Independent review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data

Final Report

Prepared by: Murray Jack (FCA)

12 May 2017

Contents

Executive summary

The Ministry of Social Development (the Ministry, MSD) funds around 2,300 Non-Government Organisations (NGOs) which are primarily community-based social service providers. Recently, as part of shifting more to a results-based investment approach to social services, the Ministry has been working with NGOs to collect some individual client-level data (ICLD) from providers.

This data was to be stored in a temporary system with access restricted to authorised users nominated by the particular NGO each folder related to.

On 31 March 2017, the Ministry was made aware that one NGO was able to see the folder for information from another NGO. While no actual client data was exposed, this highlighted an issue with user access permissions of the temporary solution (the Shared Workspace, SWS) which was reviewed by the Ministry in subsequent days. On 4 April, all user access to the temporary solution other than administrative access was removed.

The Chief Executive of the Ministry has commissioned an independent investigation into the governance and decision-making that determined the interim solution for the capture of individual client level data.

About this review

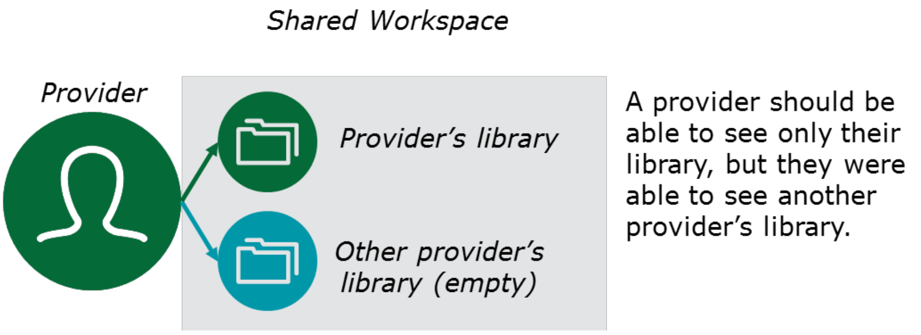
The objectives of the independent review are to address the questions raised about the temporary solution used to collect client level data from NGO providers, focusing on what happened, why it happened, what decisions were made and why, and the lessons learned.

The review also addresses the Ministry's governance and management of the client-level data work programme, with particular focus on implementation of the interim individual client-level data collection solution.

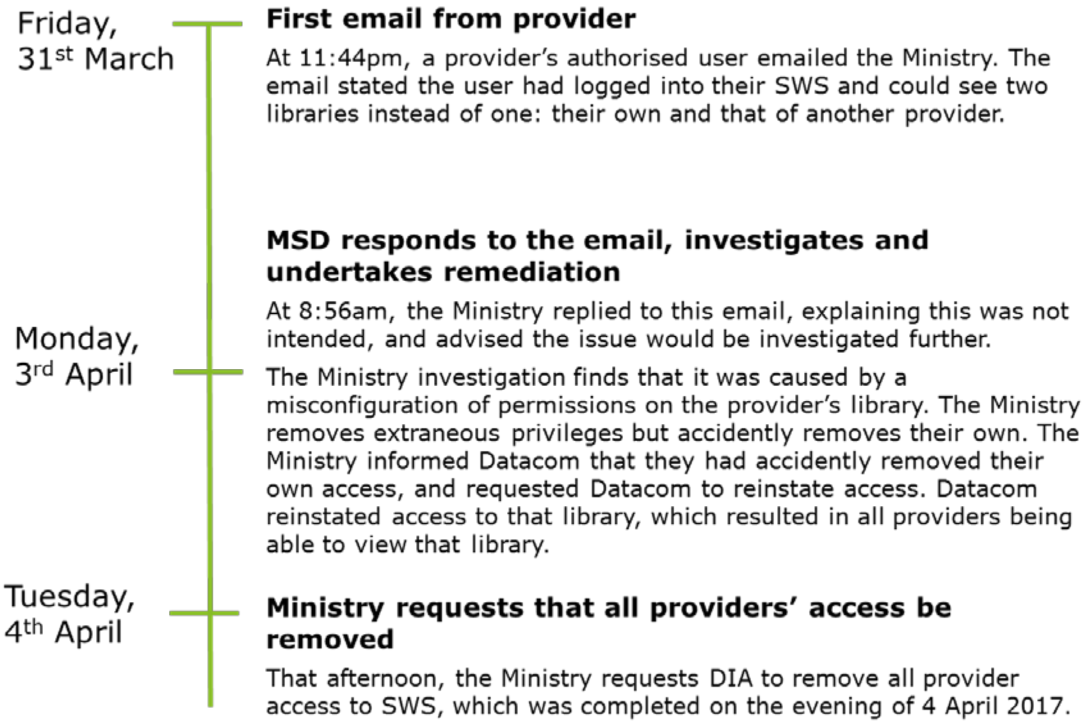
For the purpose of clarity, over time, the "temporary solution" started to be referred to as the "interim solution", even though it had not been selected as such. For the purposes of this report, the term "interim solution" referenced in the Terms of Reference scope and purpose for this independent review means the "temporary solution".

The review has been carried out by Murray Jack and Anu Nayar.

What happened?


Shared Workspace
Provider
Provider's library
Other provider's library (empty)
A provider should be able to see only their library, but they were able to see another provider's library.

No client data was in the library associated with the incident at the time.



Friday, 31st March

First email from provider

At 11:44pm, a provider's authorised user emailed the Ministry. The email stated the user had logged into their SWS and could see two libraries instead of one: their own and that of another provider.

Monday, 3rd April

MSD responds to the email, investigates and undertakes remediation

At 8:56am, the Ministry replied to this email, explaining this was not intended, and advised the issue would be investigated further.

The Ministry investigation finds that it was caused by a misconfiguration of permissions on the provider's library. The Ministry removes extraneous privileges but accidently removes their own. The Ministry informed Datacom that they had accidently removed their own access, and requested Datacom to reinstate access. Datacom reinstated access to that library, which resulted in all providers being able to view that library.

Tuesday, 4th April

Ministry requests that all providers' access be removed

That afternoon, the Ministry requests DIA to remove all provider access to SWS, which was completed on the evening of 4 April 2017.

Why did it happen?

The SWS which is provided by the Department of Internal Affairs (DIA) utilises Microsoft Sharepoint 2010, which by default, allows users to see everything within their workspace because it was designed to be a collaboration tool. Permissions for users need to be selectively removed from their default settings to prevent users from viewing or accessing materials they are not meant to. This was the Ministry's temporary solution.

The 31 March incident occurred as a result of an error in user permissions allocation. In the second instance, while seeking to fix the problem, the Ministry had accidentally deleted its own user permissions and requested Datacom to re-instate access to that library (the vendor managing SWS for the DIA). Datacom confirmed that they had restored access to the "data owner" of that library, i.e. MSD. When the access was re-instated, all privileges to that particular library were restored, which then enabled all providers to view that library.

Additionally, the susceptibility to the incident increased because the timelines for the ICLD project were challenging within the context of major organisational change, the project needed a temporary technology solution quickly since the interim solutions being considered would not be ready for use on time, insufficient rigour in the selection of the temporary solution (the SWS), and the Privacy Impact Assessment was done late in the project. These factors posed a level of risk not fully understood at the time.

Findings

Decision to suspend the solution

Upon being made aware of the issue, the Ministry responded appropriately. It identified the cause and suspended use of the solution. We support the decision to suspend the use of SWS to collect ICLD.

Decision to implement SWS

We believe there was insufficient rigour in the process that led to SWS being implemented as the temporary solution. Because it was an existing platform, already in use for a range of other initiatives, this decision was not treated in the way "go-live" decisions are generally made and governed.

Formality of the project

The project lacked some formal structures such as dedicated project resources, no formal "go-live readiness" process and limited attention to implementation of the temporary solution at a governance level.

Lessons to be learnt and recommendations

Learn from others

Some of the difficulties with using the temporary solution for the ICLD project could have been identified and mitigated better if the project team had gathered the knowledge and experience from other users of the SWS in a more structured manner. Projects should draw on experience from within the Ministry as well as from other agencies. For example, the multi-step, resource-intensive operating procedures required to configure libraries and user permissions could have been identified and procedures that had already been developed within the Ministry could have been leveraged for tailored use. Additionally, the need for "four-eyes" (in the form of peer review) over the configurations of current and changed settings by a second Systems Administrator could have been implemented.

Apply project disciplines consistently for solution deployment

Although the "go live" for the temporary solution was quite different from a "new solution" implementation (being an in-place solution already), formal project disciplines should have been applied. Specifically, this sort of project implementation can borrow from general systems-development lifecycle approaches for structured deployment phases, checking and testing, and criteria to confirm readiness for each phase. This would promote clarity on when it is considered to be in "setup phase" (where no providers are invited to use the system, and there is no client data on the system) in contrast to a "testing phase", "provider registration phase", "data upload phase" – all of which may have their respective checks and readiness approvals for deployment.

It is also important for projects to have the ability to pause and reflect when situations evolve, rather than simply react to time pressures. Formalised project disciplines can help to highlight the need for such "pauses" or avoid some of the time pressures in the first place. While it can seem difficult at the time, there can be valid reasons to delay a solution deployment rather than to put its success at significant risk.

Consider privacy early

Privacy needs to be considered early and be a consistent thread throughout projects like this. There needs to be sufficient links to relevant privacy considerations or Privacy Impact Assessments – covering, for example, any / all potential technology solution options - so a holistic view is maintained. Privacy Impact Assessments should be completed in time for review and action to confirm that risks are mitigated.

Validate information security risk mitigations

Similarly, information security activities and assessments should be carried out in time for project teams to action risks identified, and validate the appropriateness of mitigations.

Acknowledgments

We have had the full cooperation and assistance of the Ministry’s staff and management team throughout this review. We are also grateful for the time and assistance provided by people from other agencies to help us make our findings.

Introduction and background

The Ministry of Social Development (the Ministry, MSD) delivers, or purchases from other providers, a significant part of New Zealand's social services, including a range of benefits, entitlements, and services to young people and communities. Services and assistance are provided to more than 1 million New Zealanders and 110,000 families every year.

The Ministry funds around 2,300 Non-Government Organisations (NGOs), which are primarily community-based social service providers. Recently, as part of shifting to a more results-based investment approach to social services, the Ministry has been working with NGO providers (providers) to collect some individual client-level data (ICLD) from providers.

This data was to be stored in a temporary solution (the SWS) with access restricted to authorised users nominated by the particular provider each folder related to.

On 31 March 2017, the Ministry was made aware that one NGO was able to see the folder for information from another NGO. While no actual client data was exposed, this highlighted an issue with user access permissions of the temporary solution, which was reviewed in subsequent days by the Ministry. On 4 April 2017 all access for NGOs to the temporary solution was suspended. On 4 April, the temporary solution was halted altogether.

The Chief Executive of the Ministry of Social Development has commissioned an independent investigation into the governance and decision-making that determined the temporary solution for the capture of individual client-level data.

Purpose

The objectives of the independent review are to address the questions raised about the SWS that was being used to collect client-level data from providers, focusing on what happened, why it happened, what decisions were made and why, and the lessons learned.

The review also addresses the Ministry’s governance and management of the client-level data work programme, with particular focus on implementation of the interim individual client-level data collection solution.

The terms of reference for this review are attached in Appendix A.

Approach

The review broadly comprised the following activities:

- Examination of documents, project artefacts and operational outputs relevant to the scope of the review
- Interviews with relevant personnel, including with relevant third parties such as the Department of Internal Affairs (DIA)
- Reviewing inputs and outputs relevant to the solution and services associated with the data portal (the temporary solution)
- Discussions with key stakeholders including the Government Chief Information Officer (GCIO)
- Discussions and agreement among the independent reviewers
- The development of a draft and final report for the Chief Executive and relevant senior stakeholders.

Limitations and disclaimer

This report was prepared solely in accordance with the specific terms of reference between independent reviewers and the Ministry, and for no other purpose. Other than our responsibilities to the Ministry for this review, no member of the Review Team or their organisations undertakes responsibility arising in any way from reliance placed by a third party on this report. Any reliance placed is that party's sole responsibility. We accept or assume no duty, responsibility or liability to any other party in connection with the report or this engagement, including without limitation, liability for negligence in relation to the factual findings expressed or implied in this report.

The report is based upon information provided by the Ministry and interviewees. We have considered and relied upon this information. We have assumed that the information provided was reliable, complete and not misleading, and we have no reason to believe that any material facts have been withheld. The information provided has been considered through analysis, enquiry and review for the purposes of this report. However, we do not warrant in any way that these enquiries have identified or verified all of the matters which an audit, extensive examination or due diligence investigation might disclose. The procedures we have performed do not constitute an assurance engagement in accordance with New Zealand Standards for Assurance Engagements, nor do they represent any form of audit under New Zealand Standards on Auditing, and consequently, no assurance or audit opinion is provided.

Accordingly, we do not accept any responsibility or liability for any such information being inaccurate, incomplete, unreliable or not soundly based, or for any errors in the analysis, statements or opinions provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this report is based proving unjustified.

Organisational context

The Ministry delivers, or purchases from other providers, a significant part of New Zealand's social services, including a range of benefits, entitlements, and services to young people and communities. Services and assistance are provided to more than 1 million New Zealanders and 110,000 families every year.

The Ministry invests over $300 million in community-based social services each year. These services help support New Zealand's most vulnerable children, young people and adults to be safe, strong and independent. The Ministry funds around 2,300 Non-Government Organisations (NGOs) which are primarily community-based social service providers. In this report, we have used the term "providers" to refer to these organisations.

Significant organisational change

During the period considered in this report, the Ministry was preparing for, and then carrying out the transition of Child Youth and Family (CYF), Community Investment and the Children's Action Plan services to the Ministry for Vulnerable Children Oranga Tamariki (MVCOT). MVCOT was established as a new agency on 1 April 2017, and includes the functions of the Community Investment team from the Ministry that was driving the strategy and programme described below.

This transfer has been a significant change process for the Ministry and its staff. While there was dedicated project resource for the ICT component, the business side of the project relied on staff who also maintained their everyday responsibilities. Many of the business people involved in the strategy and programme were covering dual roles and working through the establishment phase of MVCOT. This posed some additional pressure and lack of clarity on the scope of responsibilities for some of these roles.

Community Investment Strategy

The Community Investment Strategy (the strategy) was launched by Hon Anne Tolley, Minister for Social Development, in June 2015. The strategy helps ensure the services delivered by providers are targeted at the right people and the right communities, based on evidence of what works.

One of the aims of the strategy is to strengthen the Social Investment approach already being applied by the Ministry and develop a more results-based approach to social services.

More information on the strategy is available at https://www.msd.govt.nz/about-msd-and-our-work/work-programmes/community-investment-strategy/.

Individual client level data work programme

As a part of the strategy, the Ministry communicated to providers that it intended to collect individual client-level data (ICLD) from providers to help the Ministry understand who is using the programmes and services they fund, and the impact those programmes and services are having. This data included:

- Client demographic information
- Dependants
- Details of the particular services the client receives.

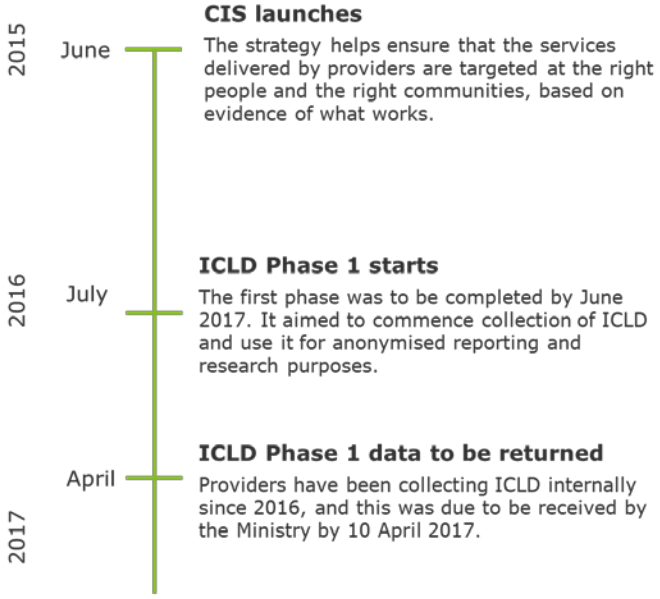
The purpose of this collection was to create an evidence-based funding model, and to improve the targeting of funding to the New Zealanders and providers that need it most. Sensitive information such as case notes was not to be collected.

Phase 1 of the ICLD Project

The first phase was to be completed in June 2017. It aimed to commence collection of ICLD and use it for anonymised reporting and research purposes.

From mid-2016, the Ministry identified an initial set of providers required to provide ICLD to the Ministry as part of their funding agreements. These initial providers were a subset of those associated with eight key programmes, and these providers covered 23% of the Ministry's provider funding in the strategy. In our interviews we were informed these initial providers delivered what the Ministry considered "non-sensitive" services and, in some cases, were already contractually required to provide client-level data to the Ministry.

Providers have been collecting ICLD internally since 2016, and this was due to be received by the Ministry by 10 April 2017 to meet contractual reporting requirements for Phase 1 of the strategy which was targeted to be completed by June 2017. Because of the incident, provision of this information to the Ministry has been put on hold.



CIS launches

The strategy helps ensure that the services delivered by providers are targeted at the right people and the right communities, based on evidence of what works.

ICLD Phase 1 starts

The first phase was to be completed by June 2017. It aimed to commence collection of ICLD and use it for anonymised reporting and research purposes.

ICLD Phase 1 data to be returned

Providers have been collecting ICLD internally since 2016, and this was due to be received by the Ministry by 10 April 2017.

Phase 2 of the ICLD Project

Decisions are still to be taken about the implementation of Phase 2.

Technology solutions

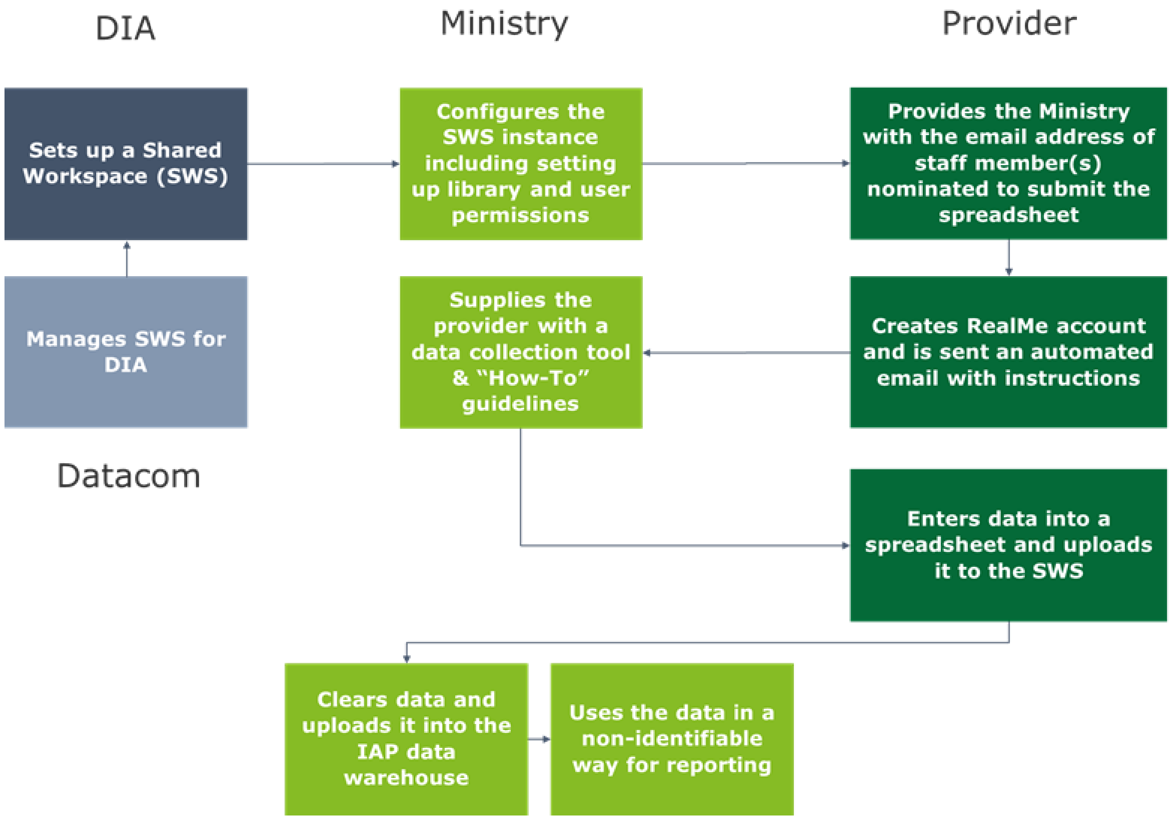
For Phase One, the Ministry considered a range of interim solutions that might be suitable. The timelines for the project were challenging within the organisational context of significant change. Because no interim solution option had been confirmed and implemented in time for the April 2017 ICLD collection to enable providers to meet their contractual reporting requirements, the SWS temporary solution was prepared instead.

Over time, the "temporary solution" started to be referred to as the "interim solution", even though it had not been selected as such. For the purposes of this report, the term "interim solution" referenced in the Terms of Reference scope and purpose for this Independent Review means the "temporary solution".

Overview of the solution

The temporary solution was for providers to use spreadsheets to record ICLD and then upload these for the Ministry to use. The Ministry purchased a Shared Workspace (SWS) from the Department of Internal Affairs (DIA) as the tool for providers to upload their spreadsheets, and for the Ministry to download them. The SWS is a platform utilising Microsoft's SharePoint 2010, offered as a standard "off the shelf" platform administered by the DIA.

The process is illustrated in the diagram below:


DIA
Ministry
Provider
Sets up a Shared Workspace (SWS)
Configures the SWS instance including setting up library and user permissions
Provides the Ministry with the email address of staff member(s) nominated to submit the spreadsheet
Manages SWS for DIA
Supplies the provider with a data collection tool & "How-To" guidelines
Creates RealMe account and is sent an automated email with instructions
Datacom
Enters data into a spreadsheet and uploads it to the SWS
Clears data and uploads it into the IAP data warehouse
Uses the data in a non-identifiable way for reporting

Authorised users of providers would log in using the RealMe platform (the all-of-government authentication service) and upload their spreadsheets. The Ministry would access these spreadsheets and process the information into the Ministry's data-store (IAP – Information Analysis Platform).

Description of SWS

Information about SWS is available at https://www.ict.govt.nz/services/show/SWS. An excerpt has been provided below:

"*SWS is a secure, online collaboration tool for government agencies to share information with each other and with their third-party project partners. It helps achieve better outcomes by allowing specialist groups and networks to share expertise, experience and good practice.*

SWS is primarily designed for project management, and uses SharePoint 2010 software with some customised member management functionality added.

SWS uses RealMe as its authentication service. All SWS users must have a RealMe login to access their workspace."

The Department of Internal Affairs (DIA) provides and manages the service for all eligible government agencies. Datacom is the vendor managing SWS for the DIA.

The DIA has certified SWS as a solution to be used for information classified up to "In-Confidence".

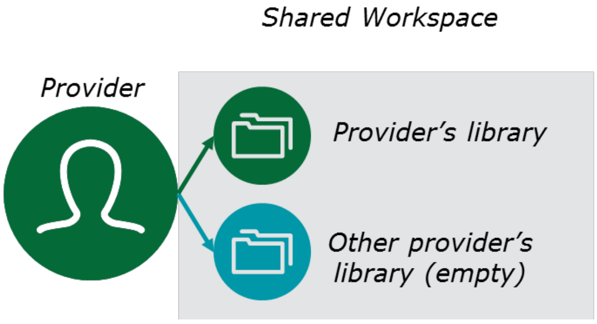
Other users of SWS

SWS was a known solution to the Ministry. It was already in use for other Ministry initiatives, including for similar purposes – for example, as a way for external parties to share information with the Ministry without those parties having access to the Ministry's internal systems.

There are approximately 250 separate SWSs operating in New Zealand with 6,000 active users. Sixty percent of users are government. The website link above includes a list of agencies using the service.

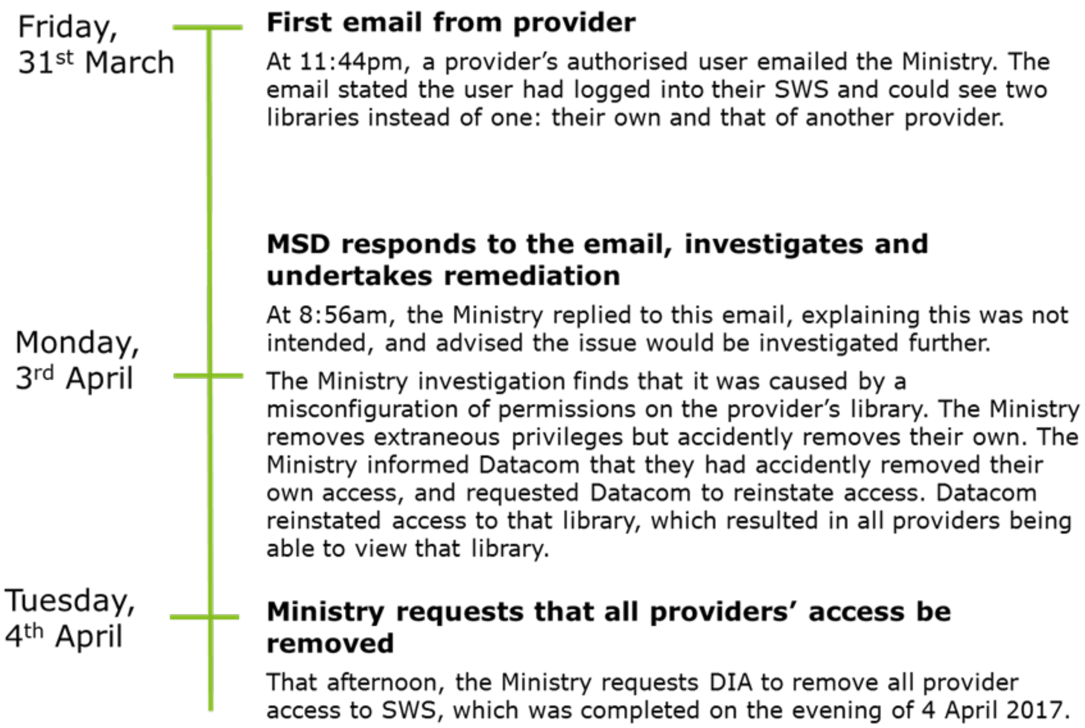
The incident in late March / early April 2017

What happened?



A provider should be able to see only their library, but they were able to see another provider's library.

No client data was in the library (folder) associated with this incident at the time.



Friday, 31st March

First email from provider

At 11:44pm, a provider's authorised user emailed the Ministry. The email stated the user had logged into their SWS and could see two libraries instead of one: their own and that of another provider.

Monday, 3rd April

MSD responds to the email, investigates and undertakes remediation

At 8:56am, the Ministry replied to this email, explaining this was not intended, and advised the issue would be investigated further.

The Ministry investigation finds that it was caused by a misconfiguration of permissions on the provider's library. The Ministry removes extraneous privileges but accidently removes their own. The Ministry informed Datacom that they had accidently removed their own access, and requested Datacom to reinstate access. Datacom reinstated access to that library, which resulted in all providers being able to view that library.

Tuesday, 4th April

Ministry requests that all providers' access be removed

That afternoon, the Ministry requests DIA to remove all provider access to SWS, which was completed on the evening of 4 April 2017.

A more detailed timeline of the event has been included in Appendix B.

Why did it happen?

By default, SWS allows all users to see everything within their workspace because it was designed to be a collaboration tool. Permissions for users need to be selectively removed from their default settings to prevent them viewing or accessing materials they are not meant to.

The 31 March incident occurred as a result of an error in user permissions allocation. In the second instance, while seeking to fix the problem, the Ministry had accidentally deleted its own user permissions and requested Datacom to re-instate access to that library (the vendor managing SWS for the DIA). Datacom confirmed that they had restored access to the “data owner” of that library, i.e. MSD. When the access was re-instated, all privileges to that particular library were restored, which then enabled all providers to view that library.

Additionally, the susceptibility to the incident increased because the timelines for the ICLD project were challenging within the context of major organisational change, the project needed a temporary technology solution quickly since the interim solutions being considered would not be ready for use on time, insufficient rigour in the selection of the temporary solution (the SWS), and the Privacy Impact Assessment was done late in the project. These factors posed a level of risk not fully understood at the time.

Discussion

The incident occurred 10 days before the first deadline for submission of ICLD by the initial set of providers. No client data was disclosed. This was confirmed by a post-incident review of SWS, commissioned by DIA, undertaken by an independent security company.

The user permission allocation in SWS is a time-intensive process for the way the Ministry intended to use it. The Ministry had to invite each of the 384 providers to the SWS and individual libraries were required to be set up for each. Phase One covered 153 providers (although only 136 had been set up). When the Ministry set up the permissions for each user, the Ministry would have to deselect a setting to prevent the user from inheriting the default permissions that would allow the user access to everything.

The intended purpose of the SWS was collaboration and therefore the default setting is to “allow all” and restrict by exception rather “deny all” and enable by exception. Because of this the process for managing user permissions requires strong controls in order to minimise human error that could cause one user to be able to see files from another user.

It was also noted there was an incident in January 2017, when one provider was setting up their folders they notified MSD that they were able to see another provider’s spreadsheet on a general shared page within the SWS. This was immediately moved to the correct location and access information confirmed that the data was only accessed by the provider who uploaded it.

Decisions made leading up to the incident

Programme summary

Programme establishment

The Minister's expectations of the Community Investment Strategy, including the collection of ICLD, were set out to the Ministry in 2015. The programme received funding of $1 million in early 2016 to:

- Develop a business case by June 2016 for an ICT solution for ICLD collection
- Implement an interim ICT solution by June 2016 for ICLD collection for Phase 1.

This recognised, at programme establishment, that further time and investment would be required for a long-term solution to collect ICLD.

Programme management and governance

Delivery of the strategy overall was initially governed by the Community Investment Implementation Programme Board, which was set up in January 2016.

The delivery of the Community Investment Strategy was initially delivered through "business as usual" (BAU) resourcing – i.e. staff who also carried out their normal everyday duties. Support from ICT was separately funded and resourced with dedicated project staff. The ICT component had a separate board for governance co-chaired by the Deputy Chief Executives (DCEs) of Community Investment and Organisational Solutions.

During the programme of work, there were various changes in key roles, project structure and governance groups. Roles and responsibilities in relation to governance across the various streams of work were sometimes unclear, and governance was not effectively applied in relation to the selection of the temporary solution, or in relation to security and privacy matters.

In November 2016, Community Investment created a formal programme of work in which ICLD was established as its own project stream.

Interim solution options

A range of interim solutions was explored. Initially, the Ministry aimed to develop its own cloud-based solution – a copy of an existing Ministry of Health system. Several other options were raised, including extending Ministry-owned systems, using providers' systems, and purchasing the Ministry of Health software.

Decisions and why they were made

How was SWS selected?

Because no interim solution option had been confirmed and implemented in time for the April 10 2017 ICLD collection deadline, a temporary solution (the SWS) was prepared instead.

There had been ongoing discussion within the programme about using spreadsheets as a fall-back option. In terms of how the spreadsheets were to be shared between the providers and the Ministry, we were informed through interviews that the idea of emailing the spreadsheets was discarded because it was considered insecure.

We were informed by the Ministry in interviews, the project team assumed SWS could be a feasible option for ICLD because it was being used successfully for a range of other purposes, both across the Ministry and in other agencies, including for what the project team believed were similar needs (i.e. sharing information between a range of parties). We have not seen any evidence of specific options analysis that led to the selection of SWS as being the preferred option to share the spreadsheets between the providers and the Ministry. We understand documentation of the solution requirements was limited to the data fields required – i.e. the "columns" in the spreadsheet and their definition.

A memo dated 7 September 2016 from the Programme Manager of the ICT Stream recommended the purchase of the SWS, subject to completion of a Security Risk Assessment and its endorsement by the CISO. This recommendation was signed off by the Associate DCE of Community Investment on 16 September 2016. The Security Risk Assessment was signed off on 28 November 2016. The first set of providers were sent communications commencing in July 2016 including the instructions for how to use SWS. On 6 December 2016, the Ministry's SWS Systems Administrators began compiling a list of providers for whom they needed to set up libraries on the system. From the last week of December 2016 to January 2017 user groups with permissions were set up, with further work on this expected on a rolling basis through to March 2016.

The nature of SWS (as an existing, operational solution) means implementation is quite different from a "new" system. From January 2017, the temporary ICLD solution could be considered "live" in that it would have been possible for providers with folders and permissions who had already been set up to be invited to use the workspace.

How was information security and privacy considered?

In late 2016, and prior to users from the providers being set up in SWS, the Ministry completed a Security Risk Assessment and a questionnaire to determine the initial security risk level. At the time, the Ministry consulted its privacy specialists to validate the decision for the "In-Confidence" classification to be used, as the information sought would not relate to sensitive services.

The Ministry revised the questionnaire early this year because it wanted to consider the ongoing suitability of the solution from a security and privacy perspective, until a longer term solution could be stood up. The Ministry was in the process of updating its Security Risk Assessment, including validating the key controls identified, when the incident occurred and the temporary solution shut down.

The project had considered privacy for what it thought at the time would be the "interim solution" (i.e. not the temporary solution using SWS), and commenced developing an internal Privacy Impact Assessment in January 2017. The scope of privacy analysis was expanded to cover the wider ICLD process including the SWS, and in late March 2017 another Privacy Impact Assessment was drafted by an independent external party. The draft was completed at the end of March 2017 and was in the process of internal review when the incident occurred.

Findings and lessons to be learnt

Findings

Decision to suspend the solution

Upon being made aware of the issue, the Ministry responded appropriately. It identified the cause and suspended use of the solution. We support the decision to suspend the use of SWS to collect ICLD. This solution is prone to human error in setting up and managing permissions on an ongoing basis for the volume of users requiring access for ICLD collection and requires strengthened permissions management processes to be implemented by the Ministry.

Decision to implement SWS

We believe there was insufficient rigour in the process that led to SWS being implemented as the temporary solution. Because it was an existing platform, already in use for a range of other initiatives, this decision was not treated in the way "go-live" decisions are generally made and governed. Specific short-comings were:

- Insufficient documentation and analysis of requirements, including security requirements
- No robust process for identifying and evaluating options for the temporary / interim solution
- Insufficient consideration of the security classification of data based on the likely impact if a data breach were to occur
- The Privacy Impact Assessment was not comprehensive and was carried out too late to impact option selection.

Formality of the project

The project lacked some formal structures – for example:

- Dedicated project resource was only provided for the ICT component, while the "business side" of the project relied on staff who also had to continue with their other everyday responsibilities. The "business side" included the MSD Systems Administrators for the SWS solution for ICLD
- No formal "go-live readiness" process, including checklists and criteria. The go-live needed to be thought through with specific steps to mitigate risks in relation to setup activities, and the configuration of libraries and user permissions since all of these activities would be occurring on a live system – since the SWS was a live platform already in use by multiple parties
- Limited attention to implementation of the temporary solution at a governance level. There was discussion and consideration of security and privacy matters within the relevant governance forums in relation to the "original" interim solution options. Through our interviews, we were informed that because the SWS was considered to be a temporary solution to collect data from providers on non-sensitive services, and would be using the SWS – a solution known to be used by the Ministry and other agencies for a similar purpose, there was nothing to warrant further attention at the governance levels.

Lessons to be learnt and recommendations

Learn from others

Some of the difficulties with using SWS for this project could have been identified and mitigated better if the project team had gathered the knowledge and experience from other users of SWS in a more structured manner. Projects should draw on experience from within the Ministry as well as from other agencies. For example, the multi-step, resource-intensive operating procedures required to configure libraries and user permissions could have been identified and procedures that had already been developed within the Ministry could have been leveraged for tailored use. Additionally, the need for "four-eyes" (in the form of peer review) over the configurations of current and changed settings by a second Systems Administrator could have been implemented.

Apply project disciplines consistently for solution deployment

Although the "go live" for the temporary solution was quite different from a "new solution" implementation (being an in-place solution already), formal project disciplines should have been applied. Specifically, this sort of project implementation can borrow from general systems-development-lifecycle approaches for structured deployment phases, checking and testing, and criteria to confirm readiness for each phase. This would promote clarity on when the solution is considered to be in "setup phase" (where no providers are invited to use the system, and there is no client data on the system) in contrast to a "testing phase", "provider registration phase" and "data upload phase" – all of which may have their respective checks and readiness approvals for deployment.

It is also important projects have the ability to pause and step back when situations evolve, rather than simply react to time pressures. Formalised project disciplines can help highlight the need for such "pauses" or avoid some of the time pressures in the first place. While we know it can seem difficult at the time, it is always better to delay a project for good reason than to put its success at significant risk.

Consider privacy early

Privacy needs to be considered early and be a consistent thread throughout projects like this. There needs to be sufficient links to relevant privacy considerations or Privacy Impact Assessments, for example covering alternate options, so a holistic view is maintained. Privacy Impact Assessments should be completed in time for review and action to confirm that risks are mitigated.

Validate information security risk mitigations

Similarly, information security activities and assessments should be carried out in time for project teams to action risks identified, and validate that mitigations are in place and working.

Appendix A: Terms of Reference

Independent Review of the Ministry of Social Development's decisions relating to the IT system used to capture individual client level data

10 April 2017

The Chief Executive of the Ministry of Social Development (the Chief Executive) has commissioned an independent investigation into the governance and decision making that determined the interim solution for the capture of individual client level data.

The review will be led by Murray Jack, (the independent reviewer) together with Anu Nayar, Deloitte NZ National Leader of Cyber, Privacy and Resilience and Adrian van Hest, PwC, National Cyber Practice Lead.

Objectives of the review

The objectives of the independent review are to address the questions raised about the portal that was being used to collect client level data from providers, focusing on what happened, why it happened, what decisions were made and why, and the lessons learned.

The review will also assess the Ministry's governance and management of the client level data work programme with particular focus on the implementation of the interim individual client level data collection solution.

Matters in scope

The review will investigate the circumstances and causes of the issue where a provider was able to view another provider's folder which had the potential to compromise the client's privacy, focusing on:

- The decision to use the portal, including:
    - analysis of the available technical options
    - work done to ensure appropriate information security was analysed
- The governance and management of the project
- Establishing how the issue occurred and the circumstances that allowed this to happen
- Review the governance around the response to the event itself. Including governance, roles and responsibilities, escalation and communication channels.

The review will identify any lessons learned and make recommendations to the Chief Executive and if appropriate, the GCIO, about findings, including any changes and improvements needed to the matters in scope.

Matters out of scope

Review of the shared workspace capability as a fully secure service offering for sensitive client data.

Deliverables, timeframes and reporting

The objective is that the first deliverable will be a draft report to the Chief Executive and GCIO. The review will be completed by 30 April 2017 in the form of a final report to the Chief Executive.

Resources required

- Provision of office space at MSD premises
- Access to documentation and material related to matters in scope of the review
- Access to staff for interviews.

Governance

The review will be supported by the MSD General Manager, Risk and Assurance, with direct access for reviewers to the Chief Executive during the review.

Signed

Brendan Boyle

Chief Executive

Ministry of Social Development

10 April 2017

Appendix B: Timeline of the incident

Friday, 31 March 2017

A provider’s authorised user (“Provider A”) emails a person within the Community Investment team (“Person D”) at the Ministry at 11:44pm, stating that they can see another provider’s (“Provider B”) library and can seemingly access the “All Documents” page of that provider, as well as their own.

Monday, 3 April 2017

Person D comes into work on Monday and sees the email, and at 8.42am they ask the Ministry’s System Administrator for this SWS to investigate.

The Ministry receives another email from a different provider’s authorised user (“Provider C”) to different person within the Ministry (“Person E”) at 11.58am, which also states they can see the folder of Provider B and a calendar entry of another provider.

The Ministry’s System Administrator reviews the permissions on the SWS and observed that all users of this SWS had permission to the library for Provider B. The System Administrator then removes all access to Provider B’s library except for Provider’s B staff but this also causes the Ministry’s access to the Provider B’s library to be removed. The System Administrator also verified that permissions to other groups were set as intended.

At 2:37pm the System Administrator from the Ministry informed Datacom that they had accidently removed their own access, and requested Datacom to reinstate access. Datacom confirms at 3:54pm that they have reinstated access to that library. This resulted in all providers being able to view that library.

Tuesday, 4 April 2017

Internally within the Ministry, at 8:04am the email from the Provider C is forwarded by Person E onto Person D. At 8:52am Person D again forwards this to the Ministry’s System Administrator for this SWS, who checked and found that all users were able to see the folder for Provider B but that there was no data content in that folder.

The Ministry’s System Administrator then deletes all permissions to Provider B’s library except for Provider B and the Ministry.

The Ministry begins to look into how they onboard users to the system and start to initiate a triple check process. The Ministry gets a second person to check the changes that the Ministry’s System Administrator made. The Ministry also has a third person to check the permissions on all other libraries.

The Ministry makes a decision to remove access to the SWS and contacts Department of Internal Affairs (“DIA”) to restrict access to the SWS at 4.55pm. At 9.04pm the Ministry receives confirmation from the DIA that they have removed all people’s access to information in SWS except for those in the Admin group.

Thursday, 6 April 2017

DIA engages with an independent security company to investigate the incident.