of events with budget etc. across SNSW and partner agencies.

9.4 Design a process that classifies events in order to trigger appropriate, trained additional resources, roles and budget for comms/media management.

9.5 Ensure strategic communications is engaged as part of the assessment and the strategy process in all breach events early in the breach or crisis event.

Priority: Playbook

Action 10: Secure specific media training

10.1 DCS media team to design specific media training for different circumstances to trusted media leaders across DCS/SNSW, including standing in front of a critical audience.

Action 10: Secure specific media training

10.2 Ensure the program is maintained as part of the annual learning program.

Priority: BAU/Project

Internal communication strategy:

SNSW deployed an internal communication strategy led by the SNSW CEO to answer the different needs of all staff members as employees and customers, to inform them ahead of public media releases and keep them informed of the data breach response progress.

Internal communication activities, both pre-notification and post-notification, ranged from town halls and site visits, live chat videos, emails raising security awareness, individual meetings and tailored notifications.

Many staff had sensitive employee (e.g. disciplinary and or health) information breached and because of this, were notified personally before letters were received. This created chatter and also meant staff who had not been notified were surprised to get a letter. Additionally, they were upset about being notified in the mass notification rounds by letter, having expected a personal outreach consistent with their role as part of the 'SNSW family'. Management now believe a series of coordinated manager huddles would have been a more controlled way to communicate key messages and address issues before the rumour mill took over and negative sentiment increased.

The SNSW CEO and executive team held many useful staff briefings which have been well-received. However, with hindsight these potentially happened late in the process and/or initially were not as widely attended as a peer or staff briefing process would have achieved. IIS has been informed that the Workplace Q&As were attended by many SNSW staff as a live event and have been kept on Workplace for continued viewing by staff who were unable to watch live. The three videos available currently have 760, 1,600 and 1,200 views[8]. IIS was informed that by the time this report was finalised management has already implemented the learning.

IIS findings:

Despite the efforts deployed, the internal communication plan did not work as effectively as planned. SNSW is already fully aware of this and working towards sustaining the trust of its employees.

Action 11: Prioritise internal communications

11.1 Develop and agree on a bespoke and tightly coordinated staff communications program utilising cascading manager briefings, a leadership communication overlay and HR/DCS channels for support to ensure announcements are conducted prior to mass letters being released.

[8] The video were launched on 9, 22 and 28 September.

Action 11: Prioritise internal communications
11.2 Provide ongoing communications to keeping staff informed of options available to them.
Priority: Current (in progress) & Playbook

5. PART B – Adherence to regulator guidance and SNSW data breach response plan

As noted earlier, the CITAF team agreed to align its response strategy in line with the OAIC guideline. IIS was also asked to consider how the response adhered to SNSW policy (in particular, its Data Breach Response Plan (DBRP)) and the NSW IPC's Data Breach Guidance for NSW Agencies.[9]

At the outset, IIS notes that the SNSW DBRP and regulator guidance provides high level steps for *what* needs to be considered or completed. However, they do not provide detail on *how* the steps should be completed. The DCS/SNSW response to the data breach is a unique case that could be described as a 'hybrid' approach. The CITAF followed OAIC guidance but also innovated during the process to ensure continuous improvement and refinement of the response, with the aim of creating a 'gold standard' that other government agencies could leverage and learn from.

IIS sets out the following sections in accordance with the high-level steps recommended by the OAIC guide. For each step, we summarise the requirements that come from the regulator guidance and SNSW DBRP, describe SNSW's actions, then make a finding (exceeded / met / partially met / did not meet).

Overall IIS findings:

DCS/SNSW has mounted a significant effort to respond and recover from the data breach, by remediating the initial and other vulnerabilities while adapting to the challenges facing the organisation and incorporating lessons learned via other crises, floods, bushfires and COVID-19.

In relation to the regulator guidance, most of the prescribed actions in the Contain, Assess and Notify phases have been met or exceeded. There was one exception – namely, 'notify individual and organisations as soon as practicable'. The Review phase is currently underway and the CPRG Group will have to monitor progress.

IIS understands that as part of Project Trust, DCS/SNSW is initiating a privacy uplift and that the SNSW DBRP will be amended accordingly taking into account the findings of this report and lessons learned by the CITAF team.

[9] https://www.ipc.nsw.gov.au/data-breach-guidance-nsw-agencies

5.1 Data breach response timeline

While the four OAIC steps were used as a guide, IIS notes that the data breach response followed an agile methodology and therefore steps were conducted concurrently in some instances along the journey.

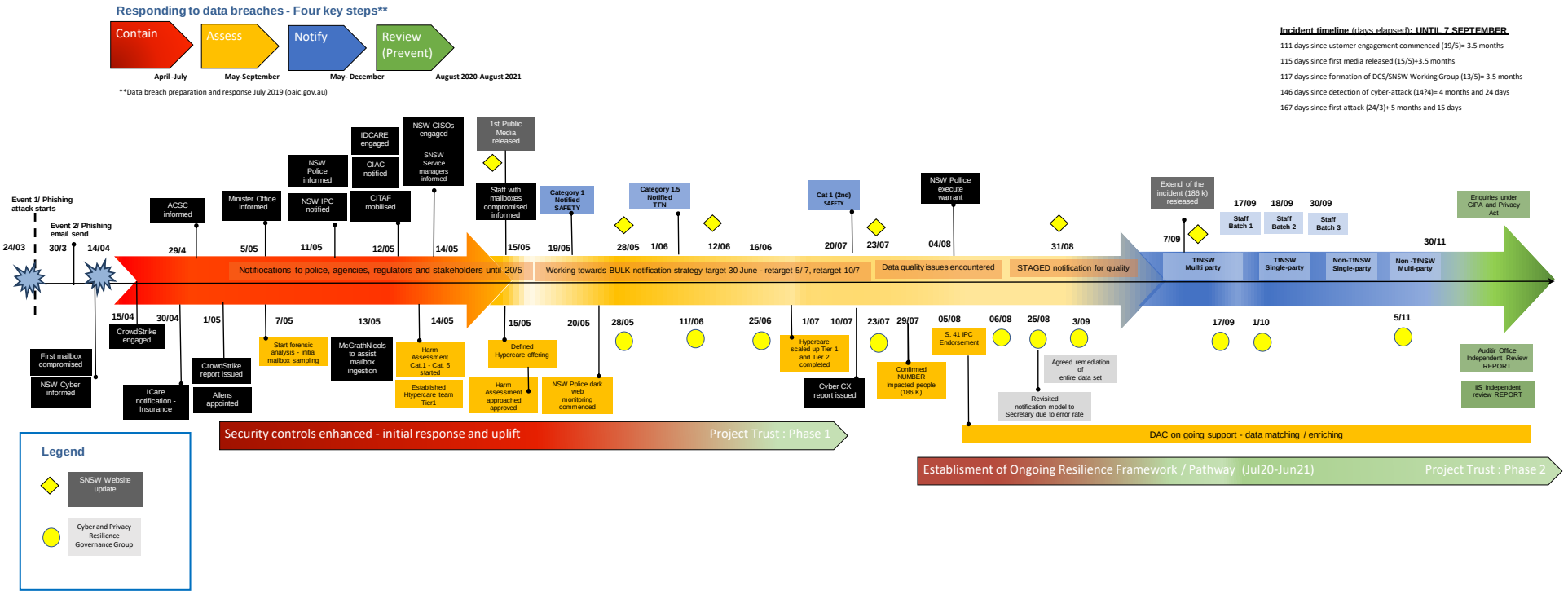


Figure 2: Data breach response timeline (IIS)

5.2 Step 1: Contain

Overview of requirement and summary of actions completed	Finding
Take all necessary steps to contain the breach to prevent any further compromise of personal information (IPC, OAIC, SNSW). Preserve evidence.	Exceeded **Met** Partially met Did not meet

As soon as the SNSW account takeover phishing attack was identified, a forensic provider (CrowdStrike) was engaged to determine evidence of data exfiltration. Relevant DCS support functions (e.g., GRP) and SNSW leadership were notified, as well as Cyber Security NSW, allowing for close involvement and observation of the recovery process to inform response to future incidents.

At the same time the DCS/SNSW incident response team undertook a series of immediate actions to limit the breach and activated the incident response teams:

- The accounts of the user sending the suspicious emails were disabled in both Office 365 and Active Directory and a forced reset of passwords was applied when the accounts were re-activated.
- Office 365 configuration automatically placed a block on the account of the user sending the suspicious emails, to prevent any further outbound mail.
- Mail rules created by the malicious actor were reviewed and removed.
- Incident tickets were raised with security service providers to run scans across user workstations to check for instances of any malware and put URL blocking in place and request access reports to identify users that clicked on the link.
- Automatically purged phishing emails from all SNSW users' mailboxes (60-day functionality).
- Advised all SNSW staff through general communication channels to report and delete the email if received.
- Applied password resets to other users that clicked on the malicious link as a precaution and preventative measure.
- Completed the rollout of MFA to key systems and applications to strengthen ICT security controls.

When preliminary findings were confirmed by the forensic provider in relation to the scope of the data exfiltrated on 24 April, the Incident Response team informed and extended the involvement to the DCS Legal, Privacy and Audit teams. At that point, DCS/SNSW suspected this would be a significant data breach and sought informal input from. Equally important, the team kept Cyber Security NSW informed of all indicators of compromise (IoC) and learnings from these findings in order to benefit the NSW government cyber ecosystem.

Once the final forensic report from CrowdStrike was made available on 1 May, DCS/SNSW:

- Designated SNSW CEO as the individual in charge and DCS COO as the co-chair
- Set up the data breach response team (CITAF) and in particular:
  - Appointed Allens as forensic investigator
  - Established an initial dedicated privacy team (Hyper Care) to support customers and engaged IDCARE and IIS as external privacy advisors
- Escalated matters as relevant within SNSW agency, cluster and to key stakeholders

External organisations notified included NSW Police, NSW IPC, OAIC and ATO. Other key stakeholders and partnership agencies were also notified including NSW cluster CISOs and the ACSC.

SNSW has worked closely with law enforcement and specialist cyber security services as a part of the ongoing investigation. The Cybercrime Squad within NSW Police initiated the monitoring of the Dark Web which is still active at the time of writing this report.

IIS findings:

IIS considers that more time could have been saved during the incident management escalations to internal and external stakeholders. The lack of readiness resulted in initial confusion, which was aggravated by the fact that for some time DCS/SNSW did not know the true extent of the cyber incident and data breach.

In discussions with DCS/SNSW staff, it was mentioned to IIS that some staff had doubts and it was not clear to whom they should escalate relevant information. As previously indicated SNSW was underprepared and the first few weeks were mainly focused on discovering and containing the full extent of the cyber incident and data breach. Up to date documentation, detailed list of stakeholders and regular testing and rehearsal of escalation paths could have assisted with clarifying and speeding up the process.

In addition, the NSW Police Cybercrime Squad was informally informed (verbally) early in the process, but the formal communication (written) was completed a few days later. Leanings already noted by SNSW are the importance of following up informal notification with a formal notification as soon as possible. This is an important requirement before the Squad can begin to investigate if an incident has occurred, the scale and the options to be considered.

Action 12: Review SNSW incident and data breach escalation procedures
12.1 Review the SNSW Information Security Incident Management Policy and DBRP. Incorporate learnings from this review and overall response. 12.2 Ensure response team structure, details and escalation sequence are clear and agreed. 12.3 Test the escalation procedure on a regular basis. **Priority:** **BAU/Project**

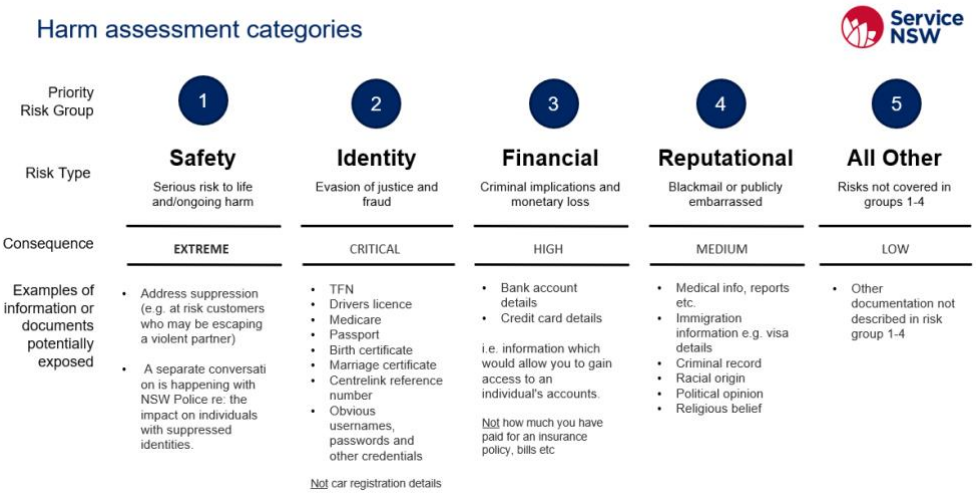
5.3 Step 2: Assess

Overview of requirement and summary of actions completed	**Finding**
Assess whether the data breach is likely to result in serious harm. Understand the risk of harm to affected individuals (OAIC)	Exceeded **Met** Partially met Did not meet
A preliminary harm assessment was carried within 48 hours, 15 days after the cyber incident forensic report was issued. It was based on type of document, personal information exposed and the corresponding response plan (including thinking about what can be done ahead of time for the customer, what can be done by the customer and what risks can't be addressed). Five categories of affected customers were created: 1-Safety/Extreme, 2-Identity/Critical, 3-Financial/High, 4-Reputational/Medium, 5-All Other/Low. The categorisation levels were developed taking into account the	

Overview of requirement and summary of actions completed	Finding

considerations set out by the NSW Privacy Commissioner and with the advice of IDCARE. The approach to notification is also consistent with the principle of minimising risk to customers.

A total of 98 personal information markers where identified.



Once the extent of the number of impacted customers was confirmed, significant data quality errors were found in the forensic work and a vast amount of time was dedicated to data remediation.

At the time of writing this report, the assessment process was still in progress due to the recurrent error rate issues encountered with the initial results.

Decisions were taken at CheckPoint and referred against SNSW harm and risk assessments. These were then documented in the Decisions Register.

IIS findings:

DCS/SNSW implemented a risk assessment model based on the harm assessment completed by IDCARE. The model applied allowed customers at extreme risk to be formally notified early (within weeks) and for safety measures to be put in place. IIS considers that SNSW's focus on reviewing the higher end of the risk spectrum cohort (Category 1 and people with TFN) and reducing the error rate was consistent with assessing the risk for individuals who could be at serious harm.

As IIS indicated at the end of the Executive Summary, DCS/SNSW encountered further issues in early November. Due to recoverable items from mailboxes (deleted emails) included in the forensic analysis, there were inaccuracies with DCS/SNSW's assessment that led to notifying individuals who were not impacted by the breach.

During the workshops conducted by IIS for this report (see Appendix F), the CITAF team recorded several lessons learned from the assessment process:

- Better understand the 'problem' that DCS/SNSW was facing with unstructured data. The forensic analysis taught a big lesson for how agencies should approach this in the future, namely, to have a clearer idea and expectation when it comes to the end-product coming from the external party conducting the data analysis.
- Brief the forensic team conducting the data analysis on the types of transactions and procedures conducted by the agency.
- Consider having an agency person supporting the forensic work and complete quality assurance along the way.
- Set realistic deadlines for the data analysis process, taking into account the complexity of the incident and the fact that SNSW did not have a single view of customers.

Overview of requirement and summary of actions completed	Finding
Take all appropriate steps to limit the impact of data breach. Consider if any remedial action can be taken to reduce any potential harm to individuals (OAIC)	Exceeded **Met** Partially met Did not meet

DCS/SNSW leadership team approached privacy and cyber professionals (IDCARE, IIS, Cybercrime Squad within NSW Police) and relevant document issuer agencies to further assess the impact to individuals.

A response plan was developed. SNSW adopted the following recommendations:

- Established a dedicated Hypercare team to support customers 24 hours ahead of the first media release and created a webpage related to the Cyber Incident to build a response approach to address immediate needs or distressed customers who were concerned.
- Worked with partner agencies including BDM and TfNSW, and with federal agencies such as ATO
- Free credit rating check for impacted customers
- Representation to Revenue NSW if there is a mis-declared penalty issued
- Replacement of key documents and drivers' licences
- Case Management support in Service Centre for face-to-face authentication (booked in advance)
- Referral to counselling support
- Representation to NSW Police if required.

Entities subject to the Notifiable Data Breach (NDB) scheme are required to conduct an assessment of suspected eligible data breaches and take reasonable steps to complete this assessment within 30 days (OAIC).	Exceeded **Met** Partially met Did not meet

The assessment in relation to the NDB scheme was completed in less than 30 days. As soon as Tax File Numbers (TFNs) were identified as part of the forensics conducted by Allens, DCS/SNSW informed the ATO on 19 May.

Action 13: Re-visit harm assessment when extent of breach is confirmed

13.1 As a matter of best practice should a breach occur in the future, after the initial assessment and once the extent of the data breach has been confirmed, re-visit the harm assessment taking into account the customer journey and the appropriate response for each category of affected individuals.

13.2 SNSW to workshop with staff the main customer types, needs and journeys that came through the system to understand how harm classification drove experience and outcomes to identify any potential groups, variations and options.

Priority: Playbook

Action 14: Plan needs and requirements to complete forensic analysis

14.1 Include in the Playbook (and if appropriate, at a high level in the SNSW DBRP) a plan for how forensic analysis should take place in the future (if needed) and partners to work with.

Priority: BAU/Project

Action 14: Plan needs and requirements to complete forensic analysis
14.2 Consider need for internal forensic capabilities and the role that the DAC could play early in the process. **Priority: Playbook**

5.4 Step 3: Notify

Overview of requirement and summary of actions completed	Finding
Consider whether individuals should be notified (IPC, OAIC, SNSW DBRP); including whether the breach is likely to result in serious harm to individuals.	Exceeded **Met** Partially met Did not meet
SNSW assessed the need to notify based on the result of the harm assessment and in accordance with regulator guidance such as the type of data involved, the significance of the data, the context into which it was breached, the identifiability of the data and the circumstances of the breach. IIS observed SNSW's approach to be consistent with the principle of minimising risk to customers.	
Consider how the notification is to occur (i.e., content and delivery) (IPC, OAIC, SNSW DBRP)	**Exceeded** Met Partially met Did not meet
The notification strategy approach was based on the harm assessment analysis results and professional advice received. Notification approached were tailored to the potential risk and needs of affected person: For customers: • Early notifications via phone call were conducted for people in Categories 1 and 1.5 (TFNs) due to heightened risk. • For individuals in Categories 2 to 4, notifications were conducted by registered person-to-person post. SNSW engaged with NSW Police Cybercrime Squad to ensure their alignment with proposed approach. Registered person-to-person post was chosen because it further protected privacy (reducing avenues for scammers to approach them) and early feedback from high risk/profile customers who were called, suggested they didn't feel comfortable with an 'out of the blue' call. • DCS/SNSW was strongly advised not to communicate with customers until it could tell them exactly what data was compromised to avoid further harm (e.g., scammers) and damage to customer trust. • For individuals in Category 5, notification was carried out through the SNSW website and media releases due to the low level of harm, which did not justify the increased cost of personalised notification. For former or current employees: • Notification related to compromised TFNs were completed verbally over the phone with a follow-up option to receive a letter via email or post. • For other impacted employees, registered person-to-person post was agreed as the best option. People & Culture and GRP also developed a notification strategy to manage conflicts of interest (for example considering impacted personnel who were working in the Hypercare Teams).	

Overview of requirement and summary of actions completed	Finding

Further efforts in relation to the notification included:

- Notification letters for each group were approved with input from relevant stakeholders including the DAC, Legal, GRP and privacy advisors such as IDCARE and IIS. The letters were framed to empower and inform people and include a call to action to engage with SNSW or IDCARE. The letters also included general advice on how to protect identity and other specific information types. IDCARE indicated that the letters were of a high standard compared to others the organisation has seen.
- The letters and engagement model were revised with:
  - Feedback received from early notifications (Category 1 and 1.5).
  - Feedback received from a customer notification pilot completed for Categories 2 to 4 (i.e., mainly CITAF team members impacted).
- Moreover, notification method was tailored for minors and high-profile individuals, taking into account their own risk factors.

A Quality Assurance process was implemented which included a review of the data received by the forensic firm and assigning a dedicated person to the mailing house.

IIS findings:

We consider DCS/SNSW's approach to be thorough and detailed. DCS/SNSW considered external advice but the final decisions were made by Leadership and recorded by the PMO.

IDCARE confirmed that the notification using personalised letters is consistent with previous breaches of high-risk information.

DCS/SNSW was relatively slow to release accessible online information to guide customers in how to protect themselves – initial guidance was raised on 14 May and there were no further updates until 7 September.

Notify individuals and organisations as soon as practicable, unless it is appropriate to delay notification in the circumstances (IPC, OAIC, SNSW DBRP) **SNSW DBRP: indirect notification, for example through a notice on SNSW's website, should only occur where the individual/s contact details are unknown or direct notification would be prohibitively expensive.**	Exceeded Met **Partially met** Did not meet

Notification was still in progress at the time of writing this report. Examples of challenges that SNSW had to overcome included:

- Working with unstructured data contained across 47 email accounts
- Setting up the systems required for engaging with the customers wanting to contact SNSW (e.g. NUIX, Salesforce, IDCARE portal)
- Obtaining a Public Interest Determination under s 41 of the PPIP Act in order to complete the data matching with BDM and TfNSW.

Once the initial mailbox forensic analysis was concluded, the data review and quality assurance process identified a 40% level of error. Two risks emerged with respect to the poor data accuracy:

- It could result in notifying customers of a breach when this didn't happen
- It could result in failing to notify customers that a particularly important piece of information had been compromised.

Resulting issues with data quality were likely due to a combination of people working at speed and human error which is always an element given the complexity of the data and nature of information that had to be extracted.

As a result, the CITAF reviewed the strategy of bulk notification. On 20 August the CPRG Group drew the conclusion that bulk notification to all customers was no longer a viable option. The CPRG Group considered five options (i.e. no change, fine tune, remediation of entire data set, general notification followed by

Overview of requirement and summary of actions completed	Finding
appointments, hybrid) The approach endorsed and adopted was to remediate the entire dataset and notify customers in a staged approach across a period of 13 weeks (expected to finish at the end of 2020).	
Consider who else may need to be notified – e.g., the Privacy Commissioner,[10] other government authorities (IPC, OAIC, SNSWDBRP) **Although NSW does not have a mandatory NDB Scheme, the NSW IPC encourages agencies, as a matter of best practice, to voluntarily report data breaches to its office and affected individuals, as appropriate.**	Exceeded **Met** Partially met Did not meet
DCS/SNSW informed NSW IPC of the data breach on 11 May and has continued to inform and collaborate with the regulator throughout the data breach response process. Other stakeholders notified include we also notified all affected NSW government agencies, the Cybercrime Squad , Banks as well as the Audit Office of NSW and Minister Office.	

IIS findings:

There are two considerations in terms of assessing DCS/SNSW's notification strategy:

- During the response period – Did it have a defensible decision-making process?
- With the benefit of hindsight – Did it make the right decision in how and when to notify, and what lessons can be learned for the future?

During the response period: IIS considers that DCS/SNSW had a defensible decision-making process and made decisions with customers on top-of-mind and based on expert advice.

DCS/SNSW always took into consideration independent advice it sought it from a range of sources including IIS in our advisory role. We raised the following considerations for the PMO and CITAF team to consider in relation to time and resource management:

- At what point is the money better spent on a general awareness campaign versus chasing the exact people who are becoming more difficult to find and contact?
- Are we getting the balance right between notifying early versus notifying late?
- How long can we continue to interrogate the data while deriving a tangible benefit?

On the balance of all the considerations, including pros and cons of alternative options, DCS/SNSW decided to wait until it could more fully understand data details, issues, and risks. IIS recognises the difficulty of the decision made in complex circumstances and agrees it was a justifiable outcome of the decision-making process.

With the benefit of hindsight: IIS recognises that all parties involved in the notification decision-making process had a slow-boiling-frog problem (including IIS). That is, decisions being made week-to-week and month-to-month may have been justifiable in the moment, but the cumulative effect was the unexpected length of time taken to despatch notifications for categories 2 to 4. For example, it

[10] The State legislation does not have mandatory notification of privacy breaches. However, it is government policy to notify where there is a risk of harm.

would not have been obvious at the four-month mark that notifications would not occur for another four or more months.

IIS observed that the notification strategy was based on professional advice at points in time and driven by dates, assumptions, and best-case scenarios. Going forward, a data breach response team should factor in more 'what if' considerations and contingency plans rather than 'best case scenario' planning.

On several occasions provider turnaround and lead times (i.e.: Computershare; IDCARE) were not clearly mapped or considered when dates/strategies were revisited, resulting in increased timeframes to the schedule or impacting the provider's service strategy.

In hindsight, DCS/SNSW could have further explored whether elements of the notification strategy could be achieved in a timely way by other means. For example, beyond putting a public notice of the cyber incident on SNSW and some steps on what individuals can do (which were updated several months apart), DCS/SNSW could have implemented a comprehensive public awareness campaign of this cyber incident specifically and data breaches more generally, including suggestions for how individuals can remain vigilant and stay safe.

Action 15: Consider alternatives to primary strategy (contingency)

15.1 Actively consider alternative options for data breach response team in case the primary strategy or option is not working as planned, including providers, outcomes, target dates, etc.

15.2 Have the Cyber and Privacy Resilience Governance Group play an active role and challenge strategies, scenarios, issues, risks, and options.

Priority: Playbook

Action 16: Assess customer risk exposure continuously

16.1 Develop a checklist for documenting how key decisions are made based on determining the risk for all parties. Balance key decisions risks of all parties involved, including workshopping risks to customers.

Priority: BAU/Project

16.2 Include in the Playbook the need for developing a decision-making checklist.

Priority: Playbook

5.5 Step 4: Review and prevent

Overview of requirement and summary of actions completed	Finding
Review and learn from data breach incident to improve its personal information handling practices (OAIC, IPC, SNSW DBRP)	**Exceeded** Met Partially met Did not meet

The following review actions have been commissioned:

- DCS Secretary to fully investigate the data breach, including the underlying cause and the changes required to prevent a recurrence.
- The Auditor Office of NSW to conduct a performance audit in relation to SNSW's handling of sensitive customer and business information. At the time of writing a draft report was being completed, to be issued in December 2020.
- IIS to complete an independent review of the data breach, with findings to be made available to the Audit Office.

Because of the nature and complexity of the incident, DCS/SNSW has adopted the approach of 'learning as we go'. The CPRG Group requested very early on in the process for the data breach response team to keep a log of lessons learned, to assist with the development of the Cyber Security and Privacy Incident Playbook (which is a Project Trust deliverable). IIS has facilitated a series of workshops, the outcomes of which will be taken into account as part of the ongoing learning and continuous improvement culture (see Appendix F for a record of CITAF lessons learned).

Implement preventative plan to prevent similar incident in the future (OAIC, IPC, SNSW DBRP)	**In progress**

Project Trust is an internal privacy and security uplift program that was established in May 2020. It is intended to manage and deliver outcomes from remedial activities undertaken in response to the cyber security incidents and associated major data breaches that have impacted SNSW and the DCS cluster.

The scope of Project Trust encompasses the entire cluster (including GovConnect NSW where applicable) and is aimed at implementing recommendations from external and internal reviews as well as ongoing activities including cyber security, privacy and information governance.

The CPRG Group has been set up to provide executive-level leadership for this project.

The key objectives of Project Trust are stated as:

- Increasing citizen trust in NSW government
- Strengthening cyber resilience across the DCS cluster
- Reducing the risk of future security and privacy incidents
- Uplifting the capability and cyber awareness for staff across DCS.

The project is funded through the NSW Government's Digital Restart Fund with a budget of $30 million.

Project Trust will be delivered in three phases.

Whereas Phase 1 of the Project was focused on the initial response, Phases 2 and 3 will focus on the actions related to the review:

- Phase 1 (May to August 2020) – Immediate response, recovery and resilience activities related to the cyber security incident that impacted SNSW in March 2020 and the associated major data breach.
- Phase 2 (July 2020 to June 2021) – Prevention and uplift. Establishment of Ongoing Resilience Framework/Pathway through the implementation of Project Trust. Includes: The development and implementation of an ongoing DCS Cyber and Privacy Incident Resilience Framework; monitoring progress on actions, process and policy changes from Phase 1; and addressing recommendations resulting from external reviews of the incident.

Overview of requirement and summary of actions completed	Finding

- Phase 3 (TBC) – Review the effectiveness of the Customer Recovery Plan implemented for the SNSW incident and share key learnings. Additionally, determine ongoing DCS actions and requirements related to Cyber and Privacy Incident preparation, prevention, education, detection, response and recovery.

In order to achieve Project Trust's goals, five core workstreams have been established with the oversight of change management**.**

Core workstreams	Objectives
Business Process and Information Governance	Implement actions resulting from incident reviews relating to business processes and information governance
Culture Capability and Awareness	Education, training and cyber/privacy awareness campaigns for DCS staff
Cyber Security Policy and Privacy Framework	Review and alignment of cyber and privacy policy / framework
Cyber and Privacy Incident Remediations	Implement learnings from incident reviews
Cyber Resilience	Build resilience against major cyber security and privacy breach incidents across the DCS cluster reducing risk of future incidents

If updates are made following the review, staff should be trained in any changes to relevant policies and procedures to ensure a quick response to a data breach (OAIC).	**In progress**

The Project Trust 'Culture and Capability and Awareness' workstream will focus on providing the training and necessary awareness across the cluster. This will also include training in relation to data breach response once the lessons learned are debriefed and agreed actions implemented (e.g., updating the SNSW DBRP). At the time of our review, the work is in-progress as part of Project Trust.

Follow up on any recommended actions and incorporate lessons learnt into understanding of Agency's data breach risk profile (IPC)	**In progress**

As part of Project Trust, a Privacy Uplift Plan was approved by the DCS Management Assurance Committee. Actions are underway to improve privacy management practice in DCS/SNSW.

The Privacy Uplift program considers among other matters the need to respond to the Audit Office performance audit of SNSW's handling of personal information, the outcomes of this report, and applying learnings across DCS cluster.

If necessary, conduct audits to ensure follow up actions and improvements are being implemented.	**In progress**

The DCS Management Assurance Committee endorsed an Enterprise Risk Management Strategy. The Strategy includes, at a minimum, monthly discussion at the executive level to monitor the implementation of audit actions. General review actions will also be added to this including the IIS actions.

6. PART C – Adherence to customer service best practices

6.1 Assessment with obligations – both regulatory and published

6.1.1 Public commitment to the customer and delivering service excellence

NSW Government has six overarching published Customer Commitments, which are: i) easy to engage; ii) act with empathy; iii) respect my time; iv) explain what to expect; v) resolve the situation; and vi) engage the community. Beyond this, SNSW strives to be a leader and innovator and has a mission to put customers at the heart of everything it does.

IIS findings:

NSW State Government and in particular SNSW both have a strong public commitment to the customer and delivering service excellence.

6.1.2 Existing service quality at NSW Government and SNSW

SNSW (relative to other comparable government agencies) has regularly received high customer satisfaction scores. The employee attribute of 'get things done quickly' had the largest positive difference in scores. Informative staff, efficient services and an omni-channel experience contributed to high consumer satisfaction with SNSW.

IIS findings:

NSW Government as a whole and SNSW specifically had strong customer sentiment and satisfaction scores in 2019.

6.1.3 Pre-incident readiness for a large-scale customer-focused breach response

SNSW had many of the key skills capabilities needed to implement the response, including a strong cultural alignment with supporting the customer. However, there were specific capability gaps including customer insights / experience in cyber breaches, customer contact information, forensic skills, etc.

IIS findings:

SNSW had mixed levels of pre-incident readiness when it came to quickly implement a large-scale breach response. However, SNSW did not have a 'ready to go', approved customer-tested breach response operating model and related technical resources.

A key learning for agencies is that in the absence of customer contact details, entities will struggle to notify customers and that a data strategy needs to be agreed on how customer will be notified and by whom. DCS/SNSW will consider this issue further in refining its future breach response.

Action 17: Review core breach response operating model and capabilities

17.1 Workshop the potential future options for creating a breach response capability either within SNSW or NSW Government. Consider team, governance structure, assessment framework, and technology architecture / customer solutions.

17.2 Review data strategy, including customer contact opt-ins and data sharing with partner agencies including systems interoperability.

17.3 Conduct a formal capability and gap analysis against that desired capability/model. These could be further scoped or assessed (i.e., add forensic capabilities).

Priority: BAU/Project

For further details on analysis, including capability gaps identified by the team, refer to Appendix E.

6.1.4 The support solution implemented

SNSW approach to providing customer support was borne out of an authentic desire to support customers and provide a 'gold-star solution' comprising personalised letters and information backed up by useful comprehensive support services.

IIS findings:

DCS/ SNSW displayed positivity, agility and commitment when responding to the breach.

The solution design comprised: A personalised letter designed to enable the majority of customers to independently assess and/or act to reduce risk if appropriate, two tiers of call centre support, and further deeper support services via IDCARE and complaints channels.

IIS findings:

The experience design with tiered call centre layers intended to provide flexibility in dealing with large (and initially unknown) volumes of consumers seeking support while the range of service options also provides customers with choice.

The question of notification approach vs timing. CITAF debated notification options using the following stated priorities: i) timely notification; ii) clear accurate; detailed information; and iii) support (call centre and data) readiness. CITAF took advice from IIS and external advisors, ultimately deciding to prioritise getting it right and to slow down the process of notification until a full understanding of breached documents was available.

IIS findings:

CITAF's decision was aligned with leadership vision / priority of customer support. In our view it was the best of a very difficult set of choices.

For further details on analysis completed refer to Appendix E.

6.2 Customer Response (System Volumes and Feedback)

6.2.1 Channel performance and volumes to date

DCS/SNSW agreed to only monitor customer sentiment of those making contact with SNSW or IDCARE. At 19 October there were 4,378 active or closed cases with only 19,922 letters delivered. This response rate of 22% is higher than the expected 10-15%.

IIS findings:

The channels have performed well in terms of supporting contact volumes, although the volumes may be larger than anticipated. Forecasting volumes – and potentially controlling flows by postponing future batch sends – remains important and challenging.

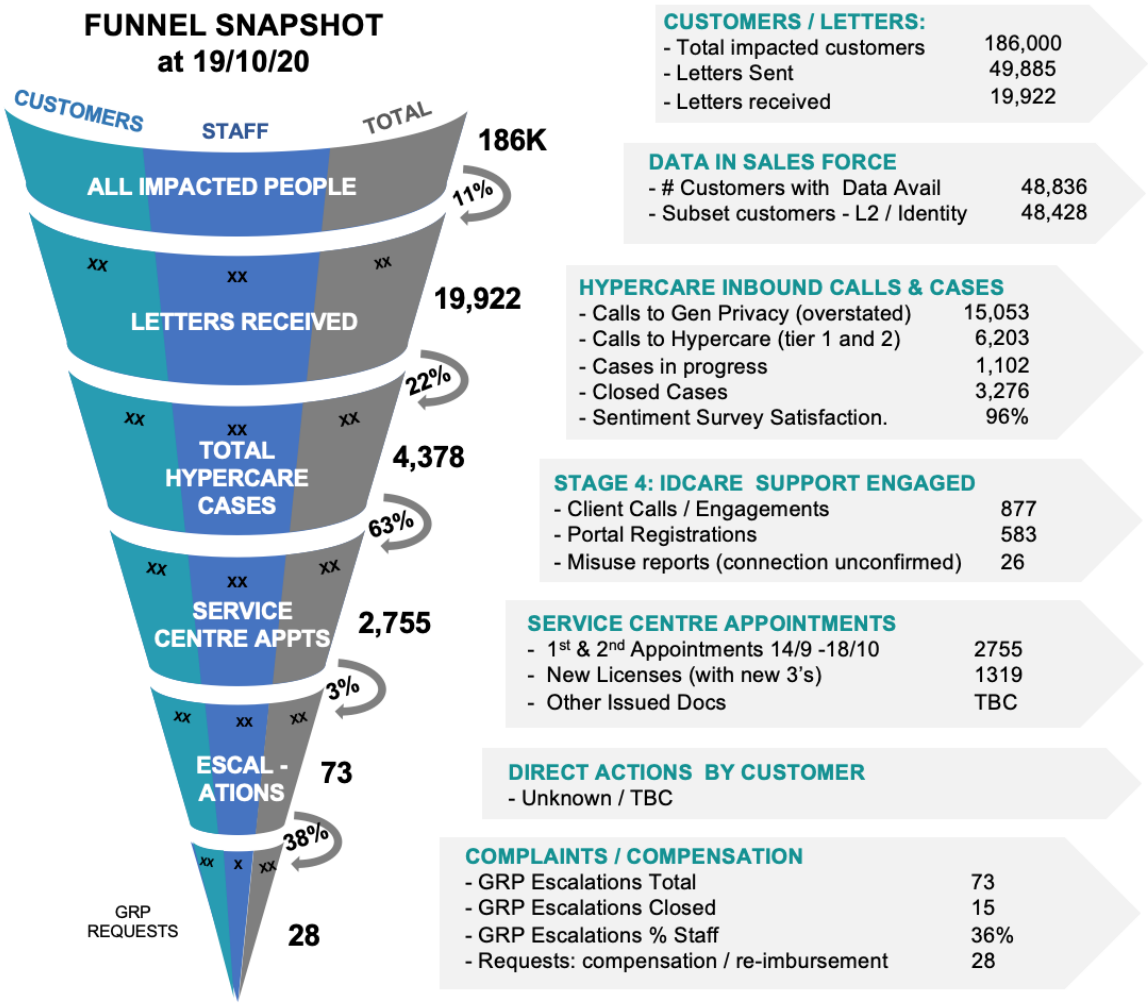


Figure 3: How customers flowed through support layers (snapshot at 19 October 2020) by IIS

Action 18: Holistic reporting showing customer effort and journey progress

18.1 Improve holistic customer reporting to provide a better view of response rates and customer engagement (ideally by cohort or segment) through the customer journey / service architecture.

18.2 Provide reports, tools, scorecards or journey diagrams that allow management to visualise how customer cohorts are flowing through the customer journey and service architecture.

18.3 Measure customer effort (time and steps) across the customer journey – again ideally by cohort and segment – ensuring exception reporting triggered for customers with extreme effort profiles.

Priority: Consideration & Playbook

6.2.2 Operational metrics

Acceptable service levels (low wait times etc.) at Hypercare have been strong and consistent.

IIS findings:

Operational metrics have been maintained at good levels, even post press release. For further details on analysis completed refer to Appendix E.

6.2.3 Customer feedback and customer service feedback at Hypercare

Overall, customers and staff were surprised and unhappy that their identity was compromised in the first place. They were disappointed by the unprofessional practices that caused this to happen and the time taken to despatch notifications. Those that have engaged with the support services have commented on the significant work and time required by them to engage the support and resolve their risk exposure. Nonetheless, the minority of customers who have leveraged Hypercare and IDCARE have provided positive feedback about the support provided (high CSAT scores for a data breach).

IIS findings:

Feedback shows staff performance is strong and redressing much of the inevitable negative customer negative sentiment towards the breach. Customers were dissatisfied about the breach occurring, the length of time taken to despatch notifications and the effort (work/time) required by them to obtain support. There are no research insights from approximately the 85% of customers who haven't contacted Hypercare and/or IDCARE.

Action 19: Collate all available customer insights from front line staff

19.1 Implement a formal process to supplement existing customer insights with insights from staff who worked on the front line. Use workshops to map journeys, discuss segments and review pain points. Collate insights regarding customers, expectations, needs, behaviours segments and journeys.

19.2 If possible, conduct supplementary customer research (post current incident) covering all key segments (adding up to 100%) of impacted customers based on response (esp. non-responders).

Action 19: Collate all available customer insights from front line staff

19.3 Leverage staff to collate all customer insights including awareness / understanding, actions taken, service preference satisfaction and brand sentiment. Where possible note and understand differences by segments.

Priority: Consideration & Playbook

6.2.4 Insights and observations by channel and/or touchpoint (via interviews)

The content of the notification letter was based on extensive guidance including from the insurer. DCS/NSW weighed up relative merits of too much and too little information. The notification letter was over seven pages and fairly complex. Many who called in to Hypercare commented that they had not read it fully or engaged with the detail in it. There is also no visibility into the effectiveness of the letter for the people who have not called in.

IIS findings:

The letter was a key part of the strategy /service capability, which relied on the majority not responding to SNSW directly. It was also designed as a key tool in enabling people to act independently to reduce their risk exposure.

SNSW made the determination that it was not possible to test the letter. The letters were enhanced and reworked throughout the process based on feedback from customers. They were also adjusted to suit different cohorts, as required - including staff.

Many customers calling Hypercare mentioned they had not read the letter. For the approximately 85% who have not called in, we have no insight into whether the letter effectively conveyed messages, helped assess risk and/or enabled independent action.

Action 20: Collate insights about effectiveness of letter and plan to conduct extra research/testing

20.1 Collate insights regarding performance and impact of letters (current incident) from front line staff and customer CSAT feedback etc.

20.2 Reconsider if/how research can still be conducted for this incident among those who received letter and didn't respond.

20.3 Explicitly consider playbook success measures among impacted non-responders segments (the majority of those impacted will not respond) and those non-impacted customers who became aware of the incident by others (such as media).

20.4 Test letter variations and optimise and build templates into playbook (create file of documents, comms assets and tools). Synthesise and share customer insights regarding the letter (e.g., understanding, response, tone, sentiment and letter elements that will drive appropriate action).

Priority: Consideration & Playbook

Batch send decision has enabled a 'just-in-time' approach and prevented unnecessary delays.

IIS findings:

The batch system has allowed notification to commence. It also provides some controls against excessive demand reducing service at the call centre.

Hypercare: At 19 October there were 4,378 active or closed customer cases. Despite the negativity associated with the event, 97% of customers were satisfied with the support.

IIS findings:

The CSAT performance of Hypercare has been excellent. While customers were not necessarily happy that the incident occurred and there were mixed feelings about the customer experience (including ease and seamlessness of the end-to-end solution), they overwhelmingly praised the quality of service provided by the Hypercare Team.

IDCARE: At 19 October IDCARE has received 877 calls, 52 emails and 583 web portal enrolments. It has provided support for the most needy/anxious and gave more capacity to Hypercare.

IIS findings:

The IDCARE experience has also been well received. We have limited information, but anecdotally Tier 2 operators say their customers valued the IDCARE service.

Service centres: By 18 October, the service centres had conducted 2,755 (first and second) privacy appointments and issued 1,319 new drivers licenses among other transactions.

IIS findings:

There have been some communication challenges and customer pain points with service centres. Much of this is now been flagged and resolved through normal quality control and feedback processes. Now that the first cohorts of customers have received letters, there are new opportunities to review and improve the end-to-end customer experience based on customer and staff feedback, especially with regards channel handover points / customer effort.

Action 21: Plan framework for tracking end-to-end customer experience and associated improvement plan during incident response

21.1 Plan creation of a more holistic view of end-to-end customer experience and centralising (rolling-up) customer experience specific improvement initiatives in a way that can be easily shared.
21.2 Display end-to-end customer experience from customers perspective, including letter, Hypercare and service centre customer handover points. Show standard service and wait times.

Action 21: Plan framework for tracking end-to-end customer experience and associated improvement plan during incident response

21.3 Create mechanisms (scorecards, reports, journey frameworks etc.) to display, report and track this – that summarise the end-to-end customer experience and shows customer cohorts by volume and stage, average time or effort spent, satisfaction etc

21.4 Log/track issues and opportunities by stage (e.g., handover to service centres, confusion around case manager roles, etc).and link to a consolidated centralised action or improvement plan.

Priority: Consideration & Playbook

GRP complaints and compensation escalations: Relatively few customers have accessed this, with higher proportions of staff who have generally felt more aggrieved.

IIS findings:

The event circumstances, the fact that notifications were slower than preferred and the amount of customer steps and effort for accessing support have been the biggest issues. Compensation for effort is not available to customers (other than staff who have received time in lieu), compounding the dissatisfaction issue.

Action 22: Review issue of compensation for effort and associated language

22.1 In future breaches, review ways in which compensation can be offered to customers (e.g. token/credit).

22.2 Ensure Hypercare and IDCARE teams are trained to set expectations of complaints and compensation outcomes to customers before they enter the process.

Priority: Consideration & Playbook

Staff support / HR and internal comms: Some staff were disappointed and/or angry that they had not been informed before customers and that they got the same letters as customers. The more staggered nature of staff communications and the lack of a cascading team huddle / comms layer exacerbated the process.

IIS findings:

Staff as a segment needed special consideration. Management have commented that in the future staff communication would be more layered, leverage managers and team leaders briefing staff in huddles (as is the normal practice) and include more senior staff comms earlier in the process.

Partner engagement and the broader customer ecosystem of support: Going into the breach SNSW did not have the appropriate senior and working relationships with all the partner agencies (as well as key third party organisations such as the major banks) required to deliver a seamless customer support response. The partner CSAT survey showed some challenges in engagement and

communication. Customers reported extremely mixed levels of awareness of the incident at the different agencies and institutions they dealt with to reissue documents, reduce their risk or update their security protocols. There was also mixed awareness and preparedness at some SNSW service centres although this was addressed.

IIS findings:

A lot of good work (which can be leveraged in the future) was done to establish the right working relationships with all partners, especially around core transactional processes and data. Ultimately the end-to-end customer experience for customers (i.e., ending with taking action at a third-party agency or bank) was not necessarily seamless and awareness of the breach within other agencies varied.

This issue can in future be addressed by more explicitly mapping all the key stakeholders (including capturing the current and post incident contact lists) and having relevant plans as well as live contacts for each group within the playbook.

Combined support services: Overall after reviewing the response and system, most support touchpoints worked effectively. Customers said it was complex and required excessive customer effort. There was some confusion regarding support roles (e.g., IDCARE vs Hypercare) and the type of case manager, as well as some stickiness at handover points. Overall staff performed well, drove up satisfaction and created 'bridges' between services.

For further details on analysis completed refer to Appendix E.

Customer steps and effort: The customer experience design resulted in many customer steps and significant customer effort. There are at least 7-8 customer steps, each of which could take approximately an hour (calls, meetings, appointments, etc.). The journey can be up to 20 steps for customers seeking to address multiple types of breached documents at third party agencies, who engaged Hypercare or IDCARE multiple times, and/or who complained or sought compensation.

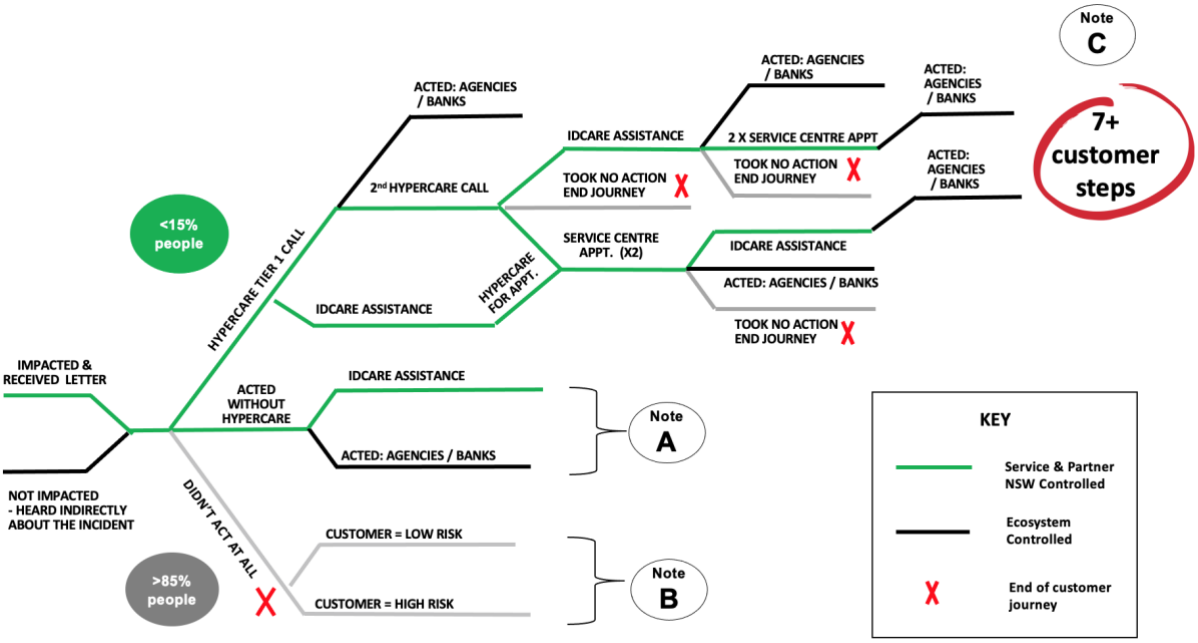


Figure 4: Overview of customer steps (IIS)

IIS findings:

In designing the customer experience / solution and services for this incident response, SNSW faced significant constraints and had to leverage existing BAU capability. SNSW coordinated the reissue/replacement of NSW Government issued POI credentials on behalf of the customer. This, by necessity, resulted in 'hand-off points'. NSW and Federal Government systems as well as processes designed around POI products contributed to the extra steps required. SNSW is/was not in a position to be able to change Agency systems and processes/policies to remove or reduce customer effort. Changes to systems in particular are incredibly expensive and time consuming

The staff interviewed are very knowledgeable about how customers approached this 'journey', their needs and what they considered pain points. They have a view on segments and their specific behaviors.

Overall, the journey was/is very time intensive for customers involving multiple steps. Many staff suggested ways the journey could be improved in the future. Handover points, in particular, often appear to compound matters.

Due to the nature of this incident response, management have limited reporting and visibility on customer effort, time spent, steps taken as well as all the different sub-journeys.

Action 23: Capture journey insights, pain-points and improvement opportunities

23.1 Before staff team disbands at the close of this incident, take the opportunity to capture insights about journey, pain-points and improvement opportunities.

23.2 Map end-to-end customer journey from the customers' perspective and by segment versus systems view. Where possible rework, compress and truncate any processes that do not add customer value.

Priority: Consideration & Playbook

Multiple handover points between services: Some customers expressed confusion about the role of support services and different case managers.

IIS findings:

There are multiple handover points and at least three different case managers (Hypercare, IDCARE and DCS). Although largely well-managed, the complexity caused some customer confusion, in particular relating to case managers and the agency role/name (e.g., IDCARE vs Hypercare sound similar).

Overall customer effort, its impact on satisfaction and measurement: Customers were annoyed about the time spent and some wanted compensation for their time. Eventually staff were given compensation in the form of time in lieu, but customers were not compensated for their time.

Ironically, the process of complaining and seeking compensation took even more of their time and did not result in compensation.

IIS findings:

Customer effort was a key metric that was not measured. Customers resented spending their time on an issue that was not their fault and were also annoyed that they had to spend extra effort if they wanted to complain. Excepting staff, time spent is not currently considered a valid cause for compensation, although the incident is ongoing, and this could change.

The two Hypercare call centre tiers or touchpoints arguably give SNSW flexibility in managing potentially high customer call volumes. However, for many customers, Tier 1 is effectively seen as an extra step that does not add customer value but resulted in additional time and effort for them.

Many customers expect to get the full information of what has been breached during the first call but effectively don't receive this information for approximately two days or until the Tier 2 call-back.

IIS findings:

The two-tier Hypercare design caused extra customer steps and anxiety, while providing operational flexibility. It may be more flexibly designed in the future and could be collapsed into one single step when call volumes and technology allows this.

This would require workshopping and scenario development however anecdotally there appeared to be opportunities to improve solutions architecture. We were advised, for example, by some front-line staff that it would be ideal if Tier 1 teams (once trained and enabled) could access the customer data required to perform a combined Tier 1 / Tier 2 call thus reducing customer steps / effort and stress (including staff stress at not being able to provide customer information). We were further advised by another team member that an additional Salesforce module would enable this from a technical perspective.

Action 24: Review flexible systems architecture and service design options to facilitate future responses

Consider systems (tech, process and data) architecture options and improvements that would support likely future breach response solutions requirements and scenarios.

Priority: Consideration & Playbook

Harm segments and how they worked in practice: While harm segments worked well generally, there were examples of where the classifications and process failed to deliver customer benefit:

- A significant number of customers received a letter explaining that documents in a high harm category had been breached. They were taken through the whole process, only to be told at Tier 2 that the data breach was insignificant because a single relatively minor personal information marker had been breached e.g., expiry date of driver's license or name of bank.

- Customers with a high volume of breached elements had an overwhelming experience. For similar reasons, they may benefit from being fast-tracked to Tier 2.

IIS findings:

The harm segments were established early and not reviewed after the extent of the data breach was clarified, nor were they given a 'reality check review' when customers started flowing through the system. The approach could/should be enhanced in the future to improve the customer experience and reduce volumes of letters and customers contacted.

Segments of focus (All impacted customers vs. those who engage): CITAF decided that no further research can be done with customers who had experienced the breach response, as it could further breach customer privacy. As such, the market / customers have been advised they will not be recontacted. SNSW therefore does not have any insight into people who received the letter but did not contact SNSW. For this group, we do not know how the letter was understood and whether it drove independent action as appropriate, nor the overall sentiment towards the SNSW brand.

IIS findings:

There was an overall lack of 'big picture view' of all customers. Specifically, there was limited understanding of customer engagement and action outcomes for the majority who did not contact Hypercare. The letter was a key part of the strategy, although it could have been more effective if time had allowed more testing and research.

Action 25: Formally consider broader customer research scope (i.e. beyond those who contact SNSW)

25.1 Review the overall scope of the research framework and investigate how customer research can be conducted (regarding this incident and in particular among the majority of impacted customers who have not called or engaged with Hypercare and or IDCARE) without impinging privacy further.

25.2 Seek to build understanding of impact of the whole program on all 186,000 impacted people and on the perceptions of other customers who had heard about the incident.

25.3 Formally consider and agree on research scope prior to making announcements that limit the ability to contact certain segments.

Priority: Consideration & Playbook

Review of how support and resources were prioritised and applied against customer segments: The system design is effectively 'self-service' and many customers in harm categories 1 and 2 who received the letter have not contacted SNSW or responded to Hypercare. They may not have acted to reduce their risk.

IIS findings:

High risk but non-responding customers have not been followed up on by SNSW. Some may have age or other capacity-related reasons as to why they have not acted.

Action 26: Review effort, cost, value added and outcomes by segment

26.1 Review which segments and groups received the major share of the effort, time, resources and cost as part of the project 'wrap-up' and debriefing process. In particular, review whether this aligned with the high-risk categories and assess success outcomes (at least partially) on this basis.

26.2 Combine with extra insights from additional primary customer research into segments that did not respond or engage with SNSW.

26.3 Consider following up with high-risk non-responders for future incidents.

Priority: Consideration & Playbook

6.2.5 Observations about customers: Journeys and segments

SNSW has a reluctance to label or segment customers too much, however segmentation can be useful for future system and service design – particularly with large groups of people needing varied support. A range of customer behaviour and segmentation related insights have been synthesised in Appendix E (untested as from staff interviews only). These include insights and comments on customers' service style (Do it For Me vs DIYers) and also on how customer personas were demonstrated (including 'Catastrophisers', 'Venters' and 'Confirmers').

IIS findings:

No systematic capture of broader segmentation information (and no research beyond the CSAT survey with customers who contacted HyperCare/IDCARE) makes 'rolling up' customer insights for future design purposes very challenging.

Customer journeys are also a useful tool in collating customer insights for future use. They are not the same as process or touchpoint maps which are already available for this incident.

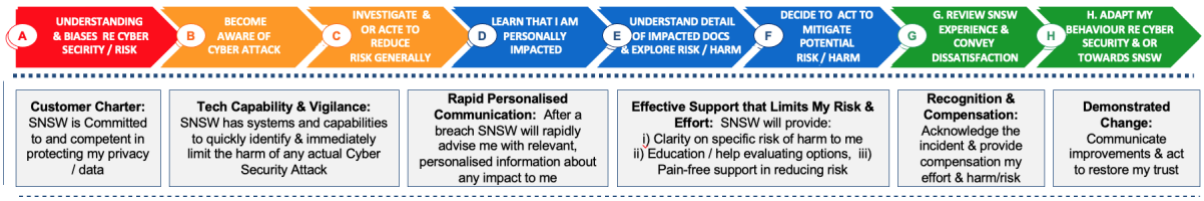


Figure 5: Illustrative map of the customer journey and associated expectations for a data breach response (IIS)

Mapping customer journeys for subgroups and personas could identify subsets of customers who have similar needs and drivers, and thus require different service design.

IIS findings:

The customer journeys (segments and personas) could be workshopped after the event and would be a useful playbook input on service design options.

Refer to Appendix E.

6.3 Assessment of customer support and customer experience

6.3.1 Did the breach response team meet its success measures?

IIS findings:

CITAF defined customer support success factors and IIS rated the factors in the below image. CITAF is largely on track to meet its goals and success measures for the incident response. The project timeline has been marked as a 'miss' because of the length in response time caused by the data issues (this is not a project management issue).

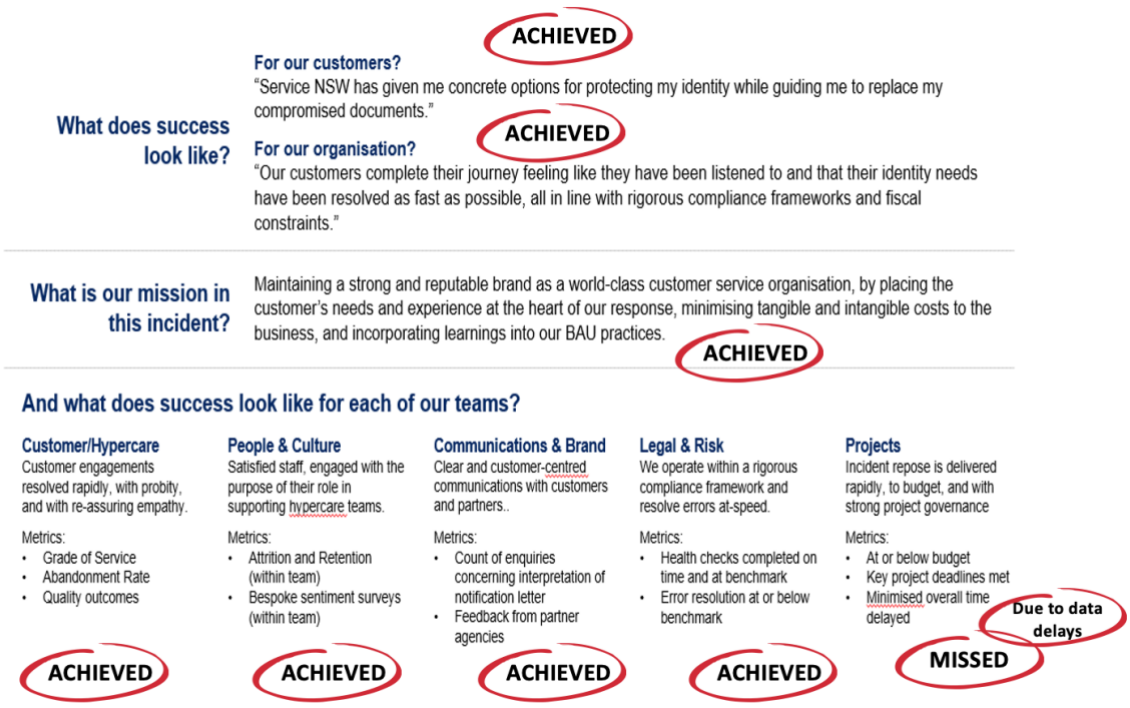


Figure 6: Customer support success factors provided by CITAF rated by IIS

For more information, refer to Appendix E.

6.3.2 Did SNSW deliver best practice customer experience?

Support was positive for the minority who engaged but unknown for those who did not. Hypercare received good CSAT feedback. Similarly, IDCARE results were extremely positive relative to almost all other breaches. Nonetheless, a small yet significant subset of people who engaged were

fundamentally unhappy with the breach occurring, the time that SNSW took to notify and the level of effort required on their part.

IIS findings:

SNSW delivered best practice customer experience for the majority of those it supported (otherwise unknown for non-responders).

The above 'big picture' satisfaction issues may not have been reflected in the CSAT surveys, given the way they were written and issued at the end of the final call on the case manager's request. Further research is required to understand the overall satisfaction of customers with the entire breach solution including the notification mechanism and timing, the service/support and the experience of taking actions at other agencies to reduce risk.

6.3.3 Was the aim of 'supporting and empowering customers to act to minimise future risk' met?

IIS only has limited data on the majority of impacted customers who have not contacted SNSW or IDCARE as to whether they assessed and or acted to reduce risk. SNSW also has imperfect data on risk mitigation actions taken via end-agencies or partner sources.

The letter provided by SNSW states what happened, why it happened, what was compromised, what SNSW has done in response and what customers can do. The letter also notes a customer's right to review, make a complaint and seek compensation. There is an inevitable conflict with providing completeness of information and doing so in a succinct manner. IIS suggests testing of letter formats and style variants for future use.

IIS findings:

We consider that the stated aim of 'supporting customers and empowering them to act to minimise future risk' was met for the important minority of customers who received direct support after reaching out. Whether this aim has been achieved for non-responders (the vast majority of those impacted) is inconclusive, pending further evidence.

Furthermore, DCS/SNSW should consider whether there should be a focus on wider public engagement, including for the potentially affected people who did not make contact and/or who have not opened or read the letter. Within this context, we note that there is a wider whole-of-government program of public engagement work to uplift cyber security awareness (including $240m allocated to Cyber Security NSW) that will help customers minimise future risk.

7. Data breach benchmark

IIS conducted high-level research on recent data breaches and how these breaches compared to the SNSW incident. We also consulted IDCARE for some examples that could be considered. IDCARE confirmed that the SNSW case is unique and there are no comparable cases in terms of the size of the breach, the unstructured data and the lack of customer database (CRM) to start with. These factors increased the length of time taken to carry out notifications, which was compounded by the COVID-19 pandemic. IDCARE indicated that they have found that organisations across the industry are experiencing longer timeframes to notify.

In conducting the research, IIS looked at data breaches that would be comparable in terms of the sensitivity of data, size of breach, method of communication, time to notify and customer support offered. We summarised our findings as follows:

1) SNSW notification using personalised letters is consistent with previous breaches of high-risk information and they took extra care to manage risks

In late 2018, the Australian National University (ANU) was breached and the payroll details of staff and students were accessed by external hackers. The breach was only discovered in May 2019 and affected 200,000 individuals. The compromised information included name, addresses, tax file numbers and bank account details, among others. Another similar breach was Melbourne TAFE in 2018, with 90,000 individuals affected and 55,000 files compromised containing contact details, health and financial data. The incident was only discovered in October 2019 and affected individuals were informed in March 2020 (this was a long ingestion period – 13 months from discovery to go live). SNSW, similar to ANU and Melbourne TAFE, was transparent with those affected by providing information about the details of the breach and how to get support on its website. Melbourne TAFE and SNSW brought in IDCARE to provide support to those affected.

Melbourne TAFE and SNSW notified impacted individuals via personalised letters which are considered to be the more trusted channel of notifications as customers may view emails as scams, although it does take longer to notify customers. IDCARE confirmed that registered person-to-person post is not a common method to notify customers. SNSW efforts have gone an extra mile to do this.

2) SNSW has been slower to release accessible online information to guide customers in how to protect themselves

In terms of similarity in size and profile sensitivity, Dr. Lacey of IDCARE highlighted the data breaches of the Australian Sports Commission (ASC) and the Australian Red Cross Blood Service (now Australian Red Cross Lifeblood). Both entities responded with a solid communication and engagement model. In the case of Sports Commission, the Chief Medical Officer made 1:1 calls to athletes.

Both the ASC and Lifeblood had good web content to guide customers on how to protect themselves along the process. SNSW had been slow to do this.

3) SNSW's actions in supporting affected individuals are in line with industry practice

IDCARE's 2020 Beyond the Breach report provided some insight into some of the common actions taken by other organisations in terms of supporting impacted persons. Some of these includes reimbursing of credential replacements such as driver's license, allowing for one to two days paid time off for employees impacted and proactive notification of tax authorities. SNSW has also taken some of these actions to support impacted customers.

8. Appendices

8.1 Appendix A – Approach and methodology

IIS has taken a consultative approach to complete the review and has worked closely with DCS/SNSW all stages.

Planning and coordination

During the planning phase, IIS shared a draft report structure with the DCS COO for review and comments. Moreover, a weekly project status meeting was set up with Executive Director, Governance, Risk and Performance to confirm scope, timelines and track risks and progress to completion. Weekly status updates were provided to DCS.

Execution of approach

- **Step 1: Review documentation**

  Conduct information gathering during and after the incident response. This includes reading background documentation and documentation used during the incident response.

- **Step 2: Conduct individual interviews with stakeholders** to:
  - Confirm the context DCS/SNSW and whole of NSW Government
  - Clarify IIS questions based on documentation review or to further discuss process and procedures used as part of the incident response
  - Gather information of any uplift controls and procedures that have been agreed during the period of the incident response to reduce the likelihood of a recurrence.

- **Step 3: Workshop and analysis**
  - Facilitated a series of six workshop discussions with selected key team members to debrief on lessons learned.

- **Step 4: Analysed available insights and metrics** in relation to the customer, employee, and partnership sentiment defined by Executive Director Service Delivery

- **Step 5: Prepare report**
  - Following the analysis stage, prepared a draft report with a high-level summary of findings. Following feedback from DCS/SNSW, prepared a final report.

8.1.1 Documents received

Documents	
Background context	
1.	DCS – Cluster Org Chart 30 July 2020
2.	SNSW Org Chart
Information security and cyber documents	
3.	SNSW 2018-10 IT General Controls – 17 September 2019
4.	SNSW 2018-03 Protiviti – Essential Eight (8) Cyber Incident Mitigation Strategy Review – 19 December 2018 (1)
5.	Detecting and responding to cyber security incidents across NSW agencies, conducted by the Audit Office of NSW- March 2018
6.	NSW Cyber Security Incident Emergency Sub Plan – December 2018
7.	NSW Cyber Incident Response Plan – Feb 2020
8.	Information Security Incident Management Policy and Process – April 2018
9.	Information Security Incident Management Policy IT Policy – October 2016
10.	Procure IT Framework v.3.2
11.	NSW Government Information Classification, Labelling and Handling Guideline V2.2_0 (2015)
12.	NSW Cyber Security Strategy 2018
13.	DCS/SNSW Cyber/ roles and responsibilities (RACIs) August 2020
14.	Cyber Governance Group Policy overview 11 June 2020
15.	NSW Cyber Security Policy 2020 v 3.0
16.	Crowdstrike report - PurpleNOte001-3: Investigation Report – May 1 2020
17.	Service NSW Information Security Incident Management Policy v1.3
18.	20200804 - K1458 - Service NSW Phishing Incident Report V1.1_FINAL
19.	Email evidence of DCS former CISO informing of the incident to management (escalation)
20.	NSW CISO INCIDENT STATS (sensitive)
21.	DCS Attestation 2019 and 2020
22.	MFA rollout evidence documentation (closing December 2018 pending action)
23.	Internal Audit evidence to close out the audit action on incident response (SNSW 2018-10 IT General Controls – 17 September 2019)
Project management CITAF	
24.	Daily and bi-weekly briefings
25.	Action and decision logs
26.	CITAF Governance and workgroups deck
27.	Data breach Risk Register (August 2020)
Risk, privacy, governance	
28.	Service NSW Fact Sheet (October 2018)
29.	AO NSW BN - Performance Audit - Item 11 - Privacy Management Roles and Responsibilities
30.	ERM CYBER PRIVACY - GRP – 21 July 2020

Documents	
31.	Service NSW Privacy Policy 2019_Endorsed
32.	Service NSW Privacy Management Plan 2019
33.	De-identified customer notification letter dated 2 June
34.	Attachment B - Data Access MOU DCS and RMS
35.	DAC Data breach response plan
36.	DAC handling of personal information
37.	Allen's affected Individual reporting templates
38.	SNSW Data breach response plan – January 2019
39.	PII Markers list
40.	DCS Security Training Completion rates 14072020
41.	Service NSW Privacy by Design _Attendees list 1 July 2020
42.	DCS Risk-and-resilience-framework Feb 2016
43.	Trim data breach training (May 2020)
44.	COI - Escalation flowchart - 29 July 2020
45.	GRP Escalation Pathway Within Salesforce High Level View
46.	GRP Escalation Process Walkthrough 29.07.2020
47.	Process Map for General and Tax File Number Complaint
48.	Process Map for Request for Information
49.	Request for Internal Review
50.	UPDATED GRP Complaint and Privacy Review Team - Proposed Structure – 4 Aug 2020
51.	SteerCo Update Meeting Pack September 2020 (1)
52.	Scope for Service NSW request audit - revised scope to DCS 110620
53.	Auditor General Commencement Letter Minister Dominello SNSW
PID PIA	
54.	Final PID PIA (endorsed)
55.	Letter to Catherine Ellis re Public Interest Direction in Relation to Service NSW 05082020
56.	Public Interest Direction in Relation to Service NSW
57.	TAB C SNSW RESPONSE TO PIA RECOMMENDATIONS (FINAL 13 JULY 2020)
58.	TAB F SNSW S41 PID BUSINESS CASE (FINAL 13 JULY 2020)
59.	TRIM Tab D deidentified notification letter (1)
60.	TRIM Tab E supports available to impacted customers (1)
Breach notifications	
61.	Service NSW Assessment Approach (3) – dated 14th May
62.	IPC Notification letter
63.	Notification to OAIC – NBD 36074
64.	Notification letter to ATO and Deputy Commissioner of Taxation
65.	BN - High Profile Notifications

Documents	
66.	CSAT Questionnaire
67.	Employee / former employee (conflict of interest) – Hypercare notification process
68.	BN024832020 ATTACHMENT TO BRIEFING NOTE Tab A Strategy for managing Conflicts of interest
69.	BN024832020 ATTACHMENT TO BRIEFING NOTE Tab B COI Training Draft
70.	BN024832020 BRIEFING NOTE BN 02483 2020 153921 BD Briefing Service NSW 30 June 2020 UPDATED
71.	BN024832020 BRIEFING NOTE BN 02483 2020 DR approval 20200807
72.	Approved BN_0High Profile Customer Notification Strategy
73.	BN-02491-2020_157838_Tab_A_Leader_Talking_Points_for_VIPs
74.	BN-02491-2020_158505_Tab_B_HPC_List_1_5
Hypercare and customer service	
75.	Prioritisation Assessment Approach v.3 14 May 2020
76.	Proposed engagement model – Hypercare team
77.	Customer Satisfaction and Performance paper (August 2020)
78.	TRIM Data Breach Incident Training (MAY 2020 PPT)
79.	V.1 Privacy Hypercare Scale Up - Training
80.	Privacy line - Pre batch CC stats
81.	CSAT Survey Summary
Cyber and Privacy Resilience Governance Group	
82.	DRAFT - ToR - Cyber and Privacy Resilience Governance Group - V3 – 26 May 2020
Communications	
83.	200907 Release F Service NSW cyber incident notification 07092020
84.	Public awareness campaign plan-on-a-page (Oct -Dec 2020)
85.	Damon Rees Live Chats
86.	Message from Damon Rees 14 May 2020
87.	Message from Damon Rees 15 May 2020
88.	Message from Secretary 15 May 2020
89.	Message from crisis controller 190 May 2020
90.	Message from the Secretary 7 September 2020
91.	Message from CEO 14 September 2020
92.	Media articles of incident (May – September 2020)
93.	Internal communications / examples
94.	Examples of key media articles and press stories
Crisis management and business continuity	
95.	DRAFT communication Plan Service NSW cyber-attack (1.06.2020)
96.	BCP Document Map 2013
97.	Service NSW - Crisis Communication Plan - 2013

Documents	
98.	Service NSW Technical Support Process
99.	Datacom Connect ICT Management – Business Continuity Plan for SNSW Contact Center - 2013
100.	Influenzas Pandemic Plan V1.0 BCP – June 2013
101.	System and Technology Business Recovery Plan V1.0 – June 2018
102.	Service DELIVERY Channels- Business Recovery Plan v1.2 – June 2013
103.	Service NSW BCP Plan v 1.0 – June 2013
104.	Business Continuity Management Policy V1.0 – 2013
105.	BCP incident evaluation – 2013 (Business Impact Analysis Summary)
106.	People & Culture Business Recovery Plan V1.0
107.	BCP Incident evaluation contacts
Project Trust	
108.	Project Trust_Overview_18Aug2020 (2)
109.	3A - CPRGG - Project Trust Update - 01Oct2020_Mtg
P&C	
110.	Quarterly CultureAmp employee engagement surveys (latest run prior incident / any surveys held post incident) -STATS ONLY
111.	Annual People Matter Employee Survey occurring in late 2020-STATS ONLY
Customer support and experience (specific request)	
112.	Documents related to (or links to) SNSW's ongoing customer experience mgt. framework and operating model e.g., customer vision/mission/ charter/guiding principles, team organisational charts, KPI's or customer related targets/goals and customer satisfaction measurement
113.	Final version of power-point 'Privacy Breach Customer Satisfaction and Performance' endorsed by SNSW CITAF governance group
114.	All main press releases (with dates) and digital / social messaging / content updates
115.	Access to view senior management videos and Q&A internal debrief sessions (Damon Rees)
116.	Hypercare CSAT survey summary (From 7th Sep-19th October)
117.	IDCARE survey summary (From 7th Sep-19th October)
118.	Detail free text comments from employees and customers received via CSAT and IDCARE survey tool
119.	Hypercare incident management team structure: Org. charts, roles, KPI's etc.
120.	Relevant NSW Govt. or Customer Service Commission guidelines etc. (or links to them)
121.	The annual trust index conducted by the Customer Service Commission
122.	The existing body of metrics that SNSW applies to all of its service delivery activities. This includes Grade of Service, Abandonment Rate, Call Quality, Average Wait Time, etc. summary (From 7th Sep-19th October)
123.	Evidence of latest Cyber incident test
124.	CSAT partnership agencies results
Additional information provided by DCS/ SNSW (post review of DRAFT report)	
125.	01. 2020-05-14 - INBOUND - Harm Assessment - IDCARE
126.	Privacy Uplift - GRP Nov 2020 (1)

Documents	
127.	F20-1663 CEO BN – Data Privacy Breach Notification Process
128.	BN20.812 TAB A – SNSW customer harm assessment categories.
129.	DCS MAC Briefing Paper - RISK APPETITE & CULTURE
130.	03. TRIM 00_Approved - Prioritisation Assessment Approach (1)
131.	CITAF - Key Learnings Register

8.1.2 Meetings held

	Department of Customer Service			Comments
	Name	**Role**	**Representing**	
1	Emma Hogan	Secretary	DCS	With Stephen Brady and Damon Rees 12 October
2	Greg Wells	Government Chief Information and Digital Officer	Digital and ICT	With Tony Chapman 22 September
3	Steven Brady	Chief Operating Officer	Corporate Services	Together with Emma Hogan and Damon Rees 12 October
4	Andrew Pilbeam	Director, Governance	GRP Governance (Digital and Services)	With Catherine Ellis 29 September
	Department of Customer Service – Cyber Security			**Comments**
	Name	**Role**	**Representing**	
5	Tony Chapman	Chief Cyber Security Officer	Cyber Security NSW	With Greg Wells 22 September
6	David Griffiths	Manager, Cyber Sec Detection and Response	Cyber Security Detection and Response	Individual – acting as DCS CISO 21 September
	Department of Customer Service – Information Technology			**Comments**
	Name	**Role**	**Representing**	
7	Anthony Ritchie	Group Chief Information Officer	ICT Security	2 October
	Brent Snow	Chief Technology Officer	GCS Chief Technology Office	
	Department of Customer Service – Governance, Risk and Performance			**Comments**
	Name	**Role**	**Representing**	
8	Catherine Ellis	Executive Director, Governance Risk and Performance	Governance, Risk and Performance	With Andrew Pilbean 29 September
	Anthony Lane	Director, Audit and Investigations	Governance, Risk and Performance	

9	Matthew Smith	Manager, Governance (Regulation and Corporate)	Governance, Risk and Performance	23 September
	Department of Customer Service – Legal and Audit			**Comments**
	Name	**Role**	**Representing**	
10	Catherine Morgan	Managing Lawyer	Legal	29 September
	Colleen Dreis	General Counsel	Legal	
	Department of Customer Service – People & Culture			**Comments**
	Name	**Role**	**Representing**	
11	Michele Paphitis	Director, People & Culture	People & Culture	28 September
	Jordan Shoveller		People & Culture	
	Department of Customer Service – Corporate Comms and Brand			**Comments**
	Name	**Role**	**Representing**	
12	Angela Kamper	Executive Director Brand, Digital and Communications	Brand, Digital and Comms	7 October
	John Kerrison	Director of Communication	Brand, Digital and Comms	
	Service NSW			**Comments**
	Name	**Role**	**Representing**	
13	Damon Rees	Chief Executive Officer	SNSW	With Steven Brady and Emma Hogan 12 October
	Service NSW Partnerships			**Comments**
	Name	**Role**	**Representing**	
14	TBC	A/Executive Director, Partnerships	Partnerships	24 September
	Catherine Buining	Manager Strategy and Performance	Partnerships	
	Service NSW Service Delivery			**Comments**
	Name	**Role**	**Representing**	
15	Jody Grima	Executive Director, Service Delivery	Service Delivery	6 October
	Christine Kosorukow	Director, Operations	Operations	
	David Walsh	Director, Channel Planning and Release Management	Service Delivery	
	Kelly Klower		Service Delivery	

	Service NSW Digital Middle Office			**Comments**
	Name	**Role**	**Representing**	
16	Melissa Clemens	A/Executive Director, Service Delivery DMO	Digital Product	23 September
	Michael Cracroft	Director, Channel Enablement	Security and Risk	
	Service NSW Program Delivery and Enterprise Change			**Comments**
	Name	**Role**	**Representing**	
17	Philip Muehleck	Director, Program Delivery	Program/Project	24 September
	James Workman	Senior Project Manager	Program/Project	
	Samantha Serratore	Change Manager	Program/Project	
	Service NSW Finance			**Comments**
	Name	**Role**	**Representing**	
18	Yvonne Deng	Chief Financial Officer	Finance	30 September
	Other key stakeholders			**Comments**
	Name	**Role**	**Representing**	
19	Narelle Grayson	Director	DAC	30 September
20	Linda King, Betsy Gordon , Danielle Tonga, Aimee Hinder, Graeme White	Customer support / experience: Learn how complaints has worked during incident and get a snapshot of customer issues and capture Lisa's insights. Pain points that may need to be considered for future. Walkthrough complaints report	Complaints GRP	16 September and 21 October
21	Karen Maccallum David Walsh	Customer support / experience: Notification (letters) and QA process	Interaction Computershare / Australia Post	16 September
22	Dale Condon	High level overview of CMT / BCM SNSW/ DCS/ NSW Gov framework. Exercise and lessons learn regime.	CMP DCS	13 September
	External Agencies			**Comments**
	Name	**Role**	**Representing**	
23	Michael Morris	Partner	Allens Security Services	13 October
	David Rountree	Managing Associate	Allens Security Services	
	Shane Bell	Partner	McGrathNicol	
24	David Lacey	Managing Director	IDCARE	28 September

	David Lacey (follow up)	Customer support / experience: reporting	IDCARE	4 November
	Hypercare Team (names anonymous)			**Comments**
25	Service Centre Tier 2- Service Managers	Two staff members interviewed	Insight on Hypercare customer – coordinate with calls with Hypercare agents	22 October
26	Level 1 HyperCare	Four staff members interviewed		21 October
27	Level 2 HyperCare	Five staff members interviewed	Tier 2 – Case management (mixt of agents that deal with different categories of risk groups / tasks)	19 October
28	Front line customer care supervisors	Nine staff members interviewed	Front line customer care supervisors at your SNSW offices	20 October

8.1.3 Stakeholder working sessions held

Session	CITAF Stream	Areas attending	Names
1	Project Office 13 October	PMO	Philip Muehleck, James Workman, Kylie Bowmaker, Cherry Mendoza, Bethany Pankhurst
2	Privacy, Legal and Compliance 15 October	Legal and GRP	Catherine Ellis, Colleen Dreis, Catherine Morgan, Graeme White, Dora Amoah-Nyampong
3	Notifications 23 October	Service Delivery, Legal, GRP, PMO	Jody Grima, Colleen Dreis, Catherine Ellis, Catherine Morgan, Kelly Klower, James Workman, Philip Muehleck, Narelle Grayson
4	Engagement, Communications and Media 19 October	Stakeholder engagement, Media and Social, Partnerships, GRP	John Kerrison, Kara Lawrence, , Catherine Ellis, Imogen Corlette, Catherine Buining, Rebecca Lang, Angela Kamper
5	Security incident response and uplift 20 October	DCS ICT, SNSWDMO, Cyber Security NSW	Michael Cracroft, Rachel Price, Tony Ritchie, Brent Snow, Tony Chapman, David Griffiths
6	Customer engagement 20 October	Hypercare team, PandC, GRP	Jody Grima, Christine Kosorukow, Michele Paphitis, Jordan Shoveller, Catherine Ellis, Linda King

8.2 Appendix B – Further context to SNSW and the breach

8.2.1 SNSW operations

SNSW has been in a state of emergency and addressing business continuity matters since late 2019. The SNSW team has been working under pressure since the 2019-20 bushfire and flood crises, which then extended to the COVID-19 pandemic. SNSW plays a critical role to support NSW Government activities in relation to the COVID-19 response. SNSW agents assist NSW residents to find out about the latest information related to the benefits and services available such as health and wellbeing, employment, skills and training, food support, housing and finances. SNSW call centres provide services 24/7 and have been responsible for issuing travel permits.

Members of the CITAF team have been working from home (WFH) throughout the cyber incident and data breach response period, which is not the working arrangement that is most conducive to coordinating a long-term data breach response effort.

8.2.2 Previous and existing audits

DCS/SNSW have undergone various assessments and audit reviews related to cyber security and information handling. These include:

- March 2018 – Detecting and responding to cyber security incidents across NSW agencies, conducted by the Audit Office of NSW
- December 2018 – Internal SNSW audit on the implementation of the Essential Eight strategies to mitigate cyber security incidents
- August 2019 –Internal SNSW IT general controls audit
- Ongoing – Managing cyber risks across NSW agencies, currently being undertaken by the Audit Office of NSW
- Ongoing – Performance audit in relation to SNSW's handling of sensitive customer and business information by the Audit Office of NSW.

  This audit was requested on 19 May 2020 by the Minister for Customer Service. In addition to the scope above, the audit report will outline the context within which this audit was requested and may also comment on the Department's response to the data breach and findings of its commissioned review(s).

As a result, the CITAF team has not only faced the pressure of responding to the data breach but also dedicating time to meet the requirements of the Audit Office, IIS, as well as other stakeholders and partners during a year of ongoing business and personal disruption at all levels.

8.2.3 Developments in the cyber environment

This breach response effort is taking place among developments in the broader cyber environment:

- The ACSC already started an awareness campaign back in March 2020 on expected malicious activity during COVID-19 (in particular scams and phishing emails) and alerted

that the incidents were likely to increase in frequency and severity over the following weeks and months.

- IPC quarterly statistics indicate that during FY2019-2020 a total of 10 local NSW government agencies had reported data breaches.
- During June 2020, Prime Minister Scott Morrison announced that Australia was the target of a state based cyber attacker. The attack targeted Australian organisations across all levels of government and industry, including the political, education and health sectors as well as operators of critical infrastructure. Mr Morrison also announced a new Cyber Security Strategy along with further investments.
- The NSW Government also announced that it would invest $1.6 billion into its digital-centric investment fund to accelerate IT projects and bolster cyber security over the next three years. The objective is to 'strengthen the government's capacity to detect and respond to the fast-moving cyber threat landscape' and make NSW the 'cyber security capital of the Southern Hemisphere'.

8.2.4 Readiness prior to the data breach

Although it is beyond the scope of this report to assess the level of SNSW readiness for a data breach event, IIS considers that it is important to describe the state of play at the time in order to understand the resulting impacts on the ability for SNSW to identify the situation early and to respond quickly.

IIS gathered the following information based on document review and discussions with DCS/SNSW stakeholders:

- There was not a full understanding of the scope of, and risks to, sensitive information contained inside email systems; the key focus for information handling was on service rather than quality or risk.
- Pending observation from internal audits were not addressed e.g., from
  - December 2018 audit – 2.2.3 MFA due in June 2019
  - August 2019 audit – 2. 8 incident management and governance due March 2020
  - However, IIS notes at the time of writing the report these observations were addressed, closed, and evidence was provided.
- Stakeholders reported there has been a history of under-investment in IT security and associated resources, process and technology that contributed to the incident occurring.
- The lack of a data breach response plan across NSW Government, including within DCS/SNSW, impacted the ability to deal with the data breach. IIS noted that the current NSW Cyber Incident Response Plan is written from the perspective of a cyber security incident management and a data breach response plan is required to address privacy.
- There was a disconnect and lack of harmonisation between DCS Cluster Cyber and SNSW Cyber when first triaging the incident and remediating against the compromise. Despite adhering to the NSW Cyber Incident Response Plan and the NSW Cyber Incident Emergency Sub Plan, consideration could be given to Cyber Security NSW playing a

coordination and enforcement role when managing such incidents, regardless if a "significant" incident has been declared by the NSW Chief Cyber Security Officer.

- The recent DCS/NSW consolidation (1 July 2019) centralised some SNSW corporate support into DCS. Several initiatives to review policies and procedures were under way but there was no formal documentation outlining the relationship between the SNSW and DCS cyber security teams in place at the time of the incident or during the response.
- The DCS/SNSW Security Incident Response event classifications are not harmonised or aligned with the NSW Cyber Incident Response Plan (i.e., not using the same labelling framework) and an event classification does not automatically trigger resources (with defined roles and intra-agency governance model) and response events.
- DCS/SNSW did not have scripted policies and plans that recognise the differences with, and relationship between, cyber security and privacy.
- At the time of the cyber incident a corporate policy and procedures harmonisation project was underway across the DCS cluster, but it was not yet complete. This resulted in initial confusion of policies and procedures to be followed and command and control structure.
- Despite having a crisis management program where desktop simulations are regularly completed as part of the testing regime, data breach scenarios had not been exercised.
- Group Risk and Performance (GRP) raised that there was no harmonised approach to risk management across the cluster and as such there were very different appetites and tolerances for risk in general.
- There was a lack of a prior large-scale data breach experience, education and communications assets (e.g., IP, source of truth, understanding of harm scenarios etc.), which meant there was a steep learning curve and also made bringing in Subject Matter Experts for media briefings more challenging.
- There were no initial data breach specific partner engagement maps or contacts such as joint partner playbooks, operating model, engagement framework, etc.

8.2.5 Challenges arising from the data breach

The large size and unstructured nature of the dataset compromised by the cyber incident had several implications:

- It made the analysis difficult and prolonged. Forensic and privacy professionals concurred that the type of data made it difficult to work with and the specifics of the breach were unprecedented in the field.
- There were challenges around mobilising a large-scale notification program, such as scammers using the opportunity to contact customers posing as SNSW.
- In addition to citizen and business information, the dataset exfiltrated also contained SNSW staff information (including sensitive information on topics such as mental health and disciplinary actions). This raised challenges in terms of a conflict for existing staff managing their own cases as well as other staff members potentially finding out information about them.

- IDCARE indicated that immediate organisation response to attacks of this size and nature should be seen as part of a much larger and longer process, as the impacts on and recovery for customers can have a very long 'tail'.

Another challenge that SNSW faced was that it did not hold a CRM database with contact details for all individuals affected. In order to contact them, SNSW needed to collect their contact information from partner agencies such as Transport for NSW (TfNSW) and NSW Register of Births, Deaths and Marriages (BDM), and associated IT systems. Legal impediments to sharing information with issuers of credentials required the SNSW to submit an application for a Public Interest Direction (PID) under s 41 of the PPIP Act and have IIS perform a Privacy Impact Assessment (PIA) to enable it to collect and use certain personal information that would be otherwise prohibited under the PPIP Act.

From a 'shared risk' perspective, the decisions, actions and inactions of DCS/SNSW in responding to the data breach would have an impact across NSW Government. How a particular government agency responds to a data breach will impact on customer expectations and trust in the NSW Government as a whole. Furthermore, the stakes are higher for SNSW as it has high levels of customer satisfaction to maintain and is perceived to be a key and trusted source of 'true data' including drivers' licences and BDM information.

IIS notes that SNSW had a key advantage in responding to the data breach – namely, it had the technical and operational capabilities including call centre, communication infrastructure and customer service experience. Despite the initial lack of specific IT systems, customer scripts and insights/monitoring, SNSW had the internal know-how to set them up as part of deploying the data breach response engagement model.

8.3 Appendix C – Further detail on key participants to the data breach response

8.3.1 Response Team: Cyber Incident Task Force

In response to the identification of the cyber incident, a *special purpose team* called Cyber Incident Task Force (CITAF) was established to quickly carry out the necessary response actions to reduce the potential impact of the data breach and to:

- Undertake forensic analysis of cyber incident and customer impact (completed)
- Provide the necessary care and support for any impacted customers (ongoing)
- Meet agency obligations under legislations (ongoing).

CITAF decided to follow the federal OAIC's guide to managing data breaches.

The scope of the task force was to:

- Mobilise all necessary organisational and make available required resources to contain, assess, and respond quickly
- Direct focus of all workstreams and make informed decisions based on the analyses for optimal remedial actions.

Command and Control: The task force is chaired by the CEO SNSW (Recovery Lead) and jointly governed with DCS COO and NSW GCIDO.

Membership and Governance:

- CEO SNSW has authority for operational decision-making supported by DCS shared functions, informs Secretary and Minister.
- Task force workstreams report into the governance group which is chaired by the DCS Secretary and co-chaired by the DCS COO
- External advisors support all decisions makers and work streams through independent expert advice.

The key deliverables from the taskforce included:

- Understanding of the severity and level of harm and risk exposure arising from the breach and the actions that would be most effective in reducing or removing these risks
- Clear and immediate communication strategy that directed prompt notification of individuals on a case-by-case basis using a level of harm classification and prioritising those with severe harm profiles such a suppressed identity
- Documentation of the response plan execution and compliance with statutory requirements
- Instructions to all staff members to sharpen awareness of immediate mitigation actions and to avoid further data breaches

- Introduction of cyber security uplift measures for all IT and digital products for prevention and business process changes (on-going)
- Learning with independent subject matter experts where possible to leverage best-practices and ensure a ‘golden standard’ response to this incident commensurate to the reputation of DCS and SNSW (ongoing)
- Sharing lessons learned and develop DCS Cyber and Privacy Response Playbook that can be leveraged across the entire NSW Government (ongoing).

8.3.2 CITAF roles and responsibilities[11]

Stakeholder Engagement, Media & Comms	Incident Discovery & Impact Analysis	Customer Engagement & Support	Legal & Compliance	Security Response, Uplift & Transition	Business Process Change Management	Taskforce Project Office
Inform Minister, key stakeholders and obligatory entities	**Identify incident severity and impact to device optimal task force decision making**	**Notify all impacted customers based on harm-level**	**Advice of statutory obligations and support risk management**	**Implement rapid response measures for all IT and Digital Products**	**Prepare preventative business process changes**	**Manage and facilitate task force cadence**
• Brief Minister & Secretary • Notify mandatory entities • Notify impacted partner • agencies & private entities • Develop media strategy & comms strategy • Manage media enquiries • Communicate to staff • Establish escalation pathways	• Discover Incident details • Analyse impact to staff and customers • Identify • Establish customer "search function" • Assess level of harm • Assess category of harm • Develop impacted customer engagement prioritisation plan	• Establish hyper care model and inbound channels • Prepare escalation model based on impact severity and external agencies such as ID Care • Prepare customer correspondence templates • Train all SD staff to respond appropriately	• Advise on statutory obligations in accordance with acts and regulations • Define access roles and access rights for • Review and endorse customer engagements • Advise on risk profile and exposure • Analyse legal and financial risk exposure • Establish task force risk register & advise response measures • Prepare for performance audit	• Perform forensic assessment of mailboxes • Implement stronger mail client access control e.g. MFA • Implement immediate incident response measures • Implement stronger staff system access controls • Refine prevention measures in conjunction with software partners	• Explore changes to data handling and caching • Prepare strategy for light touch data usage for service delivery staff • Identify new ways of data access for all business process in contact centre, service centre and middle office	• Establish task force project office capability • Mobilise task force work groups and regular cadence • Manage daily workflow and action plan • Monitor task force workstreams • Log key events • File documents • Connect streams and support facilitation

[11] Document source: PMO Office

8.3.2.1 Key frameworks and policies that the CITAF team considered

- NSW Cyber Security Policy
- NSW Cyber Incident Response Plan
- Finance Service and Innovation Information Security Incident Management Policy and processes
- SNSW Security Incident Management Policy
- SNSW Records Management and Information Handling Policy
- SNSW Data Breach Response Plan
- SNSW Crisis Communication Plan
- DCS Risk and Resilience Framework

8.3.2.2 Legislation that CITAF team considered as part of the data breach response

- *Privacy and Personal Information Protection Act 1998* (NSW) (PPIP Act) – Regulates the handling of personal information, to the extent they are modified by the PIDs
- *Health Records and Information Privacy Act 2002* (NSW) (HRIP Act) – Regulates the handling of health information, to the extent they are modified by the PIDs
- *Data Sharing (Government Sector) Act 2015* (NSW) – Establishes the framework under which SNSW request data, the purposes under which NSW agencies can share data with SNSW according to the required data safeguards
- *State Records Act 1998* (NSW) – Regulates the archiving and disposal of state records, including data involved
- *Government Information (Public Access) Act 2009* (NSW) – Regulates access to government information
- Additional obligations under Commonwealth law including the *Privacy Act 1988* (Cth), the *Tax File Number Guidelines 2011* (TFN Guidelines)
- Section 353-10 of Schedule 1 to the *Taxation Administration Act 1953*.'
- *Crimes Act 1900*
- *Various other statutes were also reviewed, including statutes governing NSW statutory bodies such as BDM and Transport for NSW*

8.3.3 Data breach governance – Cyber and Privacy Resilience Governance Group

The Cyber and Privacy Resilience Governance Group (the 'CPRG Group') was established in May 2020. The CPRG Group is chaired, by the DCS Secretary and co-chaired by the DCS COO. The key purposes of the group are to:

- Provide executive-level leadership and oversight of response and recovery activities related to the cyber security incident and the data breach

- Lead the development and implementation of an ongoing DCS Cyber and Privacy Incident Recovery Framework
- Build resilience against major cyber security and privacy breach incidents across the DCS cluster and the NSW Government sector more generally to significantly reduce the risk of future incidents.

The work and focus of the group are being delivered in three key phases under the name of 'Project Trust':

- Phase 1 – Immediate response and recovery priorities – May to August 2020 (completed)
- Phase 2 – Establishment of Ongoing Resilience Framework/Pathway – July 2020 to June 2021 (ongoing)
- Phase 3 – Lookback, review and evaluation – (TBC).

In addition to the delivery focus noted above for each phase, the CPRG Group drives the overarching goal of building and strengthening resilience across the DCS cluster. At the time of writing this report a total of 9 meeting have been held.

8.3.4 Other participants to the response

The following participants were also involved in the response of the data breach:

Name	Roles
Commonwealth	
Services Australia	Services Australia maintains the Medicare database. It assisted SNSW to obtain postal addresses for customers without a driver licence. Services Australia was unable to share data with SNSW. however Services Australia did contact some customers whose Medicare or Centrelink data were compromised and played an active role engaging with vulnerable groups (e.g. people that may be having a cancer treatment).
NSW government agencies	
Births, Deaths and Marriages (BDM)	Once the PID under s 41 of the PPIP Act was made, BDM assisted SNSW during the data matching process to ensure that SNSW did not send notification letters to deceased people.
Cybercrime Squad within the NSW Police	Investigate the incident and look to identify and prosecute the offender/s. As part of their role they are required to record the incident in the NSWPF systems - which generates and Event number. This is particularly important to victims - who at a later date may need this reference number to establish their legitimacy and identity. Monitoring the Dark Web.
Firearms Registry	Assisted SNSW with the replacement of Firearms Licences. Firearms Registry have been provided a list of impacted customers. Impacted customers can engage with SNSW Hypercare to request a replacement

Name	Roles
	Firearms Licence. The Firearms Registry can generate the replacement card and send it to the customer without the customer having to attend a SNSW Centre.
Office of the Children Guardian	Assisted SNSW with developing a notification approach for minors.
Transport for NSW (TfNSW)	TfNSW administers the Register of Motor Vehicles DRIVES database which holds information about driver licence holders and registered vehicles including up-to-date address and date of birth information. Once the PID under s 41 of the PPIP Act was made, TfNSW assisted SNSW during the data matching process to obtain postal addresses. They also implemented a fast-track process for re-issue of new driver licences.
NSW Data Analytics Centre (DAC)	SNSW is using the services of the DAC to provide the secure data exchange mechanism for the information flow between SNSW, TfNSW and BDM. It has supported the data matching and washing efforts during the quality assurance process.
iCare	iCare administered a claim for cover from the NSW Treasury Managed Fund
Other	
Computershare	Mail house provider used to print the customer letters and send them by registered person-to-person post. Provided daily statistics on printing to SNSW.
Australia Post	Delivered the person-to-person registered letters. Provided status of letters delivered, returned or in-transit to the CITAF team.
Service providers to response	
CyberCX Pty Ltd (CyberCX)	Reviewed the analysis completed by CrowdStrike, the response and the status of recommendations. CyberCX undertook additional review and provided further recommendations.
CrowdStrike Australia Pty Ltd (CrowdStrike)	Completed initial analysis of unauthorised access to the SNSW Microsoft Office 365 and Microsoft Exchange hybrid environment.
Allens Linklaters and McGrathNicol	Allens Linklater, a legal firm with a specialist cyber forensic unit and McGrathNicol, a specialist cyber forensic technology firm was appointed by TfNSW to undertake the analysis of the 47 breached SNSW mailboxes with McGrathNicol to support
IDCARE	Assisted SNSW with the preliminary harm assessment and provided ad hoc data breach response advice. SNSW partnered with IDCARE to provide advice, assistance and support to its customers on a broad range of risks and exposures. IDCARE also provided training to CITAF management and played the role of customer advocate at the CPRG Group.
Information Integrity Solutions Pty Ltd (IIS)	Independent privacy advisor to CITAF. Conducted the Privacy Impact Assessment on use of PID to enable BDM and TfNSW to share

Name	Roles
	addresses. Led the independent data breach response review as set out in this report.
External legal counsel	DCS Legal utilised external legal services as required.

8.4 Appendix D – Examples of media articles relating to the cyber incident

Articles
14 May 2020
Medianet, 'Service NSW has been the target of a malicious phishing attack of data held within staff emails', https://www.medianet.com.au/releases/187283/
News.com, 'Service NSW emails hacked in cyber attack', https://www.news.com.au/technology/online/hacking/service-nsw-emails-hacked-in-cyber-attack/news-story/8c10641e8720fa353748bb7afc28f461
iTNews, Service NSW hit by email compromise attack', https://www.itnews.com.au/news/service-nsw-hit-by-email-compromise-attack-548134
9 News, 'Major cyber-security breach at Service NSW', https://www.9news.com.au/videos/major-cyber-security-breach-at-service-nsw/cka63oqmy000i0inucyv5eq5t
16 May 2020
Digital Journal, 'Australia: NSW hit by data breach via phishing attack', http://www.digitaljournal.com/tech-and-science/technology/australia-nsw-hit-by-data-breach-via-phishing-attack/article/571714
20 June 2020
Sydney Morning Herald, 'NSW government was warned over cyber security weaknesses', https://www.smh.com.au/national/nsw/nsw-government-was-warned-over-cyber-security-weaknesses-20200620-p554iu.html
2 September 2020
iTNews, 'Service NSW still waiting to notify on data breach after four months', https://www.itnews.com.au/news/service-nsw-still-waiting-to-notify-on-data-breach-four-months-on-552706
7 September 2020
Medianet, 'Service NSW notifies customers in relation to cyber incident', https://www.medianet.com.au/releases/191172/
The Sydney Morning Herald, 'Data of 186,000 customers leaked in Service NSW cyber attack', https://www.smh.com.au/national/nsw/data-of-186-000-customers-leaked-in-service-nsw-cyber-attack-20200907-p55t7g.html
9 News, 'Service NSW reveals details of cyber-attack', https://www.9news.com.au/videos/national/service-nsw-reveal-details-of-cyber-hack/ckes9yz47000w0gqfyrm7ak8h
iTNews, 'Service NSW reveals 738gb of customer data was stolen', https://www.itnews.com.au/news/service-nsw-reveals-hackers-stole-738gb-of-data-in-email-compromise-552932

Articles
7News, 'Service NSW cyber attack results in 186,000 Australians having their data stolen', https://7news.com.au/business/finance/service-nsw-cyber-attack-results-in-186000-australians-having-their-data-stolen--c-1297423
8 September 2020
The Mandarin, 'Information of 186000 Service NSW customers stolen', https://www.themandarin.com.au/139221-information-of-186000-service-nsw-customers-stolen-in-cyber-attack/
9 September 2020
iTNews, 'Dominello says Service NSW data breach victims getting 'Hypercare', https://www.itnews.com.au/news/dominello-says-service-nsw-data-breach-victims-getting-Hypercare-552999
10 September 2020
The Guardian, 'Service NSW hack could have been prevented with simple security measures', https://www.theguardian.com/australia-news/2020/sep/10/service-nsw-hack-could-have-been-prevented-with-simple-security-measures

8.5 Appendix E – Detailed analysis of customer support and experience

8.5.1 Assessment with obligations – both regulatory and publicly promoted

8.5.1.1 Public commitment to the customer and delivering service excellence

NSW Government has six overarching published customer commitments, which are: Easy to engage, act with empathy, respect my time, explain what to expect, resolve the situation and engage the community

SNSW's strives to be a leader and innovator within government. It holds itself to an even higher standard as it was founded to deliver more customer centric, seamless and holistic access to Government. SNSW's makes multiple Public Commitments on service excellence, including its vision which is about being a leader in service provision and its mission to put customers at the heart of everything they do.

NSW Government Customer Commitments

- Easy to engage: Make it easy to access what I need. Make it simple for me to understand
- Act with empathy: Show you understand my situation. Treat me fairly and with respect. Provide service in my time of need
- Respect my time: Tell me what I need to know beforehand. Minimise the need for me to repeat myself. Make what I need to do straightforward
- Explain what to expect: Be clear about what steps are involved. Contact me when I need to know something. Let me know what the outcomes could be
- Resolve the situation: Be accountable for your actions. Be clear in decision-making. Reach an outcome
- Engage the community: Listen to the community to understand our needs. Ask us how we want services delivered.

IIS findings:

NSW State Government and in particular SNSW both have a strong public commitment to the customer and delivering service excellence.

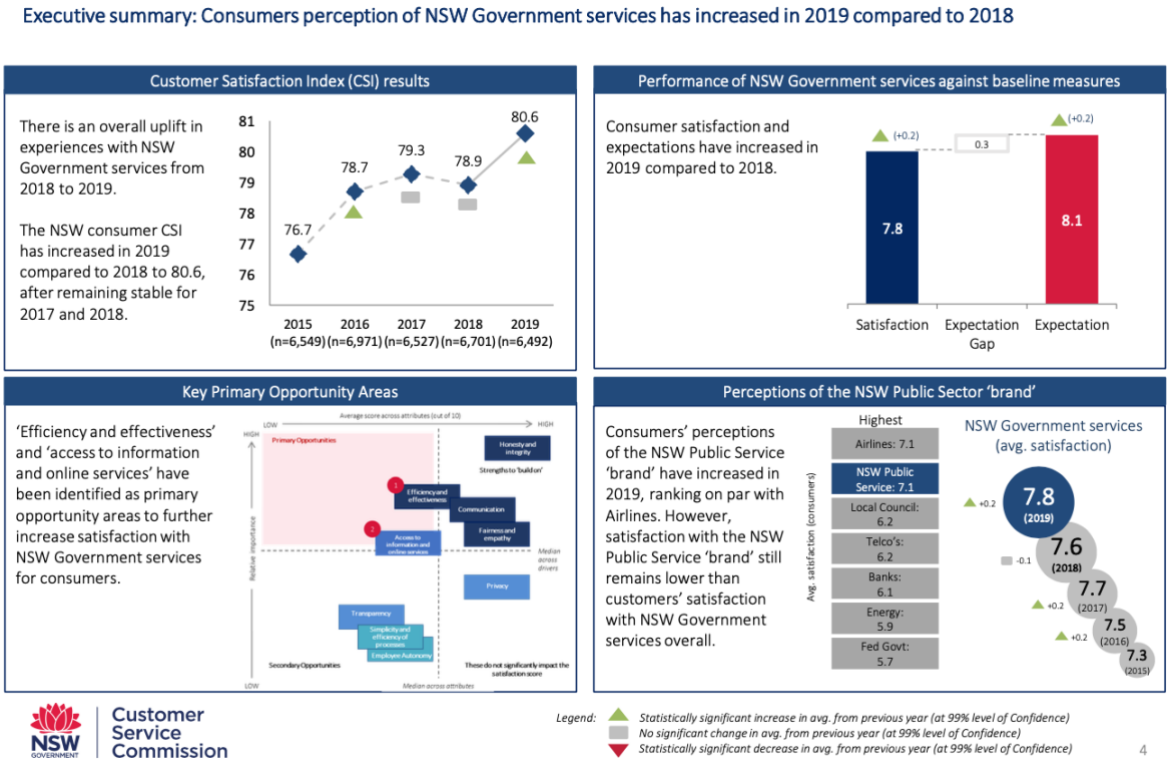
8.5.1.2 Existing service quality at NSW Government and SNSW

Based on the 2019 in annual Customer Satisfaction Measurement Survey, consumers perception of NSW Government services is strong relative to other comparable Government jurisdictions and has increased in 2019 compared to 2018. Consumer satisfaction (7.8) and expectations (8.1) have increased in 2019 compared to 2018, however there is still an expectation gap (0.3).

SNSW (again relative to other comparable Government jurisdictions) received higher scores across all attributes compared other services providing similar interactions. The employee attribute of 'get

things done quickly' (processes reduce wait times' and 'get to the right person first time') had the largest positive difference in scores. Informative staff, efficient services and an omni-channel experience (easy and efficient) contributed to high consumer satisfaction with Service NSW.

Extracts from 2019 NSW Government survey on Sentiment and Satisfaction:



Consumers and businesses who interact with Service NSW have higher expectations, satisfaction and comparison to ideal scores

Key Points

- Consumers and businesses who interacted with Service NSW, score higher across all outcomes measures as well as trust with NSW Government services.
- For consumers, the most common Service NSW interactions include 'apply/renew/modify car registration' and 'apply/renew/modify drivers license'.
- For businesses, the most common Service NSW interactions related to 'apply/renew registration for business vehicle' and 'renew driver's licence for business purposes'.

Figure 6.1: Outcome measures by Service NSW vs Non-Service NSW - Consumer

Figure 6.2: Outcome measures by Service NSW vs Non-Service NSW - Business

Figure 6.3: Top 5 Service NSW interaction types (by frequency) - Consumer

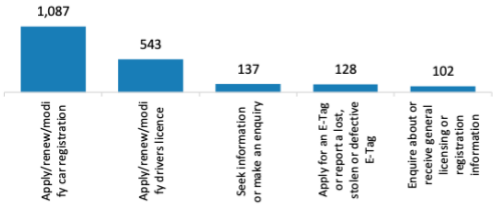
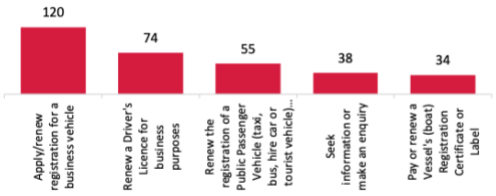


Figure 6.4: Top 5 Service NSW interaction types (by frequency) - Business



Customer Service Commission

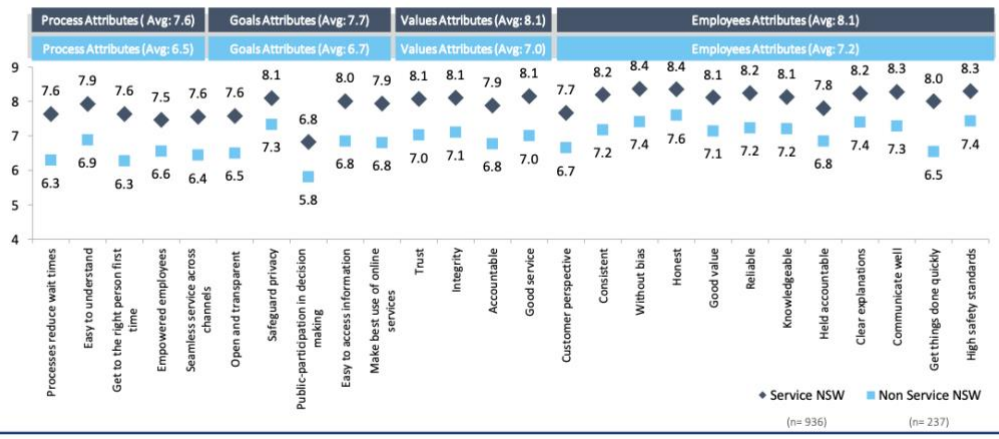
97

Service NSW scores higher across all attributes than other services providing similar interactions for consumers

Key Points

- Service NSW received higher scores across all attributes compared other services providing similar interactions.
- The employee attribute of 'get things done quickly' had the largest difference in scores, with Service NSW consumers scoring 8.0/10 whilst consumers who received the same service from another provider scored the attribute on average 6.5/10, a difference of 1.5/10.
- Process attributes had the largest difference in overall scores, of which 'processes reduce wait times' and 'get to the right person first time' both scored 1.3/10 higher for Service NSW consumers compared those who interacted with other service providers.

Figure 6.13: Average score of consumer attributes – Service NSW vs. Non Service NSW – For Service NSW interactions (out of 10)



Customer Service Commission

100

IIS findings:

NSW Government as a whole and SNSW specifically had strong customer sentiment and satisfaction scores in 2019.

8.5.1.3 Pre-incident readiness for a large-scale customer-focused breach response

SNSW is a busy operational business that as one staff member interviewed described it 'is used to dealing with customers individually and one transaction at a time' and not through mass communication campaigns.

On one hand it had many of the key skills capabilities needed to implement the response, plus it had a strong cultural alignment with supporting the customer. However, there were specific gaps in capabilities including customer insights and opt in information, forensic skills, data privacy, etc.

Assessment of the capability gaps and strengths SNSW faced moving into this event gained from interviews with the staff /team.

The following table outlines capability 'gaps' and strengths that were either mentioned by staff and / or evidenced through the breach response to date:

Aspect	Capability gaps	Strengths
Strategic Readiness	• Past experience in managing large scale breach communications and support responses • 'Ready-to-go' breach response op. model Working relationships with all agencies / at the correct levels and role	• Strong customer centric couture, • Culture of innovation, • Strong leadership
Cust Access / Insights	• Full customer contact and demographic information • Customer opt-ins – right to contact	• Empathetic staff skilled at managing customer issues and concerns, • Authority with customer as a central government agency • General customer insights about how customers (including staff) respond to breeches (expectations, preferences and behaviours) from IDCARE
Process and Technology	• Developed customer journeys and configured breach response systems. • Specific gaps in technology and systems e.g sales force modules, end to end reporting	• Established call centre, service centres and CRM system capabilities. • Transactional capabilities via service centres and partner agencies

	• Tested letters and communications	
People and Resources	• Sufficient available skilled support resources, including existing team dealing with bushfire and Covid 19 response • Analytical capability to review unstructured data and frameworks to help prioritise customers and action by category • Specific skills and experience managing large scale simultaneous mailing • Existing mail-house relationship	• Access to tested / successful IDCARE service/solution and insights • Range of Government agency / support services

IIS findings:

SNSW had mixed levels of pre-incident readiness when it came to quickly implement a large-scale breach response. While it had significant capability gaps and strained resources, it also had an aligned customer centric culture and the benefits of significant call centre and service centre operation and significant core capability in terms of Customer Support / Experience.

8.5.1.4 The support solution implemented

SNSW approach to providing customer support

The SNSW team have displayed a deep (culturally embedded) commitment to support the customer through the incident response process. They were energised in the agile way they set up the response team despite being somewhat weary after recent bushfire and Covid-19 workloads.

Best practice approach: They were ambitious in terms of the 'gold-star' solution selected which involved them deciding to contact all 186,000 impacted customers with personalised letters, offering customers a range of support options and furnishing care teams with training, bespoke operations and accurate details of the breached documents. IDCARE, who has seen a number of similar response efforts, is complementary about the scope and detail of the letter and support services and the detail thought and effort generally.

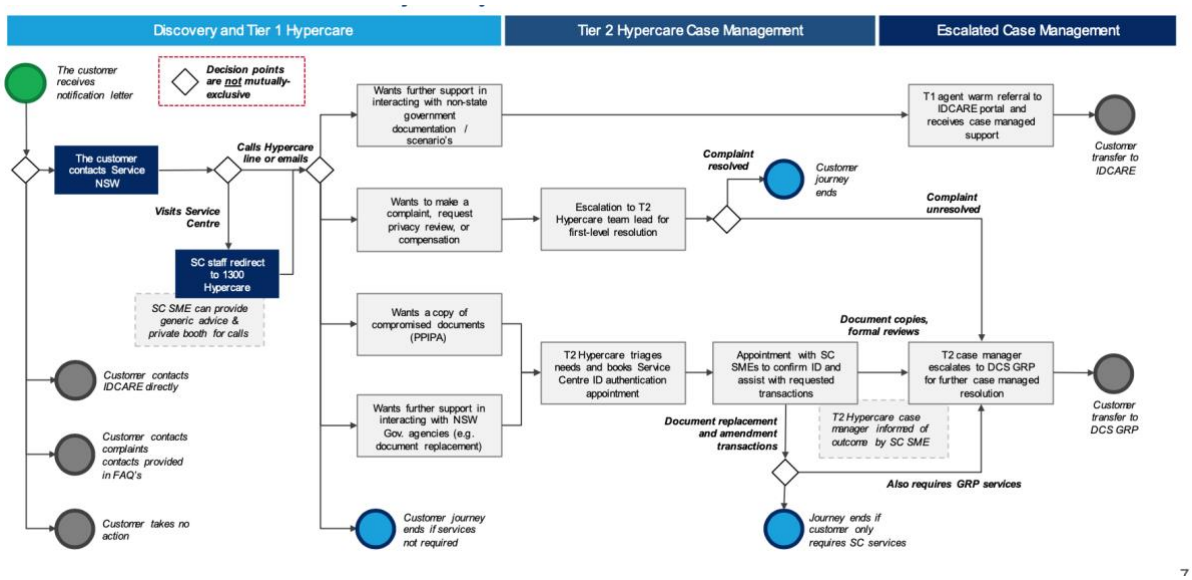
IIS findings:

SNSW displayed positivity, agility and commitment when responding to the breach.

The solution design:

The customer support system (see diagram below), was designed with two tiers of call centres and thus effectively gave SNSW a better ability to deal with any large influx of demand (Hypercare Tier 1

could act as a triage point to diffuse, log / book a longer customer call-back and the second Tier could then schedule a call to provide more support). The Hypercare and IDCARE support, combined with self-help material and links sent with the letter and available online, also gave consumers choice and options. Hypercare Tier 2 was designed to explain the letter and give each customer details of their breached documents, while also providing options for actions to mitigate risk. IDCARE and Service Centres acted as 'hand-off' points for customers needing deeper – expert – support and / or fast-tracked transactions.



IIS findings:

The experience design solution was designed with Tiered Call Centre Layers which by default provided flexibility in dealing with large (and initially unknown) volumes of consumers seeking support while the range of service options also provided customers with support / service choice.

<u>The question of notification approach vs timing:</u>

The CITAF group discussed the following priorities for the customer notification and support

- Timely Notification
- Clear informative and accurate notification communications
- Being able and ready to provide support to customers after the letters are sent.

As the challenges of working with huge quantities of unstructured data slowed down the notification process, DCS/SNSW decided to prioritise having full data before notifying taking into account advice from a number of independent sources. For several months, there was a natural tension in the management meetings between the desire for rapid notification and waiting until full information and support was available before sending letters out. Alternative options – including sending a mass communication with general information – were considered multiple times.

Expert advice from IDCARE informed SNSW's decision to understand the impact prior to making a comprehensive notification. If a notification had been provided earlier, negative customer sentiment

would have followed a general notification letter, as the details of the breach would not have been able to be communicated. Concerned customers may have also experienced significant wait times in call centres and services centres, with no definitive information being able to be provided. TfNSW would not reissue NSW driver licences, nor could other agencies place blocks or protective measures to systems without first identifying compromised data.

SNSW considers that the low ratio of calls to letters and the low number of internal review and compensation requests support the approach taken to provide a comprehensive notification letter.

IIS findings:

Decision was aligned with Leadership vision / priority of customer support.

Leadership vision:

Customer priorities were debated and set at senior levels: The CITAF Leadership Team, met regularly to shape the incident response solution design and delivery. They identified 3 Customer Priorities on 20/8/20. There was significant ongoing debate about the inherent tensions between Priority Level 1 and Priority Levels 2 and 3.

- 'The sooner we notify the customers the better to empower them to understand their situation and be able to respond'
- 'We must place a strong focus on how we notify impacted customers – communications needs to be clear, informative and most importantly accurate to minimise additional risks and harm'
- 'It is essential we are ready to support customers following notifications going out. To this end Hypercare has been established in partnership with IDCARE and partner agencies'.

8.5.2 Customer response (system volumes and feedback)

8.5.2.1 Channel performance and volumes to date

On 19 October there were 4,378 active or closed cases with only 19,922 letters delivered. This response rate of 22% is higher than the expected 10-15% customer engagement. It has potentially been bumped up by the extra media attention and the dominance of category 2 (Identity Risk) customer cohorts. It is unclear what the true response rate will be. The team has had to create new reporting views/scorecards, specific for the incident. Given the potential impact on service, the ongoing response rates will require vigilance and management. They can, however, potentially be managed by postponing/tweaking the timing of future batch sends.

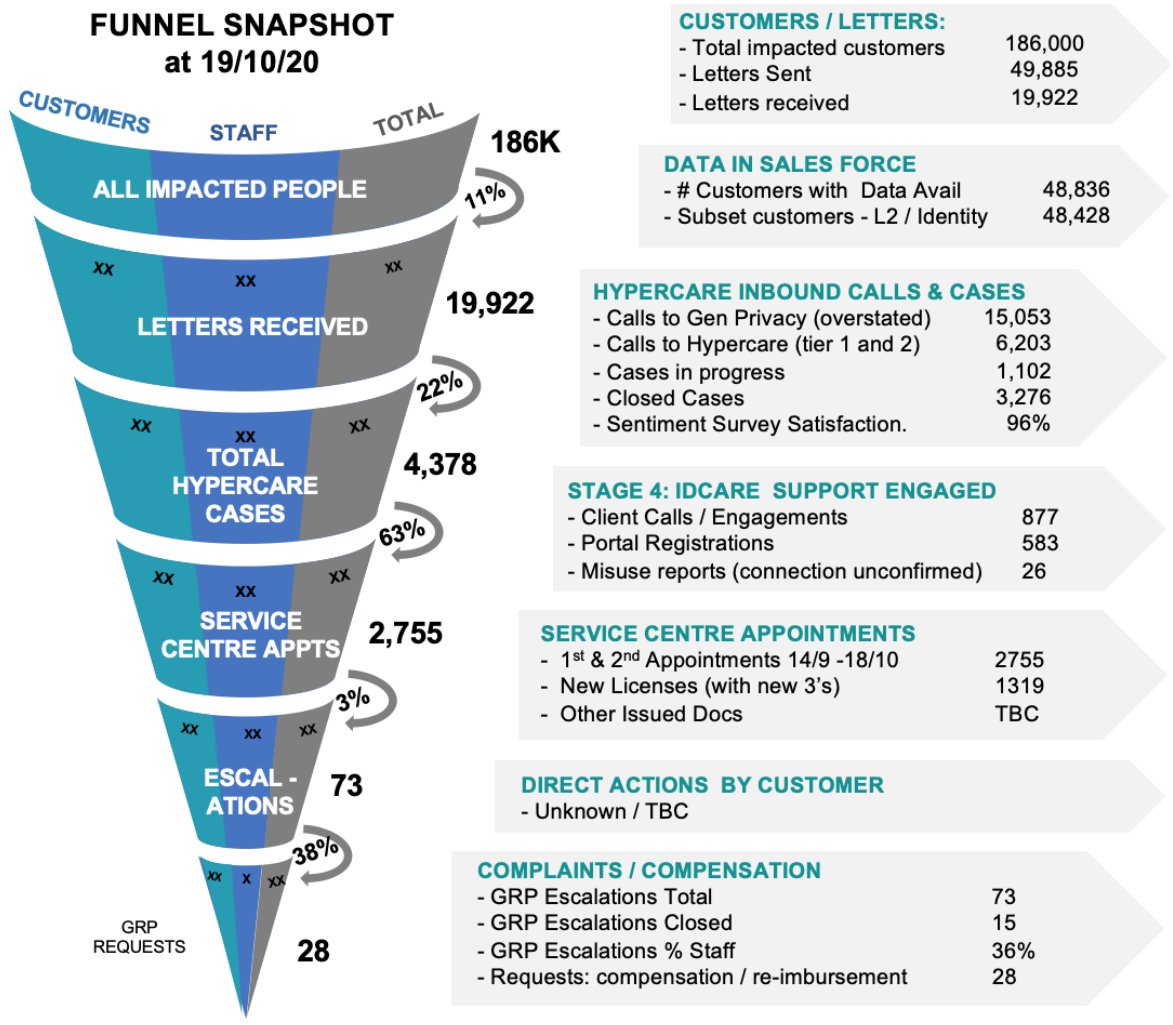


Figure 7: How customers flowed through support layers (snapshot at 19 October 2020)

IIS findings:

The channels have performed well in terms of supporting volumes, although volumes may be larger than anticipated and monitoring and forecasting volumes remains important and challenging.

8.5.2.2 Operational metrics

Acceptable Service Levels at Hypercare are similar to SNSW overall

SNSW Channel Performance Metrics (overall including privacy) for the period 7 September to 17 October – show an impressive CSAT score of over 95%.

Metrics

Frontline Channels Performance Metrics
7 September 2020 – 17 October 2020

	CSAT	Grade of Service	Wait Times	Average Handling Time	Cust. Withdrawals
Service Centres	98.03%	77%	6:24 minutes	7:05 minutes	1.27%

	CSAT	Grade of Service	Average Speed Answer	Average Handling Time	Abandonment
Contact Centres	96.7%	69.2%	2:04 minutes	7:01 minutes	6.84%

For the same period the Hypercare Team / privacy calls were slightly outperforming (at 83.3% vs 81.5%) the business generally on 'Meets' or the percentage of calls meeting SNSW acceptable service metrics.

Call Quality

Call Quality Metrics, September 2020 – October 2020

	Meets	Does Not Meet
Service NSW	81.5%	18.5%

	Meets	Does Not Meet
Hypercare Team	83.3%	16.7%

Hypercare Service Levels have only dipped slightly since the media announcement in September. If we compare Hypercare Performance (7 September to 17 October) of 83.3% with the prior period (7 May to 8 September) of 88.38%, we can see that the Hypercare team suffered only a slight drop in service after the press release and public announcement.

IIS findings:

Operational metrics have been maintained at good levels, even after the press release in September.

8.5.2.3 Customer feedback and customer service feedback at Hypercare

CSAT scores at Hypercare are high for an incident response and very similar to those for SNSW overall:

- SNSW Channel Performance Metrics (overall including privacy) for the period 7/9 (press release) to 17/9 – Show a CSAT score for call centres of 96.7%.
- By way of comparison the Hypercare CSAT measures for the incident / privacy team (based on 219 responses) at 19/10 show a similar result.
- The cumulative satisfaction score of 96% (81% extremely and 15% somewhat satisfied) and a dissatisfied score of 3%.

The 2019 Trust Index was provided, as the 2020 one is still being drafted and thus provides an opportunity to explore trust and brand impacts from the incident in more depth (i.e. by adding extra questions). Alternatively, a separate study by segment may be required to better understand the impact of the incident on brand, trust and intent to use SNSW, in full.

What customers (and impacted staff) are saying: The following themes have been pulled together from the free text CSAT survey and also interviewing front line staff.

Positives

- The Hypercare staff were almost universally found to be extremely helpful (compassionate, supportive etc).
- The services provided were appreciated and used.

Neutral

- There was mixed awareness and experiences at the service centres – they were not always aware and the process did not always work resulting in customers having to perform extra visits or staff calling Hypercare.
- The broader ecosystem of banks, agencies and government partners were only partially aware of the incident and the agreed support services. A customer contacting a number of entities may have found 50% were aware of the incident.

Negatives

- Customers impacted have been surprised and unhappy that their identity was compromised in the first place and disappointed at the unprofessional practices that let this happen.
- Customers and staff are extremely surprised and unhappy about the excessive time taken to notify them. Some commented that they do not think this was in their best interests as they were left at risk during this period.
- For many, the letter was long, vague and confusing and would have not been suitable for many (elderly, English as a second language, etc.). Many people calling Hypercare had not read it and a major task at both Hypercare 1 and 2 was explaining the letter.

- Overall, the process (of steps / calls / appointments) the customer had to go through was long, convoluted and required significant effort from the customer. Particular pain-points included not getting all the information in the first call and having to have a call back and the fact that there were two appointments at the Service Centre.

See the following word cloud comprising most frequent words/phrases used by customers in the feedback free text fields. It demonstrated both positive and negative aspects.

IIS findings:

Feedback shows staff performance is strong and redressing much of the inevitable negative customer negative sentiment in the breach scenario. Customers are dissatisfied about the breach occurring, the length of time taken to be notified and the work and time (for them) involved in engaging in the process.

<u>The notification letter</u>

The letter was designed to support, enable and empower people to act and as such it was information rich. We do not know if it was effective as we have not tested it and we cannot contact non responders to check their experience. IDCARE praised it as best practice relative to others. Nonetheless, it did not suit all customers and generated a great many complaints (at Hypercare and IDCARE) as being far too long, complex and yet also vague as it was not specific about the documents breached.

IIS findings:

Many customers calling Hypercare mentioned they had not read the letter (and they were then taken through it). This could have been a function of their segment / style / characteristics and is not necessarily a failing as the service was available for the letter to be reviewed/explained by both Hypercare Tier 1 and 2. We do not know how the letter worked for people who did not respond (was it understood and did it drive appropriate actions).

Batch send decision:

As the data of quality failed, the timeline was pushed back further, SNSW adapted the plan and decided to send the letters in smaller 'just-in-time' baches. This enabled a just-in-time approach and minimised the impact on the timing of notifications.

IIS findings:

The batch system has allowed notification to commence. It also provides some controls against excessive demand reducing service at the call centre (e.g., should there be an event (media etc) that drives excessive calls).

Hypercare

IIS findings:

The Hypercare CSAT performance of Hypercare has been excellent. While customers were not necessarily happy that the incident occurred and there were mixed feelings about the customer experience (ease and seamlessness of the end-to-end solution), they overwhelmingly praised the quality of service provided by the HyperCare Team. 97% of customers felt Somewhat or Extremely Satisfied, 82% Extremely Satisfied, 2% Dissatisfied with the staff interaction. Most who left a comment praised the team.

IDCARE

As at 19/10/20 IDCARE has received 877 calls, 52 emails and 583 Web enrolments (to its portal which contains extensive content and help). IDCARE provide a support service for the most needy and or anxious customers and as such free up Hypercare Tier 2 resources. They also record (and escalate) potential cases of misuse of data that may be attributed to the incident. There have been 26 of these reports, none of which have yet been formally attributed.

IIS findings:

The IDCARE experience has also been well received: We have limited information, but anecdotally Tier 2 operators say their customers value the IDCARE service.

Service Centres

By 18 October, the service centres had conducted 2755 (first and second) privacy appointments and issued 1319 new drivers licenses among other transactions.

IIS findings:

Initially there was some variability in the quality of engagement between service centres and Hypercare and this had a negative impact on customers. Customer – and staff - pain points have been identified and addressed. One of the biggest customer pain point is that customers often didn't understand the fact that two appointments would be required to issue a license. Additionally, there was a lack of availability of appointments at some centres (resulting in long waits) and also some customers turned up for a booked appointment and no staff member was available at that time.

Finally, in terms of relationships between Hypercare and Service Centres, there were some reports of service centre staff pushing back and even some cases of a 'them and us' attitude. We have been advised that these teething problems have now been addressed through normal quality control and feedback processes.

GRP complaints and compensation escalations

IIS findings:

Most people who have accessed this service have either requested information on how the incident happened, wanted to see their breached documents and / or have complained about the breach occurring, the time taken to be notified and or the effort involved in rectifying a situation that they did not cause. Compensation claims have been frequently about requests for compensation for time vs harm or risk and as such cannot be granted under the current frameworks (other than for staff who have been granted time in lieu). This unfortunately – despite the great efforts of the team – has a negative impact bon satisfaction. It has been noted that this policy (of not providing compensation for time) could be changed and the process is ongoing.

Staff support / HR and internal comms:

We have been advised that staff were disappointed (some angry) they had not been informed before customers and that they got the same letters as customers. They wanted and expected to be treated as part of an inner circle and be communicated to personally. Some who were notified through their managers, as is the norm for key internal announcements, received the news far better. Communication was done non-simultaneously as some staff were tapped on the shoulder and this filtered through the organisation and created negative 'chatter'. Some useful internal communications were conducted e.g., video briefings with Q&As (and received well) but management believe that a more coordinated process where managers cascaded messages down to staff supported by more senior top-down comms would have worked better.

Some adaptive changes were made to further support staff: Staff (and Ex-Staff) received comms and support and also some extra communication and services (in terms of days in lieu etc.) were put on for staff whose information had been breached. Staff were also serviced by support staff who were not peers to ensure privacy

IIS findings:

Staff as a segment needed special consideration. Management have commented that in future staff communication would be more layered, leverage managers and team leaders briefing staff in huddles (as is the normal practice) and include more senior staff comms earlier in the process

Partner engagement and the broader customer ecosystem of support

Going into the breach SNSW did not have equally established relationships with all partners and significant work was done here to build them. SNSW usefully arranged an incident police reference number that is designed to legitimise and support the customer in explaining the situation.

Customers report an extremely mixed bag of awareness of the incident at partners (banks / agencies etc) and even in relation to the agreed fast track or support processes to be provided. As an example, one customer / impacted staff member went to 6-8 entities and approximately half of these institutions had no knowledge of the event.

Partner CSAT: 7 agencies have responded to the CSAT partnership survey and while feedback about SNSW's performance is generally positive there are some mixed results about whether SNSW had responded well to the breach and about the effectiveness of its communications. Nearly 60% said they had allocated 5-6 FTE's to working on the breach. This survey was very brief and a more detailed debriefing / feedback process may be useful – ensuring engagement at both management and operation levels.

IIS findings:

The end-to-end process for customers (i.e. ending with taking action at a third-party agency or bank) was not necessarily seamless and some partners were unaware of the incident or related support services /arrangements.

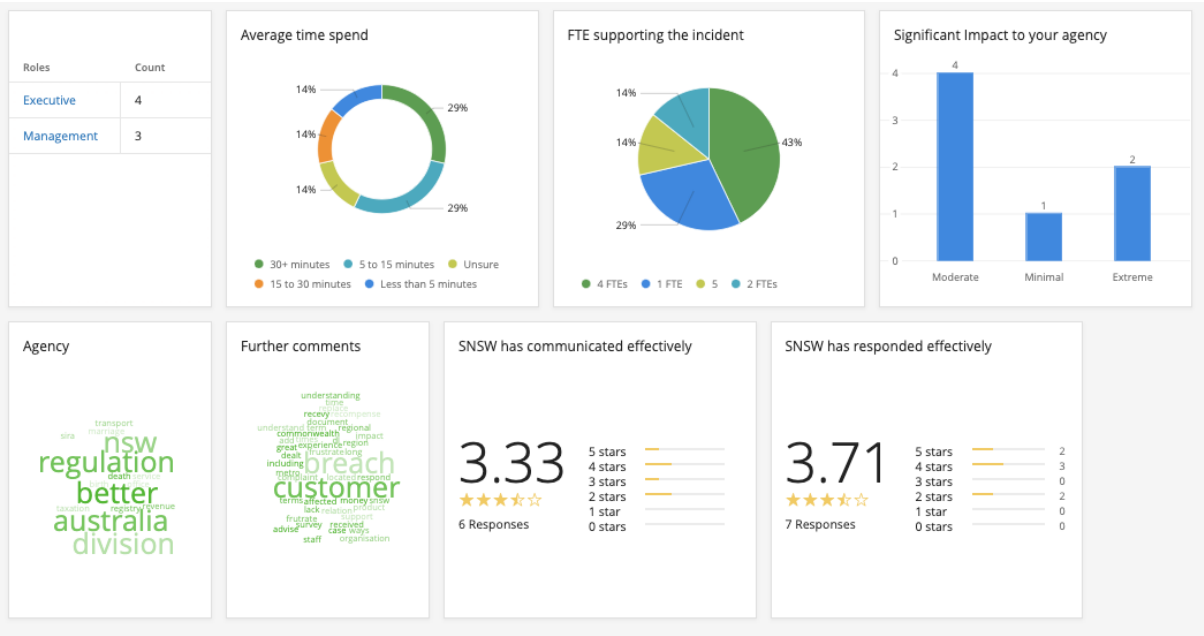


Figure 8: Partner Survey Highlights[12]

Overall IIS finding for customer feedback:

After reviewing the whole response / system, most support touchpoints worked effectively. Customers did comment that it was complex and required customer effort. Given timeframes and the fact that the solution was 'spliced together' from BAU services across multiple agencies to a large degree this

[12] Produced by SNSW Partnership teams

could not be avoided, however in future this could potentially be improved. There was also some confusion about the roles (and similar names) of entities and number of case managers. This also could be reviewed for the future. Despite the above , the staff performed well and were key in driving up satisfaction and creating 'Bridges' between services.

Observations: Customer experience pain points, opportunities and future learnings

Customer steps in the process and overall customer effort levels

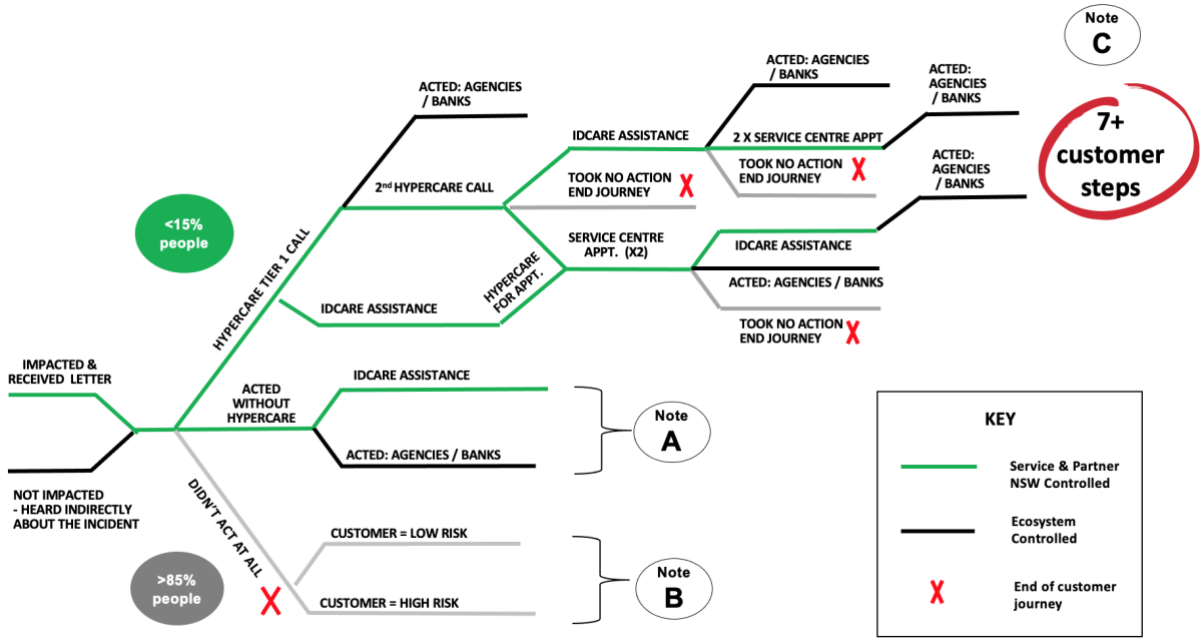


Figure 9: Illustrative master customer journey (IIS)

Pathway diagram: Demonstrates number of customer steps – and the unknown pathways of non-responders. The above diagram represents an illustrative (non-exhaustive) overview of the main types of customer pathways through the SNSW (and partner) Service Delivery Framework. The green lines represent the Service Delivery Framework that SNSW and its partners have established as engagement model.

IIS findings:

The journey is very time intensive for customers. Overall customer experience design resulted in many customer steps and significant customer effort (minimum 7 steps /hours). There are at least 7-8+ customer steps each of approximately an hour (calls, meetings, appointments etc). For customers taking this full Journey (see note C). This could be much greater (20+ Steps) for customers seeking to address multiple types of breached documents with 3rd party agencies and or who engage Hypercare or IDCARE multiple times and or who complain or seek compensation.

Number and type of handover points between 'Services'

Feedback from the complaints team and IDCARE both indicated that some customers commented that they were confused about the number and role of all the different entities and in particular the multiple Case Managers (Hypercare, DCS Complaints and IDCARE). Hypercare is effectively the master case manager and performs the role of issuing CSAT surveys, calling back customers and or closing the case. This was not always understood.

IIS findings:

There are multiple handover points and at least three case managers (Hypercare, IDCARE and DCS). Although largely well managed the sheer, complexity caused some customer confusion, in particular with regards to role of different Case Managers and name of agency (IDCARE vs Hypercare).

Overall customer effort, its impact on satisfaction and measurement

In addition to the timing of notifications and the breach occurring in the first instance, most people that complained and or sought compensation were annoyed about the effort and work they had to put in to rectify their risk situation – a situation that was not their 'fault'. This was exasperated by the multi-step process and number of different support services and case managers. Ultimately, they were annoyed about the time spent and some wanted compensation for this time. Eventually staff were given compensation in the form of time in lieu, but customers were not compensated for their time. Ironically the process of complaining and seeking compensation took even more of their time and did not result in compensation. Requests for compensation can be considered on a case-by-case basis. This is ongoing.

IIS findings:

Customer effort was a key metric not measured. Customers resented spending their time on an issue that was not their fault generally but were required specific extra effort to complain. Time lost / spent is not considered a valid cause for compensation, yet it is important to the customer.

Flexibility of system design and ability to adjust process based on demand

The two Hypercare call centre touchpoints gives SNSW flexibility in managing potential high customer call volumes. However, for customers, Tier 1 is effectively an extra step that, for many, does not add customer value but increases work/time for them. Customers expect to get extra detail during the first call but don't receive this detail for 2 days or until the Tier 2 call-back. Feedback suggests customers value the general information about the process and appreciate being taken through the letter on a step-by-step basis in the first call. The Hypercare staff have done an excellent job of managing customers through their initial disappointment in not getting more clarity and have typically managed to calm upset (venting) people down and arrange the subsequent call-back.

The Hypercare model has been clearly defined and endorsed based on input from IDCARE and IIS. The pathways into the service are via 137788 and by the dedicated 1300 number, which is provided on the notification letter to impacted customers.

On 19 October 2020, 15,053 calls went through the general privacy line. This comprises general public who have not been sent a letter and those who googled the 'general ' number rather than calling the number on the letter plus people using the quick dial (#1) which used to be a popular

transport channel. By the same date 6203 calls had gone through the dedicated number printed on the letter. This included first time callers to Tier 1 and people calling a Tier 2 case manager. For clarity of process and to understand volumes (given calls are very high relative received letters) the team are continuing to review this for the purpose of capacity planning.

IIS findings:

The two Tier Hypercare design caused extra customer steps and anxiety but provided system flexibility. It may be more flexibly designed in the future and potentially collapsed into one single step when call traffic allows this.

Harm segments and how they worked in practice

Customer segmentation into 'Harm' or Risk Groups based on their categories of compromised data: This categorisation was based on 98 PII markers, concentrated to 27 groupings. Customers in Risk Group #1 (Safety) were prioritised for notification before those in Group #2 (identity) and so on.

These were assessed at the beginning of the process and not reviewed when full extent of the breach and the data was better understood. As raised previously in the report, IDCARE were surprised they were not re-engaged to interrogate them and revisit. Some insights from the call centre team suggest there may have been opportunities to improve and or streamline them.

While this approach was useful and logical it was complex. Hypercare staff advised that there are some significant cohorts of customers for whom the outcome of the process is unnecessarily long-winded and stressful because the classification was potentially applied too literally and did not necessarily have an appropriate reality check.

Example 1 – High harm rating but single insignificant data element was breached: A significant number of customers in a high harm category with a single relatively minor personal information marker breached (e.g., expiry date of drivers-license or name of Bank). Their letter indicates either driver's license or bank acc. details have been exposed. Customers assume the worst (e.g., scan of whole driver's license breached – and are advised this is a possibility by Tier 1) and experience building stress for 2 days until Tier 2 advises the breach is minor (even if the harm category is a relatively high one).

Example 2 – Customer with high volume of breached elements has an overwhelming experience: Long letter and two complex calls reviewing all the potential categories / documents with Hypercare before understanding the extent of the breach: Customers with multiple breached docs (for whom the letter is especially complex and long. For similar reasons they may benefit from being fast tracked to Tier 2.

IIS findings:

The harm segments were not reviewed after the extent of the data that had been breached was known, nor were they given a 'reality check review' when customers started flowing through the system. Staff have advised that there were groups of customers for whom the harm segments, and their application could have been enhanced to improve customer experience and reduce volumes of letters / customers contacted.

Segments of Focus (All impacted customers versus those who engage)

Overall it remains to be seen if this exercise was justified based on cost effort and customer value added / sentiment impact. SNSW has been constrained in terms of not being able to conduct customer research beyond CSAT surveys for the minority calling Hypercare. It cannot contact non responders (due to the announcement that SNSW will not recontact customers – done to reduce scammer activity and risk). It has limited insights on how well the letter worked in driving action for the majority who didn't call Hypercare or IDCARE. We would recommend reviewing the customer insights where available and assessing the re-contacting decision around an exception for research.

The registered person-to-person letter was a central part of the strategy and was intended to prevent the majority of impacted customers from calling. It assumed (based on advice from IDCARE) that the vast majority of recipients would choose to act independently (if at all) to reduce their risk and only 10-15% would call Hypercare. We do not have any research into people who received the letter but did not contact SNSW. We do not know how the letter was understood and whether it drove action as appropriate – or the overall sentiment of people ended here.

IIS findings:

There is an overall lack of 'big picture view' of all customers. Specifically, there is a lack of customer understanding, engagement and action outcomes for the majority who did not contact Hypercare. A decision has been made by CITAF that no research can be done, as it could further breach customer privacy, which has had a big impact on insights and learnings.

Review of how support and resources were prioritised

There was an initial process to directly contact high risk customers in harm categories 1 including minors, people at risk of domestic violence etc. This appears to have been very thoughtfully scoped and executed in conjunction with partner agencies.

However, there have been customers in harm categories 1 and 2 who received the letter and have not contacted SNSW or responded to Hypercare. They may not have acted to reduce their risk but their response is unknown. These customers have not been followed up on by SNSW. Some may be old and or have other capacity related reasons why they have not acted.

It should be noted that the system design is effectively 'self-service' and as such deals with a subset of customers that may well have higher risk but may also have personal factors that drive them to have higher levels of anxiety or preferences for support and service vs self-management of risk mitigation actions. As such, SNSW has not necessarily been focusing time on those with the highest risk related need. Its decision not to recontact customers has meant it has not followed up with high-risk customers who don't engage / call. This arguably works against the overall aim of enabling action to minimise i.e., to 'support customers and empower them to take action to minimise future risk'.

IIS findings:

Time may not have been proportionately spent on those with the highest risk related need but rather be skewed towards those who valued the support. The decision (and subsequent announcements) not to recontact people who don't engage has resulted in a situation where SNSW cannot recontact

high risk customers who have not contacted / engaged or obviously taken action. There are potentially segments (elderly and or disadvantaged) who are in high-risk categories who would value more proactive support.

8.5.2.4 Observations about customers: Journeys and segments

SNSW has a reluctance to label or segment customers too much, however segmentation can be useful for system and service design – particularly when cohorts are so large and could benefit from variations in service design.

A range of customer behaviour and segmentation related insights have been synthesised in the section below (untested and from a relatively few interviews with HyperCare and IDCARE only). These include insights /comments on customers service style (Do it for me (DOFM'ers) vs DIY'ers) and also on how customer personas were demonstrated, as noted below.

The following insights relevant to segmentation could form useful segment overlays for future incidents

- **Potential Harm Grouping Overlay / Tweaks**

  The Harm Groupings proved logical and useful; however, call centre staff mentioned a couple of scenarios where they (combined with a two tier Hypercare process) drove complexity for the customer. One example is customers with a single, minor PII marker that has been breached (e.g., expiry date of drivers-license or name of Bank). This person should have probably been eliminated from the process which gave them anxiety but no ultimate reason to act.

- **Personas**

  In addition to the harm segments used to prioritise action, the team naturally anticipated a range of different types of customer needs and behaviours reactions. IDCARE, who conducted useful training in this aspect, introduced the concept of behavioural groupings in the form the following three Customer Personas:

  - 'Confirmers': Wanting to make sure they understand what they are reading/hearing and next steps
  - 'Catastrophisers': Irrational, dramatic, thinking, imagining worst case scenarios
  - "Venters': Angry disgruntled, seems nothing will satisfy them.

  These 'personas' were subsequently largely ratified by the staff as being useful. SNSW is reluctant to record or label a customer with any one persona – however could potentially explore how they can be used in training and or to derive smoother more informed handovers and better reporting.

- **Service preference**

  DIYers: These customers have a preference for being enabled to act directly on their own. IDCARE mentioned using these segments and they are commonly used in high involvement customer services like financial services. On reflection, the letter was effectively designed

for them. Unfortunately, we have limited information on whether they appreciated the letter, followed the suggestions and took action to reduce their risk (consider research options).

DOFM'ers: Conversely these are the customers that prefer to call the service centre and be stepped through something or have it done for them. Many customers calling Hypercare appeared this way. They had not read the letter (too much effort) and expected to be helped through the process, step by step.

- **Staff and power-users as segments**

  Staff: were generally more upset than customers as they had deeper trust levels and expected to be informed early and by their managers in a personal way rather than via the same letter that customers received. A bespoke communication programme and support layers are required to ensure staff remain positive.

  Power-users: Theoretically the more deeply engaged customer groups (power users) may also have felt more let down / upset and may change their future transactional behaviour with SNSW (to be tested).

  Consideration should be given to extra and personal communication steps during notification for both these 'involved' groups.

- **Customers who were not directly impacted and didn't receive a letter**

  Many customers called in who had not received a letter and or had been impacted by the breach. Some were surprisingly upset and demanding. Processes were created to handle and manage them and in future SNSW should always consider the whole customer base including these 'non impacted customers.

IIS findings:

No systematic capture of broader segmentation information (and no research beyond the CSAT survey with customers who contact CSAT) makes 'rolling up' customer insights for future design purposes very challenging.

Customer journeys are also a useful tool in collating customer insights for future use. They are not the same as process or touchpoint maps which are already available for this incident.

The Master Journey comprises all the sub-steps / tasks a customer could potentially go through from pre-notification, through notification, actions to reduce risk etc. Importantly this includes steps that are not managed by / touched by SNSW or its partners. Some customers may simply receive the letter, assess their risk and decide not to act and others may go through a majority of steps on the journey. Influencers and third parties can be significant. While each customer goes through a different subset of these tasks and has slightly different needs and experiences, however a master customer journey helps set a single framework / language for ensuring the organisation is focused on supporting a customer to end and goal vs delivery a set of pre-defined services.

Sitting under the master journey, segment journeys can be created along with segment personas. They are also useful for reviewing the larger subsets of customers who have similar needs and drivers and thus have similar journeys.

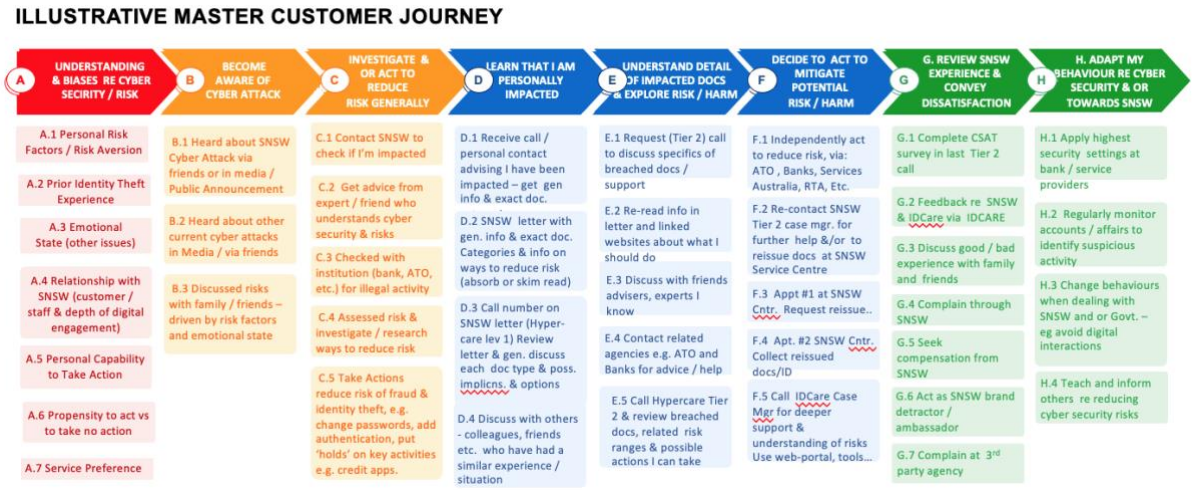
Typically, a journey diagram also included layers for customer need, trigger, emotional state and often best and worst experiences. This detail can be created for the main segments and customer / staff types to clarify differences in needs and interaction paths – and inform future incident response solution design – including variations in 'treatment paths' by segment.

IIS findings:

SNSW has a range of service flow and systems / touchpoint maps but, due to the nature of the incident, limited customer journey work has been done.

Refer further to detail below.

Using post incident Insights to create a master incident response journey is recommended. Journey maps can be created retrospectively through workshops with front line staff as part of the review process (ideally this would include customer research – in this case SNSW could use staff or family/friends as a proxy). We have added a draft / illustrative one below



In summary, this tool can be useful in cementing customer insights and refining user experience design. It can be beneficial in the following ways:

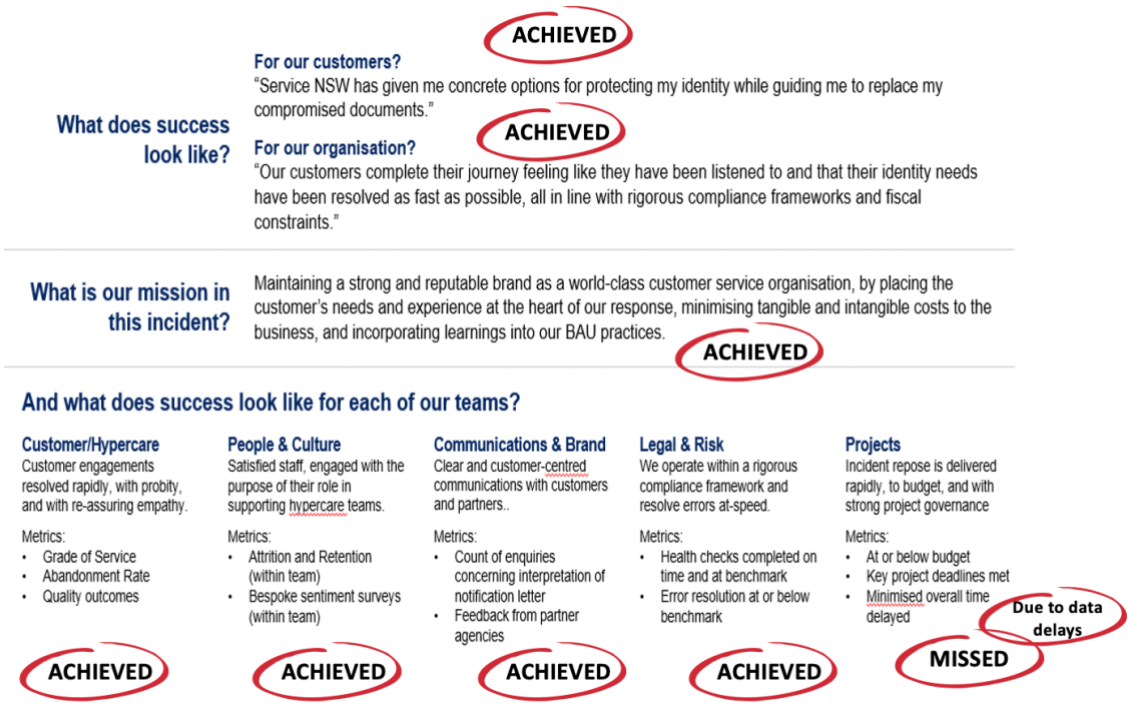
- Culturally, keeping the customer vs our processes front and centre
- Designing seamless end to end user experiences (considering variations / exceptions)
- Providing management with end to end understanding of the customers experiences (an outside-in view vs systems or transactional view of what's happening)
- Creating customer data frameworks, segmentation views and reporting generally
- Tool for training
- Assessing and understanding of capabilities and resource priorities. Service strategies and system or resource requirements and gaps can also be assessed against the customer journey.

8.5.3 Assessment of customer support and customer experience

8.5.3.1 Did the breach response team meet its success measures?

CITAF was tasked with delivering the breach response have defined customer-centric success measures for the breach response. These include the overall outcome driven aim of supporting customers and empowering them to take action to minimise future risk, and statements about providing choice, speed, exceptional service and maintaining brand trust:

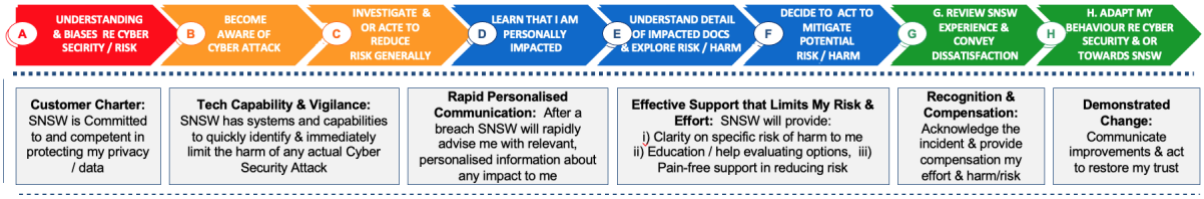
- **SNSW Aim:** To support customers and empower them to take action to minimise future risk
- **Customer Success Definition:** SNSW has given me concrete options for protecting my identity while guiding me to replace my compromised documents
- **SNSW Success Measures:** SNSW remains a trusted service provider for customers and partners with highly engaged staff
- **Mission for the Incident:** Maintaining a strong and reputable brand as a world-class customer service organisation…by placing the customer's needs and experience at the heart of our response … incorporating learnings into our BAU practices
- **Hypercare / Customer Team Success Measures:** Customer engagements resolved rapidly, with probity, transparency and re-assuring empathy
- **Code of Conduct – What is Expected of Me**: In the performance of your duties, you are required to ensure that our customers are always your highest priority and that the delivery of an exceptional customer experience is fundamental to all aspects of your work within SNSW, in compliance with this Code.



IIS findings:

The team is largely on track to meet its goals and success measures for the incident response. The project timeline has been marked as a miss because of the impact on response timing caused by the data issues (not a project management issue).

8.5.3.2 Did SNSW deliver best practice customer experience?



Whole customer journey: Overall, customer experience must be considered across the whole customer experience from awareness to resolution, is less clear (vs assessment of support).

Consider expectation and experience: Satisfaction is a function of Expectation and Experience and we can only guess at both given our narrow base of research.

All impacted customers vs responders: A majority of impacted customers did not engage/call in after receiving the letter and due to lack of research we do not understand how the letter landed and their overall journey (awareness, comprehension, resolution, action, satisfaction).

Support was positive for those who engaged: The experience, was largely positive for the minority who engaged. Hypercare received good CSAT feedback by any standard. Similarly, IDCARE results were extremely positive relative to almost all other breaches.

Nonetheless, a small yet significant subset of people who engaged were fundamentally unhappy with the breach occurring, the length of time taken with notification and the customer effort and steps required on their part. These ‘big picture’ satisfaction issues may not have been reflected in the CSAT surveys, given the way they were written and issued at the end of the final call, on the case managers request. Further research is required to understand the overall satisfaction of customers with the entire breach solution including the notification mechanism and timing, the service/support and the experience of taking actions at end agencies to reduce risk.

IIS findings:

SNSW delivered best practice customer experience for the majority of those it supported (otherwise unknown for non-responders).

8.6 Appendix F – Record of CITAF lessons learned

As part of the data breach response, a total of six workshop sessions were held with CITAF members and supporting functions to debrief and share their own views of lessons learned. The strawman used to assist the discussion was the data response timeline. The themes most commonly uncovered were leadership, organisational resilience, decision making, strategy and expectation, resources, communication and notification.

The tables below are a record of CITAF members' learnings.

Lessons learned – Leadership
What worked well: • Approach to the incident response was structured early on and the strategy was clearly defined. • Structure and discipline of PMO – diligent in taking action logs, decision making and coordinating with groups across SNSW, the cluster and third-party advisors**.**
What could have been better / improvements moving forward: • SNSW leadership needs to have a better understanding of cyber security and privacy risks – risk acceptance. • Improve security and privacy governance. • Senior leaders' approach and attention paid to staff members impacted by the incident (as either employees or customer) was well received but should have happened earlier and in a more comprehensive way. Staff expected to receive a more personal notification process versus the letter received by customers.

Lessons learned – Organisational readiness
What worked well: • Due to SNSW's agile approach, teams were ready for implementing changes as required. • As part of the continuous improvement culture, teams were tracking feedback received and adjusting the model as required (e.g., engagement model). The process was refined and adjusted listening to customer feedback.
What could have been better / improvements moving forward: • Security could have been more prepared to respond to these types of incidents and to have the right procedures in place. • Privacy and security risks should be recorded as 'business risk' within the central risk register. • Set realistic expectations and better manage stakeholder expectations (e.g. obtaining the Public Interest Determination for BDM and TfNSW to share information).

Lessons learned – Decision making

What worked well:

- Decisions were documented and tracked.
- Management had the relevant information needed to make the decisions.

What could have been better / improvements moving forward:

- Better appreciate the role of the Communications Team and include them in certain decision-making processes, especially in decisions that could affect reputation.
- Have the right resources available to prevent decision making from slowing down.
- In situations where decisions have to be made during stand-up calls, it would be better to minimise the size of the group of participants if possible.
- Plan out the remediation and compensation matters earlier on.

Lessons learned – Strategy and expectations

What worked well:

- PMO's role and its ability to provide information to the Senior Leadership Team but also challenge them.
- SNSW constantly keeping agency partners informed, worked collaboratively to find solutions and obtained their support.
- Have kept in mind throughout the whole process that it is all about the customers.

What could have been better / improvements moving forward:

- Better understand the 'problem' that DCS/SNSW was facing with unstructured data. The forensic analysis taught a big lesson for how agencies should approach this in the future, namely, to have a clearer idea and expectation when it comes to the end-product coming from the external party conducting the data analysis.
- Brief the forensic team conducting the data analysis on the types of transactions and procedures conducted by the agency.
- Consider having an agency person supporting the forensic work and complete quality assurance along the way.
- Set realistic deadlines for the data analysis process, taking into account the complexity of the incident and the fact that SNSW did not have a single view of customers.
- Set realistic expectations surrounding steps related to ensuring data sharing compliance with all key stakeholders (e.g., the PID process, police warrants, Services Australia's role).
- Bring in the Communication Teams earlier, get them involved in discussions with Hypercare and front liners.
- Better understand early in the piece who your stakeholders are and have a regular governance forum.
- Where possible, seek to reduce customer steps required to provide them with personalised/appropriate advice.
- Have the capability to assess the data of each customer impacted much quicker.
- Always expecting the 'perfect' result and experience for the customer had an impact on quick notification.

Lessons learned – Resources

What worked well:

- Team from a range of disciplines and variety of skill sets; had the right people at the table from early on (e.g., legal, GRP, internal stakeholders) to provide shared knowledge, support and expertise.
- Working regime and ongoing support received from partner agencies or impacted agencies; government coordination.
- Tools available to the CITAF team to coordinate efforts (e.g., Planner and Microsoft Teams).

What could have been better / improvements moving forward:

- Have better planning and ensure adequate staff are available at NSW service centres (some customers turned up and could not be attended to).
- The selection / hiring of resources such as for Hypercare teams were done very quickly (with less behavioural testing elements) which, according to some Hypercare team leaders has meant a compromise on quality in some cases. The team have dealt with this by management of performance.
- Ensure that all streams had the right resources and capability.
- Have dedicated resourcing; free people up from their BAU to focus on the incident.
- Provide training for service centre staff as to what they should expect when a customer comes in and how certain processes work to ensure that customers receive the help they need.
- Provide refresher training for Hypercare teams along the way**.**

Lessons learned – Communication and notifications

What worked well:

- Continued refinement of letters as feedback was received.
- Notification to customers via letters was the preferred choice as customers would not have appreciated finding out over the phone.
- Staged notifications worked well as we were not prepared for bulk**.**

What could have been better / improvements moving forward:

- Bring People & Culture as a stream member early.
- Notify staff earlier on.
- Provide support and ensure that leader-led conversations are held with impacted staff.
- For managers to brief staff in person and not rely on internal communications (e.g. video, emails) as some staff may not read all internal communications that come through.
- For managers to be briefed before having to notify staff.
- The Knowledge Area documents shared with Hypercare teams could have been better. There was an overload of information and it would have been better if amendments and updates were communicated better to the team members.
- Improve communication between Hypercare Tier 1 and Tier 2 teams so that Tier 2 is more prepared for when they engage with customers.
- If possible, for Tier 1 advise customers whether they are low risk or not.
- If possible, make the letters going out to customers shorter.

Lessons learned – Communication and notifications
• Letters could have been more specific, to provide further clarity for customers (e.g., telling customers if they were low risk). • To have better and more media training for executives to ensure better alignment on stance and messages before responding to the media. • To be more transparent with IDCARE – inform them of staggered notifications approach early on and provide them with clear information of what SNSW had told other agencies.

INFORMATION
INTEGRITY
SOLUTIONS

Information Integrity Solutions Pty Ltd
PO Box 978, Strawberry Hills NSW 2012, Australia
P: +61 2 8303 2438
F: +61 2 9319 5754
E: inquiries@iispartners.com
www.iispartners.com

ABN 78 107 611 898
ACN107 611 898