



Ministry of Social Development

Independent Review of Information Systems Security

Phase 1

**Circumstances and Causes of, and Response to, the
“Kiosk” Security Breach**

FINAL REPORT

1 November 2012

Contents

Executive summary	3
Introduction	8
Development of the “kiosks”	12
Operation of the “kiosks”	20
Events and the Ministry’s responses	24
Conclusions	36
Appendix A: Terms of Reference	39
Appendix B: Development of “kiosks” timeline	41
Appendix C: Timeline of the events	42
Appendix D: Response timeline – Technical focus	43
Appendix E: Response timeline – Management focus	44
Appendix F: Glossary	45

Executive summary

Confidence that information is secure is vital to the trust-based relationships needed to provide effective services

The Ministry of Social Development (“Ministry”) provides services to those in need, helping them become successful in their lives. To have a real impact in people’s lives requires that the Ministry establishes and maintains a high level of trust with the people it deals with. The Ministry is New Zealand’s largest government department providing services to more than 1.1 million clients, receives in excess of 230,000 calls a week, and approximately 40,000 online applications a month.

This has become even more important with the changes in technology experienced globally over the last decade or so, and the associated changes in customer expectations and service delivery opportunities. These have made many public and private sector organisations re-look at how they are delivering to their stakeholders and seek to become more customer focussed, making it easier for people to access the services they need.

But along with new opportunities have come new challenges – in particular how to ensure that richer and more readily available information can be protected so that individuals can have confidence that it is used appropriately and is secure from unauthorised access and use.

Government services are complex and involve many thousands of daily interactions, and information is vital to their effectiveness. No matter what levels of physical and system protection are in place breaches of security and the associated privacy implications as a result of system failures and human error may occur. Nonetheless, individuals should expect that all reasonable efforts are made to provide physical and technical environments that ensure personal information is secure from unauthorised access and use.

Restoring confidence is crucial for the Ministry to resume its important services to job seekers

Like many organisations in the public and private sectors, the Ministry has sought to improve how services are delivered, and one of these initiatives was the implementation of self-service “kiosks” that was completed in October 2011. In the Ministry environment the “kiosks” are essentially ordinary computers that are readily accessible to the Ministry’s clients in its Work and Income service centres, and provide valuable information and tools – with a particular focus on supporting job seekers.

But public confidence – and more importantly the confidence of the Ministry’s clients – has been eroded. It has been eroded by the disclosure on 14 October 2012 that the Ministry’s information security had been breached. The breach related to information that should have been secure, but with determined effort, was able to be accessed from “kiosks” on the Ministry’s own premises

That breach has naturally led to questions that need to be answered, and it has also led the Ministry to cease provision of “kiosk” services. Those services cannot be resumed until there is confidence that the weaknesses that led to the breach have been fixed, and confidence that the Ministry has taken the appropriate steps that may be required to ensure that any broader security issues have been mitigated effectively.

The Ministry commissioned an independent review of its information systems security to understand what occurred and to help restore the level of confidence and trust that is needed.

Objectives of the review

The objectives of the independent review are to address the questions raised about the security of the Work and Income self-service “kiosks” focusing on what happened, why it happened, the lessons learned, and the actions the Ministry needs to take to address any security issues raised.

The review is in two phases. This report presents the findings from the first phase, investigating the circumstances and causes of, and the response to, the security breach.

The second phase will assess the appropriateness and effectiveness of the Ministry’s wider information systems security, particularly publicly accessible systems, and consider broad aspects such as culture, governance, policies and capability.

How did this happen?

We identified three primary causes of the “kiosk” security weaknesses that enabled the security breach to happen.

- **Security was not adequately considered in the “kiosk” design and implementation.** Computers providing similar (though more limited) functionality to clients have been in place since 1998. While the risks of having these computers connected to the Ministry’s corporate network were known at the inception of the “kiosk” concept in 2009, the Ministry lost sight of that risk and the need for separation of the “kiosks” from the network as the “kiosk” concept evolved and was rolled out.
- **The exposures identified through independent security testing were not appropriately addressed and followed up.** In April 2011, almost six months before the “kiosk” roll out was completed, penetration testing by Dimension Data clearly highlighted security issues that needed to be addressed – including the lack of network separation. These findings were not appropriately followed up, addressed or escalated for management visibility and action, which meant that the risks remained substantially unaddressed.
- **The risk management processes did not effectively escalate security exposures to management, nor ensure appropriate mitigating actions were taken.** The security risks highlighted by the Dimension Data report were recognised, but their significance was underestimated, by the project team responsible for delivering the “kiosk” computers and the Ministry’s IT security team. That meant that the risk was not escalated and dealt with

appropriately. It is evident that the risk management processes in use for the “kiosk” project did not represent best practice.

Findings of the review

Phase 1 of the review has been tasked with answering specific questions. These findings are discussed in detail in the body of the report and summarised below.

The establishment and operation of the self-service “kiosks” in Work and Income service centres.

Insufficient work was done to ensure appropriate information security was put in place at the time that the “kiosk” infrastructure and services were designed and built. Sound independent testing was done to assess the security of the “kiosk” and what risks it posed to the Ministry and its data. This identified specifically the weaknesses that allowed the breach to occur. **The Ministry’s consideration of security requirements during the design and implementation of the “kiosks” and the response to security issues identified during the testing was inadequate.**

Information provided to the Ministry by third parties raising security concerns about the “kiosks” and the appropriateness and effectiveness of the Ministry’s response to these concerns.

On Monday 10 October 2011, shortly after complete implementation of the “kiosks”, the Ministry was notified of concerns by Ms Kay Brereton who had been invited to a session to become familiar with the “kiosks. While the information provided was unclear – and the Ministry sought further details – **the Ministry’s response to the notification did not follow a good practice incident management process, with associated tracking and formal close out requirements.** This meant that the Ministry did not identify the nature of weaknesses in “kiosk” security and therefore did not remediate them.

More recently, on Monday 8 October 2012 the Ministry was contacted by telephone by Mr Ira Bailey who had identified a security issue. Again, the information provided was not specific enough to fully identify the issue – and it did not suggest that the “kiosks” were involved. **In this instance, the issue was escalated and the Ministry responded by, seeking more information to identify the nature of the issue and commencing security testing to identify weaknesses. The Ministry then took a coordinated approach that included appropriate notification to external stakeholders.**

The appropriateness and effectiveness of the Ministry’s response to the security breach.

On Sunday 14 October 2012, shortly after the telephone notification on 8 October, a Mr Keith Ng revealed that there was a security breach relating to the “kiosks” at the Ministry, to the media and also to the Office of the Privacy Commissioner. That evening, the Ministry was contacted by the media (becoming aware of the breach) and immediately convened an internal meeting. The Ministry established a response team, stopped the “kiosk” service due to the risk of exposure of clients’ private information, began the process of determining the potential harm that the breach may have

caused its clients, and initiated implementation of measures to respond to both the vulnerability and the security breach. The Ministry has eliminated the potential for unauthorised access to data via “kiosks” and commissioned this independent review.

The Ministry’s response to the security breach it became aware of on 14 October has been appropriate and effective.

Conclusions

It is clear from the analysis and the findings that a number of people within the Ministry’s IT function were aware of the “kiosk” security weaknesses and the risk posed in relation to the access to information on the Ministry’s corporate network.

Appropriate follow-up action was not taken to remediate the identified weaknesses, either within the project team or the IT Security Team.

Failure to apply best practice risk management processes in the governance and management of the “kiosk” project resulted in the security risks that were identified not being escalated to appropriate levels that , had they done so, may have resulted in action being taken to remediate them.

Having been made aware of the security breach we find that the Ministry’s response has been appropriate.

- The “kiosks” were disabled and access to network shares containing Ministry and personal information were restricted or shut down.
- Comprehensive technical analysis to identify any potential downloading of information from any “kiosks” commenced and is on-going. As at the date of this report there are no further identified breaches.
- On identification that Principle 5 of the Privacy Act had been breached an extensive investigation of potential harm that may have been caused to individuals was commenced and as of the date of this report is on-going.

Next steps

The Ministry should continue its evaluation of the options for restoring a secure “kiosk” service and progress work on the selected option. There are two broad options:

- Physically separate the “kiosk” network from the Ministry’s network.
- Logically separate the “kiosks” from the Ministry’s network using firewalls or strong access control lists.

These options require careful analysis, and once the preferred option is selected and implemented should be subject to thorough testing prior to “kiosk” service restoration.

It is recommended that the full “kiosk” service is not resumed until network separation is implemented and its effectiveness subjected to thorough testing.

Phase 2 of the review will commence immediately upon completion of Phase 1. As set out in the Terms of Reference, Phase 2 will review the wider information systems security management including policies, governance, capability, and culture elements.

This second phase will contain recommendations as necessary for improvement of the Ministry’s security environment.

Introduction

Background

Self-service “kiosks” have been fully deployed at the Ministry of Social Development’s (the Ministry’s) Work and Income Service Centres in their current form since October 2011. They are used by Work and Income clients primarily to search for job opportunities and provide a capability to prepare curricula vitae (CVs) to assist with job applications. The implementation of “kiosks” was not a complete step change; “Worktrack PCs” had been in place since 1998 providing some similar, although more limited functionality to clients.

On 14 October 2012, Mr Ng alerted the media and the Office of the Privacy Commissioner to a security issue with the “kiosks”. During the previous week, another member of the public, Mr Bailey, made the Ministry aware of a security vulnerability. The Ministry was attempting to determine details of this at the time that Mr Ng’s information became known.

In response to the information provided by Mr Ng, the Ministry has ceased providing “kiosk” services, engaged with the Office of the Privacy Commissioner and other stakeholders, issued a Terms of Reference for an Independent Review of the Ministry’s Information Systems Security on October 17, and established an independent Steering Group to govern the review.

Terms of Reference

The Terms of Reference for the Independent Review is included in detail in Appendix A. It includes two phases.

- The first phase of the review will investigate the circumstances and causes of the “kiosk” security breach which compromised privacy of the Ministry’s data.
- The second part of the review will assess the appropriateness and effectiveness of the Ministry’s wider information systems security, particularly publicly accessible systems, and including the policies, governance, capability and culture.

Purpose of this document

The objectives of the Independent Review are to address the questions raised about the security of the Work and Income self-service “kiosks” focusing on what happened, why it happened, the lessons learned, and the actions the Ministry needs to take to address any security issues raised.

The purpose of this document is to present the findings from the first phase of the review. Specifically, this includes:

- The establishment and operation of the self-service “kiosks” in Work and Income service centres, including:
 - The work done to ensure appropriate information security was put in place at the time that the “kiosk” infrastructure and services were designed and built;
 - The independent testing done to ensure the security was operating as designed; and
 - The Ministry’s response to any security issues identified during the testing.
- Information provided to the Ministry by third parties raising security concerns about the “kiosks” and the appropriateness and effectiveness of the Ministry’s response to these concerns.
- The appropriateness and effectiveness of the Ministry’s response to the security breach.

Approach

The Review Team took the following approach to conducting Phase 1 of the review:

Understanding the ‘as built’ environment and design of the “kiosks”

Gaining clarity on technical specifications and functionality of the “kiosks” and their interactions with the Ministry’s corporate network through:

- Interviews
- Reviews of design documentation
- Reviews of technical documentation
- Reviews of extracts of relevant IT configurations
- Physical inspection

Understanding how the ‘as built’ “kiosk” design was arrived at, including testing performed and the Ministry’s response

Establishing, as much as possible, the details of the project work to implement the “kiosks” through:

- Interviews
- Reviews of project documentation, including design documentation and meeting minutes
- Reviews of email communications

Reviewing the findings of security testing performed and establishing how the Ministry responded to these through:

- Interviews
- Review of terms of reference for testing performed and findings reported
- Reviews of project documentation, including meeting minutes
- Reviews of email communications

Understanding details of the events, focused on the concerns raised by third parties and the security breach

Establishing what specifically happened in the events through:

- Interviews with participants in the events and others
- Reviews of email communications
- Reviews of records of telephone communications

Corroborating from a technical perspective, to the extent possible, that description of the events are accurate through:

- Reviews of log files
- Forensic analyses of system components involved

Understanding the response of the Ministry to concerns raised by third parties and the security breach

Establishing what the Ministry has done in response to each event through:

- Interviews
- Reviews of email communications
- Reviews of the technical response actions

Assessing what needs to be done to restore the service and to review the broader aspects of the Ministry's information systems security for Phase 2

Considering the weaknesses in information security relating to "kiosks" and assessing how these should be addressed through:

- Review of the 'as built' design
- Review of third party recommendations
- Reviews of the technical response actions
- Informing the approach for the broader review to be done in Phase 2 based on initial observations.

Disclaimer and limitations

This report is prepared in accordance with the specific terms of reference between Deloitte and the Ministry of Social Development ("Ministry"), and for no other purpose. Other than our responsibilities to the Ministry and the Steering Group for this review, neither Deloitte nor any member partner or employee of Deloitte accepts or assumes any duty of care or liability to any other party in connection with this report or engagement.

The report is based upon information provided by the Ministry and interviewees. Deloitte has reviewed, and relied upon this information. Deloitte has assumed that the information provided was reliable, complete and not misleading and has no reason to believe that any material facts have been withheld.

Accordingly, neither Deloitte nor its partners, directors, employees or agents, 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 views provided in this report resulting directly or indirectly from any such circumstances or from any assumptions upon which this report is based proving unjustified.

This report dated 31 October 2012 was prepared based on the information available at the time. Deloitte has no obligation to update our report or revise the information contained therein due to events and information subsequent to the date of the report.

Acknowledgments

The Review Team has had the full cooperation and assistance of the Ministry's staff and management team throughout this review.

The input and guidance contributed by external stakeholders to the review is acknowledged and appreciated.

The Review Team would also like to thank the members of the public involved in the events, and the ex-Ministry staff, who gave their time and information through interviews.

Development of the “kiosks”

Background

As part of Work and Income's strategy to improve the percentage of people moving into jobs, Work and Income sought to provide a self-service facility for job seekers with the tools to search for jobs online and create their CVs. Computers, with limited functionality, have been provided for job seekers for this purpose since 1998 (the “Worktrack PCs”).

In 2009 a “kiosk” concept was developed as the preferred way to improve the self-service experience for clients. It is important to note that what are called “kiosks” at the Ministry are actually ordinary PCs that have been configured and allocated specifically for client use.

The “kiosks” were not a complete step change from the current state at that time. Worktrack PCs had existed since 1998. They were normal PCs located at Work and Income sites to help clients get back to work as soon as possible by providing access and support to job search tools. The computers provided Microsoft Office software such as Excel, PowerPoint, Word and access to specific job search websites. The Worktrack PCs user interface was upgraded to make them easier to use. Over the years the PC hardware and the monitors were changed to keep up with technology (e.g. moving to flat screens). The transition to “kiosks” consisted mainly of the addition of some functionality and the purchase of new, more attractive furniture to house the PCs. The transition also involved the setting up of the “kiosks” at the front of house, in addition to the training rooms previously used to house them. The PCs that made up the “kiosks” included the existing Worktrack PCs and newly purchased machines. Around the same time the Worktrack PCs operating system was upgraded to Windows XP, along with other software and technical changes. The following outlines key features of the two:





Feature	Worktrack PCs	“Kiosks”
Primary Function	<ul style="list-style-type: none"> • Job Search • CV creation 	<ul style="list-style-type: none"> • Job Search¹ • CV creation • My Account² and online applications • Links to other Government external websites (e.g. IRD)
Location	Training room	Front-of-house / Training room
Operating System	Windows 2000 (mostly)	Windows XP

¹ Job Search - Links to job websites

² My Account - An online Work and Income application allowing clients to access information and services. Examples of use include viewing contact details, booking and cancelling appointments, and viewing payment details.

Feature	Worktrack PCs	“Kiosks”
Authentication method	Manual logon with a generic username and password	Remote machine auto logon using generic username and password
Internet Access	List of links provided, others could be accessed by typing directly into the browser, protected by a white list ³ . This would have been in alignment within the NZISM ⁴ as a preferred approach	List of links provided, others could be accessed by typing directly into the browser, protected by a white list until recently superseded by a black list ⁵ . This is in alignment within the NZISM ⁴ as a secondary approach ⁶
Applications	MS Word, MS Excel, MS PowerPoint	MS Word, MS Excel, MS PowerPoint
USB Device Access	Functionality to access or save files on USB	Functionality to access or save files on USB

The pictures below depict the physical layout and the “landing page” where users would first begin when they are using the PCs.

	Work Track	“Kiosk”
What the service looked like		
What the user interface looked like		

³ A website white list is a list of pre-approved websites that may be browsed to and accessed by this device or user – this limits the device or user to only a few that are allowed.

⁴ The New Zealand Information Security Manual v1.1 June 2011

⁵ A website black list is a list of blocked sites that prohibit the device or user from browsing to or accessing them – this provides the device or user more accessibility and only blocks known inappropriate or harmful sites.

Implementation approach and timeline

Overview

The “kiosk” concept was developed from mid-2009 and two separate project streams were involved to deliver the end solution:

- Online Strategy – Self-Service Project** (the “Self-Service Project”): This project was part of Work and Income’s strategy to provide self-service facilities to job seekers. This strategy initiates the investigation into how Work and Income can utilise kiosks to assist job seekers. It produces a preliminary business case for the use of kiosks. User trials are conducted on various kiosk types before it is decided to reuse the Worktrack PCs and turn them into “kiosks”. The scope of the final business case is to purchase “kiosk” furniture, redevelop a user friendly portal page for the Worktrack PCs and to purchase new PCs to supplement the current fleet of Worktrack PCs.
- Infrastructure Roadmap – MSD desktop upgrade, Non-National Office Environment Project** (the “XP Upgrade Project”): This IT project was part of a wider programme to upgrade the operating system version the Ministry used across its environment as it was going to become unsupported. Upgrading the operating system of the Worktrack PCs to XP was one component within the scope of this project. Also within the scope of this project was implementation of additional software related to security features to be installed on the machines. Within the wider Infrastructure Roadmap, Active Directory was implemented for centralised IT administration of user accounts and permissions. The “XP Upgrade Project” sought to utilise Active Directory to create a trust privilege for the “kiosk” to exist in Active Directory as an authenticated Ministry user. This enabled the “kiosk” to have permission to access internal Ministry machines and devices that were not explicitly restricted.

The governance and review arrangements are set out below:

Governance	Technology focus	ITGC ¹	
	Business focus	OIPBSG ³	DUSG ⁴
Sponsor		DCE Work and Income	DCE People Capability and Resources
Project Reported to		Director Online and Infrastructure Work and Income	CIO
Project		Self Service Project	XP Upgrade Project

- The *IT Governance Group (ITGC)* was a Ministry wide governance group that was re-established in 2009 after a hiatus. The ITGC provided “direction on, and controls, current and future significant IT projects. It provides an oversight of significant projects and ensures IT projects are driven by the Ministry’s business needs”. The ITGC membership comprised all of

the Deputy Chief Executives who all regularly attended. In October 2011 leadership agreed to trial a new governance arrangement in which three groups were created (Leadership Team Board, Business and Strategy). These groups were tasked with providing overarching governance for organisational performance capability, risk, strategic issues, direction, budgeting and business management, and scoping discussions of business initiatives. The membership of these comprised the Chief Executive, all Deputy Chief Executives and the Director of the Office of the Chief Executive. This new governance arrangement was confirmed in May 2012

2. The *Work and Income – Online and Infrastructures Projects Business Steering Group (OIPBSG)* is a governance committee that was set up to cover all Work and Income projects. This governance committee formed in December 2010 and evolved from a Work and Income Programme of Work Steering Committee which began mid-2008. The membership of this governance committee has changed over time. Attendance has included representatives from Work and Income, Finance, Risk and Assurance, IT and Deputy Chief Executives.
3. The *Infrastructure Roadmap - Non-National Office Environment Project Business Steering Group* began in June 2010 to provide project governance. This governance group then changed its name to *Infrastructure Roadmap - MSD Desktop Upgrade Steering Group* in July 2010 (**DUSG**). Membership predominately comprised IT staff but also included representatives from Work and Income and StudyLink. The governance committee disbanded at the end of the project around September 2011. There were a few small items to wrap up in early 2012 these were passed from the project to day to day operations.

Design

The “Reference Architecture Self-Service Kiosks” document was prepared in June 2009 by a Technical Architect. This paper outlines two possible options for the “kiosks”. One option is to provide a direct Internet Service Provider (ISP) connection for access to the internet. This was stated as the preferred option. The secondary option was to integrate the “kiosks” to the Ministry’s corporate network, particularly if value added services such as workflow and communication link integration with Ministry applications was required for services. The outline of the secondary option specifically required network separation for security to be addressed and for appropriate circles of trust to be implemented if this option was to be used. This aligned with the subsequent Government Cybersecurity Plan and the NZISM relating to the requirement for “server separation when connected to public systems”, such as the “kiosks”. The Preliminary Business Case in 2009 also discusses separation of “kiosks” from the Ministry’s corporate network. However, this does not appear as either a requirement or as a key assumption in any of the projects’ requirements or design documents.

In the information provided to the Review Team to date, there was no explicit, overall analysis of security and privacy risks associated with public access, or of risks and implications of connections to the network in relation to the “kiosks”.

Design work and testing focused on the user experience – for example, the Self-Service Concept trials in 2010. At that point, options such as touchscreen and custom devices other than upgraded PCs were still being considered.

It is unclear at what point the assumption or requirement for “kiosk” separation from the network was lost. **In the information provided to the Review Team, the first point at which it is missing is within the May 2010 Statement of Work High Level Planning for Self-Service Concept Trial and Technology Solutions.** No evidence of any reassessment or analysis of security and privacy risks associated with the loss of network separation as an assumption or requirement has been found.

Various security requirements were specified and implemented for the “kiosk” machine itself. These measures were mostly in alignment with good practice and, the subsequent Government Cybersecurity Plan and the NZISM. We would expect these measures to be in place for any system that would be used as a “kiosk”. They included

- End point protection software that provides malware protection, prevents the PC from being booted with a USB drive, and is able to check for key logging software. This software is to protect the kiosk device itself from being compromised, for example from a virus outbreak.
- End point agent software that provides the functionality to update software, and collect hardware and software inventory data.
- The automated clean-up of history and cache files to reduce the risk of being able to view other people’s internet browsing history or other session information.
- An automated rebuild procedure to ensure malware hacking code is not installed on the PC.
- Automatic machine shut down and start up at an agreed time every day. This prevents unauthorised use of “kiosks” outside of normal operation hours, and was part of the security feature to clear out any changes made on the kiosks and additional information stored.
- Not having a roaming profile or data storage for the PC user account. This is to prevent information or settings stored by one user, being accessed or used by a subsequent user.

It was found that at the time of deployment, a decision was made to not patch the “kiosks” with operating system security fixes. This is a deviation from good practice and the NZ SIGS⁷ and the NZISM. Notwithstanding the operating systems patches were not applied, this did not change the security risk profile of the “kiosks” in relation to this breach.

Testing

The project team for the XP upgrade that covered the “kiosk” environment approached the IT Security team about the security team’s requirements for project completion. The IT Security team engaged Dimension Data (through its subsidiary, SecurityAssessment.com) for a penetration test in April 2011, as part of the XP upgrade project for “kiosks”.

The penetration testing that was commissioned appeared to be in alignment with typical testing of this nature, commissioned within a project, and was scoped to focus on whether the “kiosk” could be compromised to access the Ministry’s data. The penetration testing reported six findings, composed

⁷ NZ Security in the Government Sector

of one critical rated finding, two urgent rated findings, and three medium rated findings. The critical rated finding was related to weaknesses on the protection measures at the “kiosk” itself. The two urgent rated findings consisted of the lack of network separation and the access to potentially sensitive data via network shares⁸, respectively.

Each finding was supported by a specific recommendation. **The executive summary highlighted the network separation issue as the most pressing, and made a clear recommendation that the “kiosk” solution should not be deployed into a production environment until network separation was achieved.**

Two meetings were held in relation to the Dimension Data report.

1. A presentation by Dimension Data on the findings from the penetration testing. There is only anecdotal information on which staff from the Ministry attended. It included technical members of the Ministry’s IT team covering security, MS Windows, network and testing. It is unclear whether other Ministry staff attended.
2. A meeting with the XP Upgrade project team and technical members of the Ministry’s IT team covering security, MS Windows, network and testing. This meeting discussed the actions to be taken based on the Dimension Data report findings.

The decisions recorded in the notes from the second meeting were:

- That the Critical finding would be addressed.
- Various options were discussed relating to the Urgent finding on network separation. The IT Network Services team preferred the option of implementing routers with security features to provide firewalling functionality. An action was agreed that the preferred option for network separation be costed and funding be requested.
- That no action would be required on the other Urgent finding on access to sensitive information, because this issue would be resolved with network separation (above).

The action taken by the Ministry in response to the finding that sensitive data was uncovered on an unrestricted network share was to restrict access to that share immediately. However, no further work was conducted to identify any other accessible network shares at this time.

The risk associated with the lack of “kiosk” network separation was recorded both in the XP Upgrade Project risk register and the IT Security External Threat risk register. The risk was rated “medium” overall, comprising “rare” likelihood and “major” impact. Further, the IT Security team requested that the risk arising from the lack of network separation be escalated beyond the project to the Desktop Upgrade Steering Group, and a member of the IT management team was copied on this request. However, there is no evidence that the security risks around the “kiosks” or any of the penetration testing findings were escalated any further.

⁸ A network share is a set (directory) of information on a computer that can be remotely accessed from another computer, via a local area network transparently as if it were a resource in the local machine

The costing of router replacement was completed and a funding request prepared. However, the funding request did not discuss the security risk and it appears that the funding request was never formally accepted or acted upon. The Review Team was informed that the network refresh programme that this funding request related to has now been replaced by a wider network programme that is still in progress as at the date of this report.

No further meetings occurred to verify that the recommendations of the Dimension Data report were implemented. There is no evidence that the “kiosks” were retested prior to the roll out.

The following table summarises the actions taken against each of the Dimension Data report’s findings.

	Finding	Action
Critical	<ul style="list-style-type: none"> • “kiosk” device weaknesses 	<ul style="list-style-type: none"> • Resolved prior to roll-out
Urgent	<ul style="list-style-type: none"> • Lack of network separation • Access to sensitive data via network shares from the “kiosk” 	<ul style="list-style-type: none"> • Not resolved • Not resolved
Medium	<ul style="list-style-type: none"> • Three “medium” rated findings. 	<ul style="list-style-type: none"> • One resolved • Two not resolved

The following outlines some of the key timeframes in the development of “kiosks”.

Date	Event
1998 – 2009	Pre-“kiosk” machines, referred to as Worktrack PCs were installed for use by job seekers. These machines were standard PCs that allow clients to access the job sites on the internet and work on their CVs. These machines were connected to the Ministry’s corporate network and allowed for the use of USB keys.
June – October 2009	<p><u>Stream 1: “Self Service”</u> – As part of Work and Income’s online strategy to provide greater efficiency, the concept of a self-service use “kiosks” is explored.</p> <p>A Reference Architecture document is developed for kiosks which provide options and recommendations for future kiosk design. The recommendations cover both network options. One option is for the kiosks to have direct internet access. The other option is for integration into the Ministry’s corporate network. Requirements specified include measures for integration from a network perspective. This would have been in alignment with the Government Cyber Security Plan.</p> <p>A Preliminary Business Case is developed. The Preliminary Business Case identifies security risks (associated with the then current state Worktrack PCs as well as looking ahead to “kiosks”) and suggests that separation of the devices from internal systems would remove the risk.</p>
February 2010	<u>Stream 2: “XP Upgrade Project”</u> – A project to upgrade the operating system running on the desktops and laptops outside of the main Ministry campus is approved by the Information Governance Steering Group Committee. The scope of the project includes the Worktrack PCs (which account for less than 10% of the machines that were to be upgraded as part of the project).

May 2010	Statement of Work High Level Planning for Self Service Concept Trial Online and Technology Solutions paper is released. There is no mention of security requirements or network connectivity changes required. This appears to be the first point where the requirement for “kiosk” separation from the network is missing.
June 2010- August 2010	<u>Stream 1: “Self Service”</u> – Work and Income trials various types of “kiosks” including the use of touchscreen technology.
October 2010- January 2011	Based on user feedback from the kiosk trials the decision is made that the self-service kiosk will be based on existing Worktrack PC architecture.
February 2011 onwards	<i>The Ministry’s Canterbury earthquake response activities commence with a number of key personnel being seconded out of their roles for this effort. This has a major impact on business as usual and projects within the Ministry.</i>
March 2011	<u>Stream 2: “XP Upgrade Project”</u> – A new Windows XP “kiosk” PC image is developed to support the Self Service programme for Work and Income. The design was refined based on usability feedback and test results.
April 2011	<u>Stream 1: “Self Service”</u> - The final business case for the Self Service project is approved by the Information Technology Governance Group. This scope covers purchasing of additional PCs and “kiosk” furniture.
April 2011- May 2011	<u>Stream 2: “XP Upgrade Project”</u> - “Kiosk” penetration test conducted by Dimension Data over the proposed new Windows XP build. Dimension Data present the findings presented and release the report. Six issues are identified.
May 2011	<u>Stream 2: “XP Upgrade Project”</u> - Meetings to discuss the issues and recommendation of the Dimension Data report. The risk relating to “If a Worktrack PC is compromised, a user may be able to gain unauthorised access to the Ministry’s data” is raised on the XP Upgrade Project Risk Register by the project team. The risk is rated “medium”. The risk is not escalated to the governance level.
May-June 2011	<u>Stream 2: “XP Upgrade Project”</u> - Migration of Worktrack PCs to the new “kiosk” build occurs. This includes implementing two out of the six security recommendations that were identified in the Dimension Data report. Decision made to not update patches. The Review Team could not find any mention in Desktop Upgrade Steering Group minutes of any mention of penetration testing having been done, any security vulnerabilities identified, or the decision not to patch.
July 2011	<u>Stream 2: “XP Upgrade Project”</u> – The risk relating to lack of “kiosk” network separation is raised on the IT Security External Threat Risk Register by the Ministry’s IT Security team. The risk is rated “medium”. The register is maintained by the IT Security team as an informal capture point for various security threats and risks across the Ministry. No formal governance or escalation process exists for this register.
August- October 2011	<u>Stream 1: “Self Service”</u> – The rollout of “kiosks” is completed as per the Self Service Business Case. The total number of computers available to clients after the rollout is more than 700.

During the development of the “kiosks”, it is also worth noting by way of context, that between February 2011 – June 2011, 120 staff from the Ministry’s IT function of approximately 400 staff,

spanning key areas including senior members of the management team, were dedicated to the work in Canterbury, following the earthquakes in February 2011. The work included assistance in setting up CERA. This caused many impacts including putting pressure on business as usual and project activities, and stress on personnel. This series of circumstances would likely have contributed to a lack of “normalcy” in the IT organisation during that time.

Findings

Insufficient focus on security and privacy during design and build

Security and privacy were not key aspects in determining the requirements of “kiosks” within the design and build activities. **Though there was a Reference Architecture for Self Service “kiosks” in existence, the guidance provided was not followed when the “kiosks” were developed and deployed.** There is little evidence, at the design stage, of analysis of security and privacy risks, specification of requirements based on such analysis, and assessment of the solution design to ensure that requirements are met and risks are mitigated. There was no explicit focus on evaluating and implementing security measures to prevent possible access to the Ministry’s data from a public area.

The Preliminary Business Case identified security risks (associated with the then current state Worktrack PCs as well as looking ahead to “kiosks”) and suggested that separation of the devices from internal systems would mitigate risk. **However, in the Final Business Case, while other kinds of project risks were identified, there was no discussion of security risks.** It is unclear at what point a decision relating to the separation of the “kiosks: from the network was made, and no evidence that the security risk was reassessed.

Appropriate independent testing and advice to ensure security

The work carried out by Dimension Data to test the security of “kiosks” was appropriate, and in line with the scope and objectives set out in their engagement terms with the Ministry. **Their testing identified the issues that have contributed to the security breach.**

Inadequate response to findings from security testing

The Ministry’s response to the findings and recommendations of Dimension Data’s report was inadequate. Only two out of the six findings were remediated. **The Dimension Data report detailed the lack of network separation and the existence of accessible network shares. These findings were not remediated by the Ministry. The findings of the report were not escalated.** Rather, the Ministry’s development focused only on hardening the “kiosks”, instead of separating the “kiosks” from the Ministry’s corporate network. **If these two findings had been remediated, the security breach could not have occurred in the manner that it did.**

Inadequate risk management and escalation within the IT organisation

The risk associated with the lack of “kiosk” network separation was recorded both in the XP Upgrade Project risk register and the IT Security External Threat risk register. The risk was viewed purely from a project scope perspective rather than in a broader business and organisational context. There appears to have been an assumption held by some of the project and IT team members that only project risks that were rated above “medium” were to be escalated to Steering Groups or other senior member of the Ministry’s management team. The policy guidelines are silent on the escalation of risks that are not rated as “high” or above. Best practice provides for escalation of all risks. **The IT Security team had requested that the risk arising from the lack of network separation be escalated beyond the project to the Desktop Upgrade Steering Group, and a member of the IT management team was copied on this request. However, there is no evidence that the security risks around the “kiosks” or any of the penetration testing findings were escalated any further or acted upon. Neither is there any evidence of further follow up by the IT Security or project teams on this matter.**

Incomplete project information and policies

It has been difficult to identify the exact scope and relationships between the projects involved in the “kiosk” build because the type of project documentation we would usually expect (e.g. charters, initiation documents, explicitly approved design documents) does not appear to have been developed, maintained consistently and signed off. **The Review Team has also found that project risk management and escalation policies applied in the “kiosk” project were not sufficiently prescriptive and could be subject to different interpretations, resulting in the potential for risk related decision making that was flawed, and made at the wrong levels of the organisation.**

Operation of the “kiosks”

Overview

736 “kiosks” are deployed across all of the Work and Income Service Centres. The “kiosks” allow Work and Income clients to:

- Access internet job sites
- Access email – for example, to check for job notifications
- Create, store and maintain CVs or application letters

Operating practices

Self-service “kiosks” are available to clients during normal opening hours of the Work and Income Service Centres, which are

- 0930 – 1700 on Wednesdays
- 0830 – 1700 on Mondays, Tuesdays, Thursdays and Fridays.

Functionally, they provide internet access, access for USB storage devices, Microsoft Office applications and printing.

The fleet of “kiosks” is centrally managed, with automatic daily start up and shut down at 0700 and 1710 respectively. The “kiosks” are purged nightly, and updates associated with the end point software protection such as anti-virus signature updates are made once per week. However, there is no patching, proactive monitoring and alerting, and no logs of “kiosk” usage outside of trending data on the patterns of use. “Kiosks” are monitored as part of the overall network performance monitoring across the large amounts of network traffic on the network.

Security guards are located in each Work and Income Service Centre. However, their role is to prevent physical threats on the site. Limited physical monitoring of client activity on “kiosks” occurs. Privacy screens are intentionally in place so that client activity is difficult to observe. Given their intended purpose, it is not unusual for clients to spend several hours on the “kiosks”.

Findings

Lack of adequate monitoring

Based on the “kiosk” architecture having been implemented without network separation, the Ministry did not have the processes in place to moderate the risk exposure through appropriate monitoring for malicious activity from the “kiosks” on the Ministry’s network.

Insufficient audit trail information

The “kiosks” have a security feature to prevent storing of user changes to the “kiosks” and preventing information leakage between two user sessions. This feature prevents any changes from being stored permanently and therefore, precludes the ability to store logs on the “kiosks”. However, there are other logs available that provide varying levels of visibility of the traffic between the “kiosks” and the network. Based on the risk exposure of the “kiosk” deployment as a result of not using network separation, and the trust privileges the “kiosks” had to the Ministry’s network, a higher level of audit trail visibility and retention required to moderate the risk would be expected. This was not found to be in place.

Policy and process on the level of trust to be assigned to the “kiosk” device is unclear and inconsistent

There are no defined security processes relating to the business use of “kiosks”. The level of trust the Ministry wishes to assign to the “kiosk” device is not clear at a policy and process level for effective approaches to be considered

No alerting of suspicious activity

There is no alerting or notification if the security-related software is disabled or tampered with, or other security controls on the “kiosk” are by-passed. Some of the technical measures may be constrained in terms of the alerting functionality available.

Events and the Ministry's responses

Overview

This phase of the review considers three events where information was provided to the Ministry by third parties raising security concerns about the “kiosks” and the Ministry's response. These are:

10 October 2011	<i>Ms Brereton, a Beneficiary Advocate, raises an access to information issue with Work and Income.</i>
08 October 2012	<i>Mr Bailey calls the Ministry, indicating that he knows of a vulnerability in the Ministry's systems.</i>
14 October 2012	<i>Mr Ng alerts the media and Office of the Privacy Commissioner to a security vulnerability in the Ministry's systems.</i>

The latter two events are related, with Mr Bailey and Mr Ng collaborating to an extent.

Our understanding of the event involving Ms Brereton is limited to an interview conducted with her and reviews of emails that were sent in relation to the event. No technical information to confirm technical details of the event is available.

Our understanding of the latter two events is based on interviews with Mr Bailey and Mr Ng, as well as reviews of network logs. We have also been able to confirm details of the Ministry's response to these events through review of emails, meeting notes and interviews.

Beneficiary Advocate Ms Brereton's notification of a potential incident

Ms Brereton was attending a session to familiarise Beneficiary Advocates with the new “kiosks” when another Beneficiary Advocate, a volunteer, who also worked as a systems administrator in another role, uncovered a way to gain access to computer names and internet protocol address information which Ms Brereton considered sensitive. She raised the matter with a Work and Income manager. Work and Income escalated the issue to the IT Security team. Ms Brereton's details were forwarded to IT Security. IT Security made an unsuccessful attempt to contact Ms Brereton. No further attempts were made.

Date	Event
Mon 10 th Oct 2011	At the invitation of the Ministry, Beneficiary Advocates attends a session to become familiar with the new “kiosks”. During this session Ms Brereton is shown by one of her staff how to access internal Ministry

information. Ms Brereton raises the issue with Work and Income staff

Tues 1 st Nov 2011	Ms Brereton raises the access to information issue with a senior business manager. This information is recorded as being a concern raised around the disclosure of "IP addresses of all PCs including staff PCs in the office through the kiosk" and the issue is forwarded within the Ministry to be investigated.
Wed 2 nd Nov 2011	Work and Income escalates the issue to the IT Security team <ul style="list-style-type: none">The IT Security team requests more information, especially the date when the issue was detected and the site at which it was detectedWork and Income provide information on the date when the issue was detectedThe item is not logged as an incident
Tues 29 th Nov 2011	Work and Income queries the IT Security team about progress on this issue.
Wed 30 th Nov 2011	The IT Security team informs Work and Income that they have not been able to replicate the issue and require more information about the issue. <p>The IT Security team also states that the "kiosks" has been tested by a firm of penetration testers and that one of the recommendations was to deploy firewalls at all sites to isolate the "kiosks". This recommendation was still in the planning/budgeting stage. While awaiting the recommendation to be implemented, the IT Security team's view is that the risks the "kiosks" exposes the Ministry to, are acceptable. These views are expressed to the Work and Income staff following the issue up.</p> Work and Income query the IT Security team about the risk of this issue. <p>The IT Security team expresses confidence that at the time of the testing the "kiosk" was secure.</p>
Thurs 8 th Dec 2011	Ms Brereton raises the issue again and Work and Income forward her contact details to the IT Security team.
Mon 12 th Dec 2011	IT Security staff attempt to contact Ms Brereton, unsuccessfully.
Dec 2011 – Feb 2012	Ms Brereton was away from the Beneficiary Advocates office. No further follow up activity occurred.

Additional Information

Date	Event
Thurs 4 th Oct 2012	Connections are made from a "kiosk" in Newtown using the network mapping features. Based on log analysis, the Ministry has subsequently identified that it does not appear that files were downloaded through this network access. At this time we cannot confirm who made the connections using the network mapping feature.

Mr Bailey notifies the Ministry about a security vulnerability

While using a “kiosk”, Mr Bailey notices that he is able to map network drives from the “kiosk”. He explores what kind of information he can access. He telephones the Ministry, who sought further information from him about the vulnerability. The Ministry tries to identify the vulnerability and commissions penetration testing.

Date	Event
Fri 5 th Oct 2012	<p>Mr Bailey uses a “kiosk” in Newtown and discovers it is directly connected to the corporate network, that he can map network drives, and that he can see files on servers that he believes should be secure.</p> <p>Based on subsequent log analysis, the Ministry has also identified that connections are made from a “kiosk” in Willis Street.</p>
Mon 8 th Oct 2012	<p>Mr Bailey calls the Ministry seeking information on whether it provides rewards for security vulnerability information.</p> <p>The Ministry attempts to obtain further information. Mr Bailey declines.</p> <p>Information provided by Mr Bailey is circulated within the Ministry.</p>
Tues 9 th Oct 2012	<p>Based on terms used by Mr Bailey in his call, the Ministry thinks it is a website related vulnerability, and does not consider that it could be a “kiosk” related vulnerability. It appears that this leads them down an incorrect path for their initial investigation and actions.</p>
Wed 10 th Oct 2012	<p>A senior member of the Ministry’s management team contacts Mr Bailey to seek further information and to inform him that the Ministry does not pay for information about security vulnerabilities. Mr Bailey refers to issues with servers and the ability see</p> <p>Mr Bailey mentions that he has been talking to a journalist and does not provide any further specific details of the vulnerability.</p> <p>The Ministry commissions penetration testing of its websites.</p> <p>The Chief Executive and Minister’s Offices are informed.</p>
Thurs 11 th Oct 2012	<p>The Ministry implements an unrelated web application change.</p> <p>The Ministry requests KPMG to undertake testing of its high risk web applications because the IT team assumed that Mr Bailey’s information is related to the web application.</p> <p>No formal report has been issued. KPMG were asked to verbally provide feedback on any major issues uncovered. No information was able to be obtained on what the feedback is, but it was understood anecdotally that no major issues were uncovered.</p>
Tues 16 th Oct 2012	<p>Mr Bailey emails copy of screenshots he accessed from his mobile phone to the Office of the Privacy Commissioner following publicity by Mr Ng.</p>

Mr Ng alerts the media and Office of the Privacy Commissioner to a security vulnerability in the Ministry's systems

Mr Ng is alerted to the security vulnerability by Mr Bailey. The vulnerability is demonstrated by Mr Bailey to Mr Ng at one of the offices. Together and independently they explore the nature of the information they are able to access. Mr Ng alerts the media and Office of the Privacy Commissioner, and releases his findings on his blog. The Ministry contacts Mr Ng to understand the details of the vulnerability, and takes immediate action to cease "kiosk" services as a result.

Date	Event
Mon 8 th Oct 2012	Mr Bailey informs Mr Ng of the security vulnerability.
Mon 8 th - Tues 9 th Oct 2012	Mr Ng and Mr Bailey access the Ministry's corporate network using the "kiosks" at the Willis Street Work and Income Service Centre. Mr Bailey explains and demonstrates to Mr Ng how to access the network and a range of information.
Wed 10 th - Fri 12 th Oct 2012	The Ministry's corporate network is accessed from "kiosks" at the Newtown Community Link and Willis Street Work and Income Service Centres
Sun 14 th Oct 2012	<p>Mr Ng notifies the Privacy Commissioner about the security breach.</p> <p>Mr Ng informs Radio New Zealand about the security breach.</p> <p>Radio New Zealand contacts the Ministry about the security breach. The Ministry calls Mr Ng to receive more information. Ministry staff meets to discuss the security breach. Mr Ng emails the Ministry, detailing servers he accessed.</p> <p>The Ministry communicates with the Office of the Privacy Commissioner.</p> <p>The Chief Executive and the Minister's office are informed.</p> <p>Mr Ng releases the information about the vulnerability on his blog.</p> <p>The Ministry's IT function begins responding to the vulnerability and the security breach.</p> <ul style="list-style-type: none"> • The "kiosk" machine account is disabled. • Server permissions on all servers in Mr Ng's email are changed to restrict access. • "Kiosk" settings are changed to ensure "kiosks" do not start up on Monday morning.
Mon 15 th Oct 2012	<p>The Chief Executive and the Minister are briefed about the security breach.</p> <p>The Ministry announces that there will be an independent review.</p> <p>Mr Ng provides the USB device to the Office of the Privacy Commissioner. The Office of the Privacy Commissioner copied the files from the USB device as part of their own investigation. The Office of the Privacy Commissioner provides the USB device to the Ministry. The Ministry begins classifying the information on the USB device to determine potential privacy impacts.</p>

Tues 16th Oct 2012 Deloitte appointed as the Independent Reviewer. The Ministry commences activities to determine potential hardening options of the “kiosks” in the test environment.

Wed 17th Oct 2012 The Terms of Reference for an Independent Review of the Ministry of Social Development's Information Systems Security is agreed and published.

Work on the Independent Review commences.

What information was accessed?

Ms Brereton's notification

There is no clear information on what information was able to be accessed as part of the Ms Brereton event. Communications between the Ministry and Ms Brereton suggested that the issue related to accessing of IP addresses. There is no evidence that any personal information was accessed, or that any information was copied.

Mr Bailey's and Mr Ng's notification

Through discussion with Mr Ng we understand that all data he retrieved from the network or received from Mr Bailey were copied to the USB device that was subsequently provided to the Office of the Privacy Commissioner and then the Ministry. Mr Ng has stated that he does not have any further data in his possession.

Through discussion with Mr Bailey we understand that he provided Mr Ng with all the data he had and that he has not retained any data with the exception of the screenshots he took.

In determining the nature of the information that was accessed, the Review Team has:

- Interviewed Mr Ng and Mr Bailey
- Obtained USB analysis conducted by the Ministry
- Obtained image of USB device
- Reviewed files on USB via the USB image forensically to understand what types of data were accessed during the breach, and also to assist us in identifying which servers in the Ministry's Corporate Environment had been accessed during the breach.
- Reviewed network log information to corroborate which servers had files copied from them to understand which kiosks had been used in the breach and when, and to correlate this back to which servers the kiosks had accessed

The USB drive contained 7307 files in total. This includes 533 CERA invoices. CERA is dealing with the assessment of the privacy implications of these files separately. The Ministry undertook a process to assess the impact of the security breach on individuals. As a result, the Ministry has identified are 10 individuals who are in the high impact category. This process is discussed in further detail later in the report.

The files were divided into the following groups:

- 6777 files which are images of invoices created by the scanner at the Ministry's accounting function. Some of these invoices have private personal information of clients, including names, addresses, financial information and medical information. To date the primary disclosures of sensitive information identified by the Ministry have been as identified as being a result of the disclosure of the invoice images.
- 378 files from a file store. The information in these files provides information on the names and usage of different Ministry servers. To date the Ministry's review of these files has not discovered any significant violations of individuals' personal information.
- 91 files from the Ministry's call recording system. These files require specific utilities to be played. Both Mr Ng and Mr Bailey indicated that they were unable to open these files. To date the Ministry's review of these files has not discovered any significant violations of individuals' personal information.
- 1 file that reports on the load balancing of the Ministry's email system. This file discloses some Ministry user names, meeting rooms, and car number plates. To date, the Ministry's review of these files has not discovered any significant violations of individuals' personal information in these files.
- 60 images which are screenshots of the "kiosk" screen showing a variety of Ministry and client information. This includes images of folder structures that list fraud investigations, the investigator and the relevant client. To date the Ministry's review of these files has not discovered any significant violations of individuals' personal information.

How was the information able to be accessed?

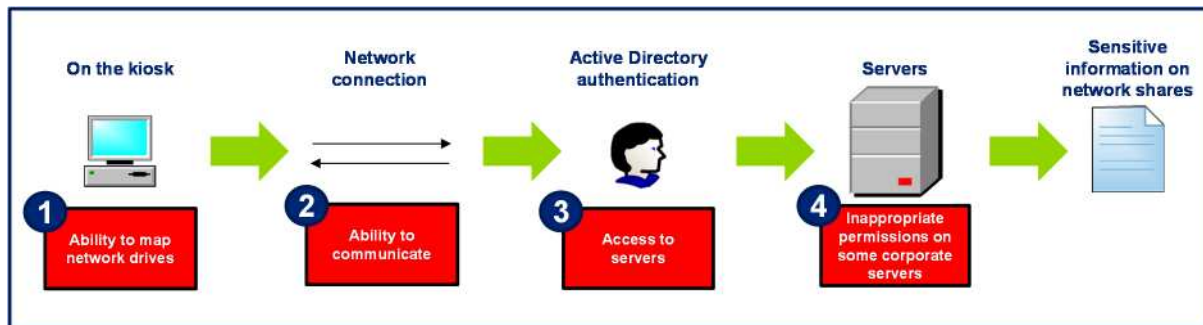
Ms Brereton's notification

The exact method that was used to access information in October 2011 is not known based on the records reviewed. However, the descriptions provided by Ms Brereton during the interview with the Review Team, and the documentation trail suggested that the vulnerability involved access to Internet Protocol address, and computer name information.

Weaknesses identified through the Mr Bailey and Mr Ng notifications

Descriptions provided by Mr Bailey and Mr Ng are consistent, and they corroborate the technical weaknesses outlined below, and the nature of the accessed information that has been able to be established.

There are four technical aspects that enabled access to the information. This is illustrated in the diagram, and described more fully below:



1. The ability to map network drives was not restricted on the “kiosk”

The “kiosk” build allows users to map network drives, utilising existing functionality within the Microsoft Office suite. Being able to map network drives gives “kiosk” users the ability to connect to available shares on the Ministry’s corporate network.

2. Lack of separation between “kiosks” and the Ministry’s corporate network

The “kiosks” are connected directly into the Ministry’s corporate network. There is no physical network separation or logical firewalling to prevent or limit the ability for the “kiosk” to connect to the corporate network, which provided a communication path for information.

3. “Kiosks” operated as an authenticated user on the network Active Directory domain

“Kiosks” are an authenticated device on the corporate network Active Directory domain. This means that “kiosks” have privileges to access shared drives and other resources on the domain that are available to authenticated users. Being an authenticated user in addition to having network connectivity, means that a “kiosk” could not only connect to the corporate network, but also have sufficient privileges to connect and access resources on the network that are not otherwise restricted, for example, printers to support CV printing, and default technical documentation.

4. Shares containing sensitive data on the network are not appropriately restricted

The shares visible on the network contained sensitive data and did not have appropriate permissions applied to restrict access. There were folders on the network that were open in such a way as to allow any authenticated user access to copy files. In this instance, not only were shared folders available but information that was sensitive (e.g. images of invoices) was being stored. However, there is no evidence based on the log analysis work completed at this stage, that any Tier 1 Ministry systems (i.e. those that contain the bulk of the client personal information held by the Ministry) have had their client data breached.

The review team understood these actions to be what took place:

1. On the landing page of the “kiosk” there was an icon which let the individual launch Microsoft Word (or Microsoft Excel / Microsoft PowerPoint).

2. Within Microsoft Word, there was a “File -> Open” option. When this was clicked a dialogue box popped up that had an option to map network drives. When clicked this showed the Ministry’s main network domains.
3. Selecting the Corporate network provided the individual with a list of servers. Some of the servers had drives which could be mapped.
4. After a drive was mapped, the individual opened the files on the share within Microsoft Word and then saved the file to a USB drive.
5. To speed up this process, the individual opened Microsoft Excel at the same time as Microsoft Word, and navigated to the USB drive within Excel. By selecting a file in Microsoft Word then changing to Microsoft Excel using ALT + TAB, the individual copied files directly to the USB from the share, without first saving to Microsoft Word.
6. The individual systematically browsed through the 100’s of servers on the Ministry’s network, and mapped the few drives that were available. Using this method the individual was able to gain access to a variety of file shares, and copy any viewable files.
7. A variety of information was copied including PDFs of invoice images, proprietary media files of call recordings, system/virtual machine default configuration files and information on file directory naming structures.

Although access to map network drives at the “kiosks” does not require a high degree of IT literacy, the further access of network shares to “open” and “read” those files based on the file types involved, required a higher level of IT literacy. It also required a significant and determined effort, and the use of a USB drive, to download and transfer the volume of files that were accessed.

What has happened to the information that was accessed?

Through discussion with Mr Ng we understand that all data he retrieved from the Ministry’s corporate network or received from Mr Bailey was copied to the USB device. Mr Ng has stated that he does not have any further data in his possession and that all other data has been erased.

Through discussion with Mr Bailey we understand that he provided Mr Ng with all the data he had and that he has not retained any data with the exception of the screenshots he took.

Mr Ng gave the USB device to the Office of the Privacy Commissioner on the 15th of October. The Office of the Privacy Commissioner copied the files from the USB device as part of their own investigation.

The Office of the Privacy Commissioner handed the USB device to the Ministry on the 15th of October.

As at 30th October, Mr Ng has signed a statutory declaration confirming that he has removed all of the Ministry’s data he accessed from the “kiosks”. Mr Bailey has provided his verbal assurance, but as at this time, has declined to sign such a statement.

Findings

Inadequate response to Ms Brereton's notification

Work and Income staff escalated the security concern with the Information Security Team and followed up multiple times. The Information Security Team did not have enough information to substantiate or replicate the issue. While there was an attempt to obtain more detail about the issue, this was unsuccessful. **The notification did not follow a clear incident management process, with associated tracking and formal close out requirements.**

There is no evidence that, as a result of the event, the "kiosk" security requirements, design, testing or findings of testing were reviewed to determine whether there was any direct relevance.

The Ministry attempted to obtain further information based on Mr Bailey's notification

Initial communication and escalation of the issue by the Ministry staff member who received the call was prompt. **The Ministry then contacted Mr Bailey within 48 hours. Information provided at the time did not indicate that the vulnerability related to "kiosks".** The Ministry pursued more detailed information appropriately.

There were multiple weaknesses in the security of the "kiosks" that enabled the breach

Four key weaknesses enabled the security breach:

- The ability to map network drives was not restricted on the "kiosk". This means that it was possible to view unrestricted network shares using standard MS Word functionality.
- Lack of separation between "kiosks" and the Ministry's corporate network.
- The "kiosks" operated as an authenticated user on the network Active Directory domain which gave "kiosks" by default, a trusted level of privilege to the Ministry's corporate network.
- Shares containing sensitive data on the network were not appropriately restricted

If any one of these weaknesses had not existed, this particular breach could not have occurred in the manner that it did. The descriptions of the events involving Mr Bailey and Mr Ng were consistent with the weaknesses in "kiosk" security and network log information.

There is no evidence based on work done to date that the Ministry's core tier 1 systems (such as SWIFTT) were compromised

The accounts of the events provided, and the information that was accessed, do not indicate that access was gained to the Ministry's core tier 1 systems. **The Ministry maintains transaction logs for tier 1 systems and has not identified a security breach to these.**

Sound response to Mr Ng's notification

The Ministry has dealt with the notification in a timely and appropriate manner, including escalation and communication of the issue, and engagement with relevant stakeholders such as the Office of the Privacy Commissioner. The Ministry established a war room, stopped the “kiosk” service due to the risk of exposure of clients’ private information, began the process of determining the potential harm that the breach may have caused its clients, and initiated implementation of measures to respond to both the vulnerability and the security breach.

A triage effort to evaluate the privacy impact was prioritised.

The Ministry identified that principle 5 of the Privacy Act was breached in that access to some personal information was obtained by individuals not authorised to access the information. Principle 5 of the Privacy Act requires an agency to take responsible measures to ensure that personal information that it holds is kept secure against loss or unauthorised use, modification or disclosure. If any harm has been caused to any individual as a result of access to the information, then the law requires an agency to redress the harm. The Ministry placed a priority on determining what personal information was on the USB device and to determine the risk of potential harm to individuals. The Ministry’s legal team has analysed all of the files on the USB device received from Mr Ng via the Office of the Privacy Commissioner to determine what, if any risk of harm has been caused to its clients. The Ministry created and implemented a process to enable the legal team to efficiently analyse the files and identify appropriate follow up actions expeditiously.

A technical response was commenced with the tactical focus on shutting down “kiosk” functionality at the sites and in identifying network shares across the population of servers.

The Ministry implemented a cyclic scanning and remediating process. The Ministry used a combination of automated tools and manual checking to identify all accessible network shares. Once an accessible network share was found, the Ministry determined whether the network share was needed or if it could be removed. Where the network share was needed for business processes, the permissions on the share were modified to restrict access to only those users or systems that needed the access. A total of 40 shares have been shut down or restricted.

Based on the actions taken by the Ministry, the potential for unauthorised access to data via “kiosks” has been eliminated.

Key Ministry responses which reduced the risk were to physically disconnect the “kiosk” network points and restricting access to network shares. The physical disconnection of the “kiosk” network points removed an attack channel whereby the Ministry could be targeted. The removal or restriction of the network shares limits the data that is available on the Ministry’s corporate network.

What was the Ministry's Response

Follow up on the events

The Ministry's response to the October 2012 breaches was prompt, consisted of a number of threads and focused on achieving the following key objectives:

- Containing the exposure with urgency to limit the potential impact or harm to its clients and stakeholders
- Frequent communications with the Minister, the GCIO, the Office of the Privacy Commissioner and the State Services Commission
- Establishing service capability to support Work and Income clients to compensate for the lack of self-service "kiosk" functionality.
- Determining the privacy impacts and potential legal implications associated with the specific data that was exposed.
- Investigating the technical details of how the breach occurred and to determine potential technical remedial actions required for restoring "kiosk" functionality to service.
- Obtaining an independent perspective on the causes of the breach and the Ministry's response.

Focused effort has been applied across all of the objectives, and these continue to be a priority for the Ministry. The management response was observed to be well considered and coordinated to cover all appropriate priority areas for a breach of this nature.

Follow up associated with the privacy related consequences

The Ministry has assessed the potential privacy breaches as a result of the personal information disclosed by this security breach. The Ministry has reviewed each disclosure separately, the following questions were used by the Ministry to assess the potential disclosure and the level of harm that the individual may suffer or has suffered:

- Is it possible to identify individuals by virtue of non-common surnames that were disclosed?
- Is the full name of the individual disclosed?
- Are further additional pieces of information disclosed in addition to the individual's full name?
- What is the sensitivity of the non-identifying information that is disclosed?
- Is the individual whose information was disclosed one of the Ministry's vulnerable clients?

This process was observed to be comprehensive, with all appropriate aspects of privacy being considered, including the evaluation of whether any harm as a result of the breach had occurred. Numbers reviewed indicate that there are 10 individuals who are in the high impact category. The Ministry will work with each of these people on a case by case basis to respond to their needs.

Actions taken to stop access from the "kiosks"

The technical response appeared, at a tactical level, to be focused initially on shutting down the “kiosk” functionality at the sites and identifying network shares that were accessible to apply restrictions. Through engagement with the Review Team, further measures were identified to improve risk mitigation and to close off the exposure of access from “kiosk” connection points to the Ministry’s network and data. The Ministry has also commenced an analysis of its logs across all “kiosks” and servers to verify that no other breaches of this nature have occurred. At this point in time, no evidence has been observed to indicate that any of the Ministry’s Tier 1 applications that hold the bulk of the Ministry’s and individuals’ sensitive data have been breached.

Conclusions

Primary causes of the “kiosk” security weaknesses

Based on our review, the following have been identified as the primary causes of the security weaknesses in the “kiosks”:

Security was not adequately considered in the “kiosk” design and implementation.

The “kiosks” as deployed were not designed with the appropriate security requirements.

- The original high level security requirements for network separation were outlined within a “Reference Architecture” document from June 2009. The security elements of this appear to have been lost during the course of the design and deployment process. “Kiosks” were connected to the corporate network (although that was not the preferred option in the Reference Architecture) and without the appropriate separation measures being implemented (deviating from the specified pre-requisite for this option to be used).
- The trust relationships between “kiosk” devices and the Ministry’s corporate network and resources were not defined to be appropriately restrictive. Being an authenticated user in addition to having network connectivity, meant that a “kiosk” could not only connect to the corporate network, but also had sufficient privileges to connect and access any accessible network resources such as network shares that were available to credentialed Ministry users.
- It appears that the wider security threats and risk implications of the “kiosk” in relation to potential access to the Ministry’s data was not considered as a deciding factor when designing and deploying the “kiosks”.

The exposures identified within the Dimension Data penetration test report were not appropriately addressed and followed up.

The findings in the Dimension Data clearly identified the risk exposures of the lack of network separation and the ability to access potentially sensitive data on the Ministry’s network. These findings were not appropriately followed up on, addressed or escalated for management visibility and action, enabling the exposure to remain.

The risk management processes did not effectively escalate security exposures to management, nor ensure appropriate mitigating actions were taken.

The “kiosk” lack of network separation risk was noted within a project risk register and rated as a “medium” risk. There was a perception amongst some staff within the Ministry (including project management) that only “high” rated risks required explicit escalation. The Review Team was not provided with any project risk management policy to confirm whether that perception was correct. As a result of lack of escalation, there was no risk oversight or governance that would have enabled this security risk to have been recognised and assessed at a higher management level. As a consequence, the appropriate risk mitigation responses could not have been considered.

It appears that the decisions and judgements that were made in connection with the security design, security testing and follow up, and risk assessment rested within the IT Security and project teams. There is no evidence that security risk issues or testing results were escalated to the governance level. There is also no evidence that those involved in the governance of the “kiosk” and XP Upgrade projects made inquiries that could have identified the security issues.

Adequacy of the Ministry’s Response

The Ministry’s response to the October 2012 breaches was prompt. The management response was observed to be well considered and coordinated to cover all appropriate priority areas for a breach of this nature.

The Ministry is going through a process of assessing potential privacy breaches as a result of the personal information disclosed by this security breach. This process was observed to be comprehensive, with 10 individuals identified who would be in the high impact category.

The technical response was initially focused at a tactical level, on shutting down the “kiosk” functionality at the sites and identifying network shares that were accessible to apply restrictions. Through engagement with the Review Team, further measures have been implemented. The Ministry has also commenced an analysis of its logs across all “kiosks” and servers to verify that no other breaches of this nature have occurred.

Restoring “kiosk” service

“Kiosk” services have been stopped in response to the security breach. This prevents the Ministry from providing onsite, online job search functionality. Initial investigations have indicated that a range of security protection measures will need to be implemented for the existing “kiosks” to be restored to service.

We recommend the Ministry does not restore full “kiosk” service without implementing robust network separation measures. There are two broad options:

- Physically separate the “kiosk” network from the Ministry’s network.

- Logically separate the “kiosks” from the Ministry’s network using firewalls or strong access control lists.

These options require careful analysis, and once the preferred option is selected and implemented should be subject to thorough testing prior to “kiosk” service restoration.

Also, the following weaknesses should be addressed in relation to the network separation option selected, and the effectiveness of the measures applied verified:

- **The ability to map network drives from the “kiosks” not restricted on the “kiosks”**
- **Operating “kiosks” as an authenticated user on the network Active Directory domain**
- **Inappropriate restriction of network shares containing sensitive data on the network not appropriately restricted.**

Considerations for Phase 2

Phase 1 of the review was limited to identifying the primary causes of the breach, and consequently was not intended to identify a range of specific recommendations for the findings from the investigation of the breach events and causal factors. Drawing from these and other observations from this Phase 1 review, and taking into account the GCIO⁹ review currently in progress, the scope, approach, and areas of focus for Phase 2, will be determined.

Next steps

The Review Team recommends that the Ministry completes the comprehensive log analysis across all connections from the “kiosks” to Ministry servers that are currently underway.

The Ministry should also complete the evaluation of the options to restore a secure “kiosk” service and progress work on the selected option. It is our recommendation that the full “kiosk” service only be resumed once network separation is implemented.

Phase 2 of the review will commence immediately upon completion of Phase 1. As set out in the Terms of Reference, Phase 2 will review the wider information systems security management and governance across the Ministry, to include people, processes, capability, policy and culture elements.

⁹ Government Chief Information Officer

Appendix A: Terms of Reference

TERMS OF REFERENCE

Independent Review of the Ministry of Social Development's Information Systems Security

17 October 2012

The Chief Executive of the Ministry of Social Development (the Chief Executive) has commissioned an independent investigation into the security breach that occurred through the Ministry's self-service "kiosks" at two Work and Income service centres, which compromised privacy.

The review will be carried out by Deloitte and will be led by Murray Jack, Chairman, Deloitte (the Independent Reviewer).

A Steering Group, with external stakeholders, including the Office of the Privacy Commissioner and Office of the Government Chief Information Officer, has been set up to provide independent oversight of the review.

This review will take into account the recently announced review of publicly accessible systems by the Government Chief Information Officer.

Objectives of the review

The objectives of the independent review are to address the questions raised about the security of the Work and Income self-service "kiosks" focusing on what happened, why it happened, the lessons learned, and the actions the Ministry needs to take to address any security issues raised.

The review will also assess the Ministry's wider information systems security including the policies, governance and culture, and will make recommendations about the actions needed to be taken to restore and increase public confidence in the Ministry's information systems security.

The review will happen in two phases.

Phase One – Matters in scope

The first part of the review will investigate the circumstances and causes of the "kiosk" security breach which compromised privacy, focusing on

- The establishment and operation of the self-service "kiosks" in Work and Income service centres, including:
 - The work done to ensure appropriate information security was put in place at the time that the "kiosk" infrastructure and services were designed and built;
 - The independent testing done to ensure the security was operating as designed; and
 - The Ministry's response to any security issues identified during the testing.

- Information provided to the Ministry by third parties raising security concerns about the “kiosks” and the appropriateness and effectiveness of the Ministry’s response to these concerns.
- The appropriateness and effectiveness of the Ministry’s response to the security breach.

Phase Two – Matters in scope

The second part of the review will assess the appropriateness and effectiveness of the Ministry’s wider information systems security, particularly publicly accessible systems, and including the policies, governance, capability and culture.

The review will identify any lessons learned and make recommendations to the Chief Executive about any changes and improvements needed to the Ministry’s information systems security.

Timeframes and reporting

Phase One - The objective is that Phase One of the review will be completed within two weeks.

Phase Two - The timeframe for the completion of Phase Two of the review will be determined following completion of Phase One.

The reports on both phases of the review will be made publicly available.

Governance

The role of the Steering Group is to provide independent oversight of the review and advice to the Chief Executive.

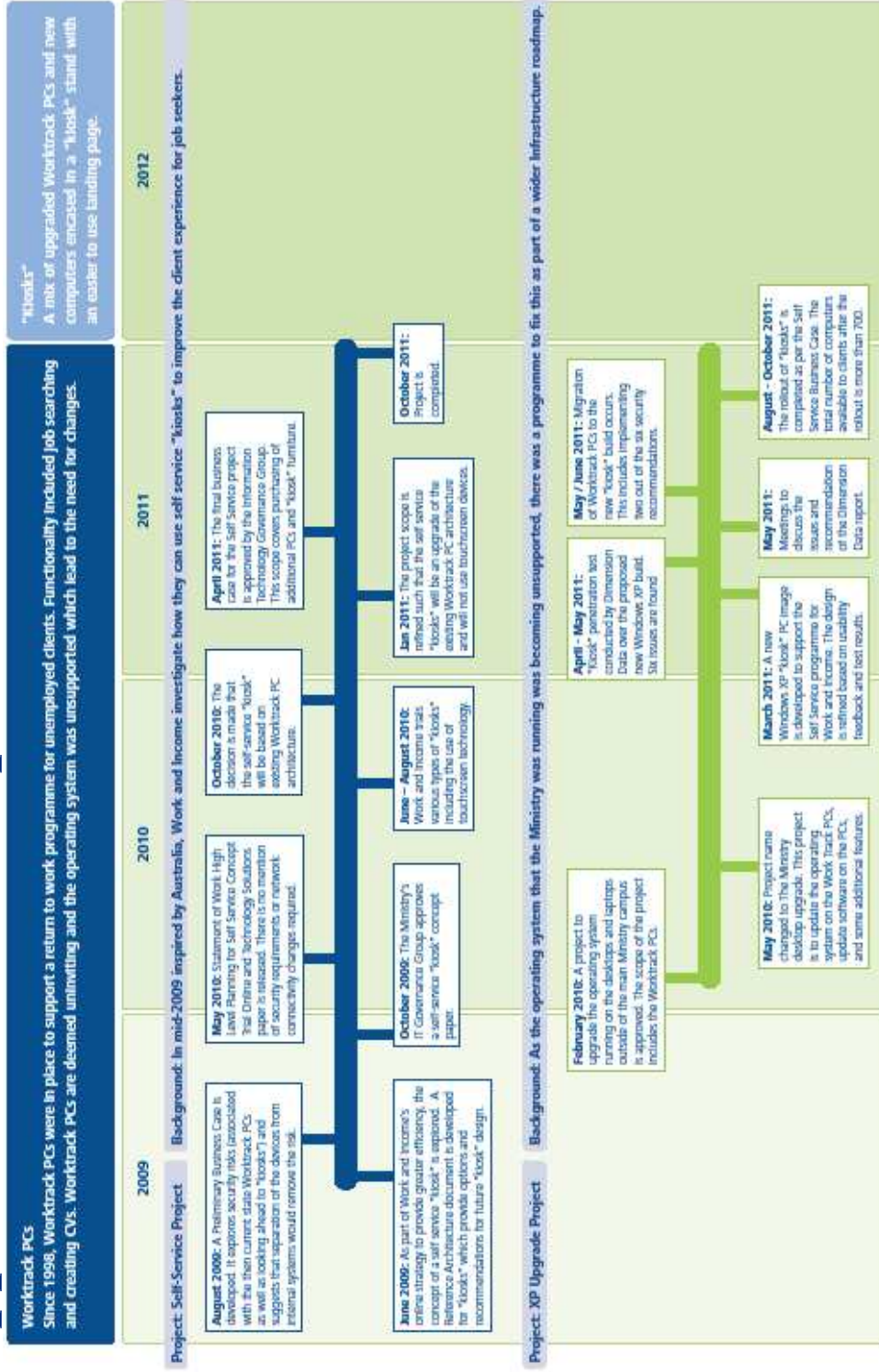
The Steering Group will consist of external stakeholders. The members are:

- James Ogden – Independent Chair
- Erik Koed – Assistant Commissioner, State Services Commission
- Stuart Wakefield – Director, Office of the Government Chief Information Officer
- Katrine Evans, Assistant Privacy Commissioner (Observer)

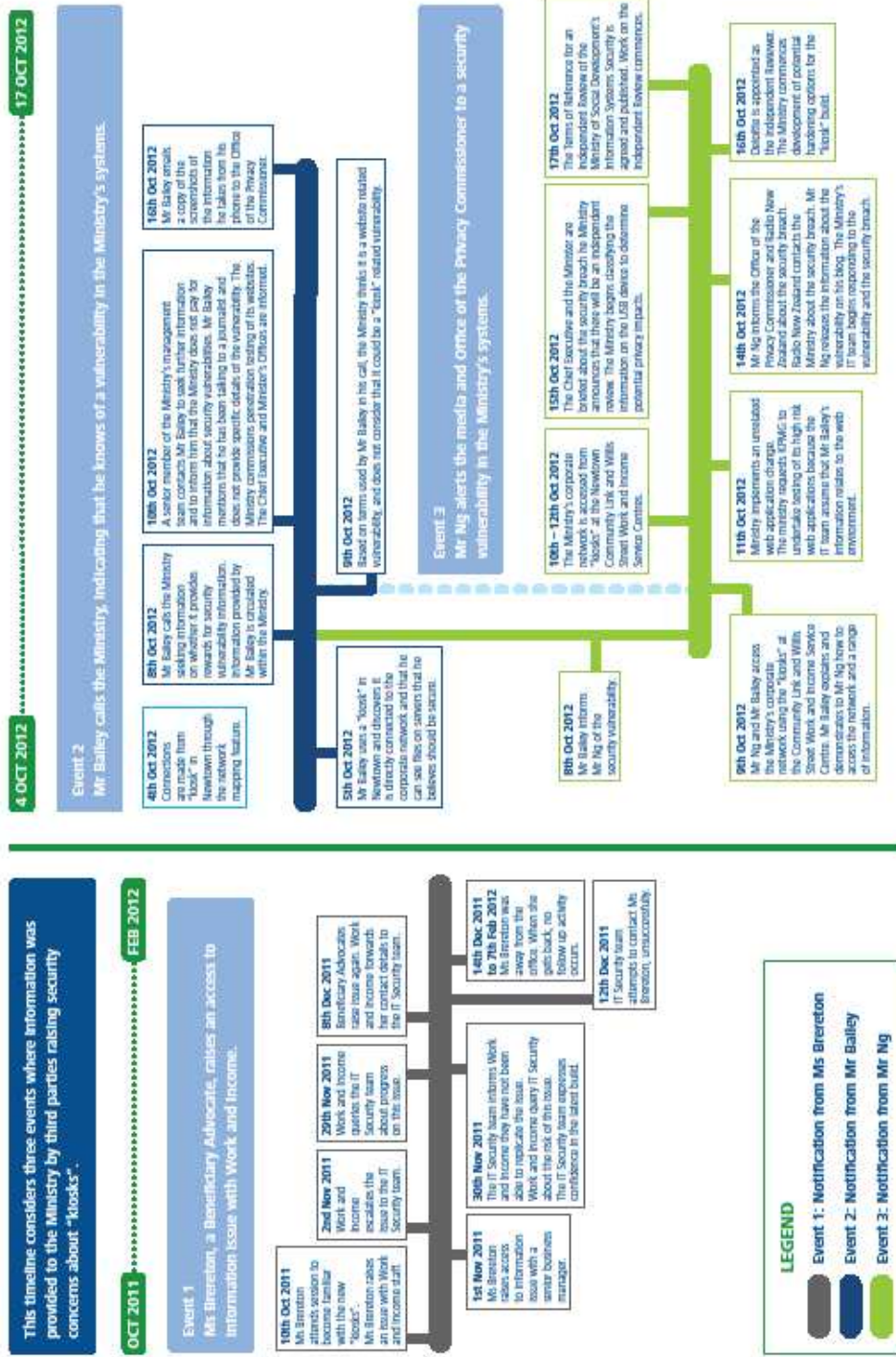
In addition, the following people will attend and participate in the Steering Group.

- Murray Jack – Independent Reviewer
- Brendan Boyle – Chief Executive

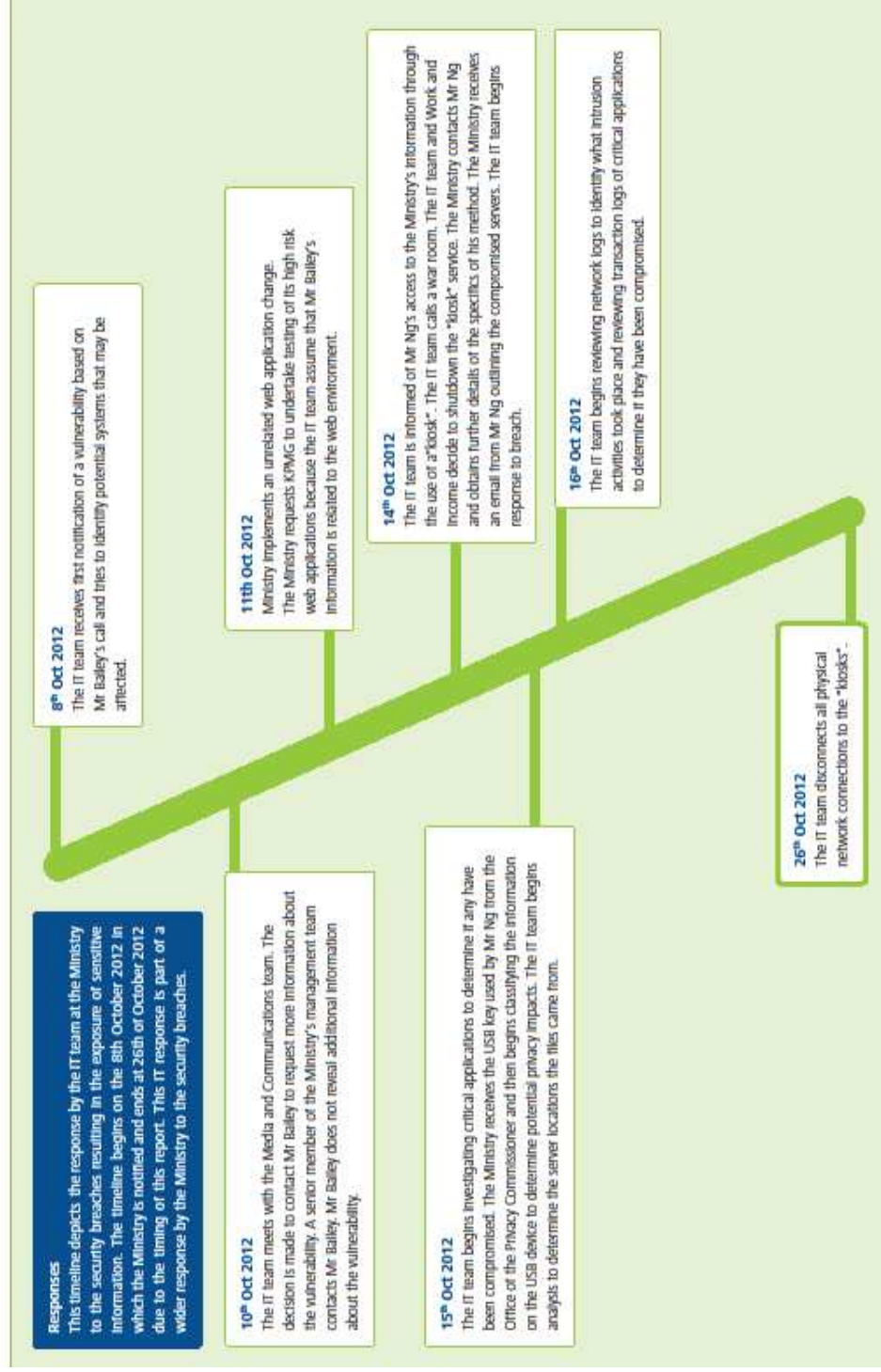
Appendix B: Development of “kiosks” timeline



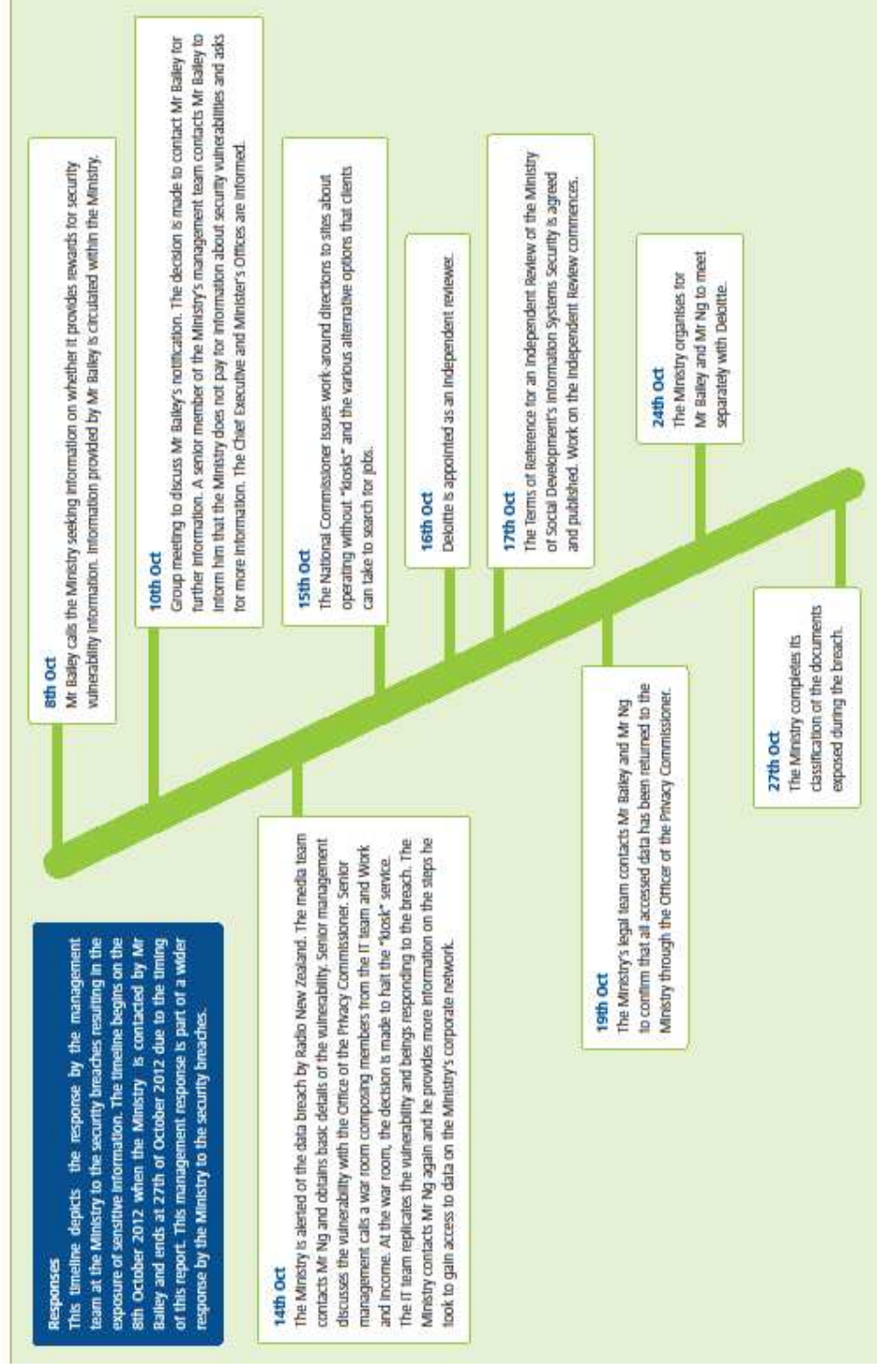
Appendix C: Timeline of the events



Appendix D: Response timeline – Technical focus



Appendix E: Response timeline – Management focus



Appendix F: Glossary

Term	Explanation
“Kiosk”	For this report, “kiosks” refers to the computers, and the associated stands and devices (e.g. keyboards) provided at Work and Income offices for self-service to enable job seekers to create CVs, search and apply online for jobs. “Kiosks” are the successors to the previous <i>Worktrack PCs</i> . Key features of a “kiosks” compared to a <i>Worktrack PCs</i> is that they have additional stands, are designed to look more inviting and have an updated operating system.
Active Directory	Is a technology created by Microsoft that is used to assist in managing a network. Active Directory is used by the Ministry to centrally manage whether a user should be allowed onto the Ministry’s corporate network and what data and systems they are allowed to access.
Authenticated User	A user who has successfully logged into the network. An authenticated user on the Ministry’s corporate network is allowed access across the corporate network and can access data and systems that are not specifically locked down.
Blacklist	A blacklist approach is an approach in which undesired activities or actions are specifically blocked. For example, a website blacklist on a “kiosk” is a predefined list of websites which a user is not allowed to access. The user is able to access anything that is not explicitly on the blacklist. This allows a user greater ability to evade website restrictions than compared to a <i>whitelist</i> approach.
Corporate Network	The primary network used by the Ministry to manage and support the provision of services to Ministry users and clients. Additional authentication and restrictions apply within the Corporate Network for subsets of the environment such as on the Ministry’s Tier 1

Term**Explanation**

Applications.

Deputy Chief Executive (DCE)

A senior member of the Ministry's management team.

Dimension Data

An IT services and solution provider. Its subsidiary *SecurityAssessment.com* was the firm commissioned to perform penetration testing over the Ministry's "kiosk" in April 2011.

Firewall

A software or hardware device on a network that is designed to control and restrict traffic that passes through it based on a set of predefined rules. Traffic that violates the rules will not be allowed through. A firewall is a device that can provide *network separation*.

Forensic Analysis

Examination of digital media with the objective of obtaining and recovering additional data present on the media. This recovered data can be analysed to identify and retrieve hidden and deleted files or data.

Information Technology Governance Committee (ITGC)

A governance committee in place between July 2009 and October 2011 that provided direction on and controlled significant IT projects within the Ministry. Membership comprised the Ministry's Deputy Chief Executives. The ITGC was replaced by different governance arrangements in October 2011.

Job Search

A listing and functionality to link to external job search sites on the "kiosks".

MSD Desktop Upgrade Steering Group (DUSG)

The steering group which provided advice and oversight across the project which was responsible for the operating system upgrade for the *Worktrack PCs* to become "kiosks". This was previously named the *Non-National Office Environment Project Business Steering Group*.

Term

Explanation

My Account

An online Work and Income application that allows clients to access information and services such as the ability to view contact details, book and cancel appointments, and viewing payment details.

Network Separation

The separation of two or more networks so that a system in one network cannot communicate with a system in another network, or is only able to connect in a very controlled and restricted manner. This prevents direct communication and access. Devices such as *firewalls* are used to provide network separation.

Network Shares

Resources (often folders) on a computer or server that are shared across a network, so that other users on the network are able to access it.

New Zealand Information Security Manual (NZISM)

Document produced by the Government Communications Security Bureau to provide technical policy advice and requirements to assist government departments and agencies in securing information systems and the data stored in those systems. The latest version was released in June 2011. <http://www.gcsb.govt.nz/newstroom/nzism.html>

New Zealand Security in the Government Sector

Manual issued by the Interdepartmental Committee on Security which sets out protective security policies, principles and procedures. Additional guidance and more detail is provided in the NZISM. Together they provide updated guidance on securing government functions, resources and information from any sources of harm. <http://www.nzsis.govt.nz/publications/security-in-the-government-sector.html>

Non-National Office Environment Project

The project initiated by the Ministry to migrate all Windows PCs outside the national office environment from Windows 2000 to either XP or Vista. This project included the upgrading the *Worktrack PC*'s operating system as part of the conversion to them becoming "kiosks".

This project was later renamed the *MSD Desktop Upgrade project*.

Term**Explanation**

Non-National Office Environment Project Business Steering The steering group which provided advice and oversight across the *Non-National Environment Project* which was responsible for the operating system upgrade for the Worktrack PCs to become “kiosks”. This was later renamed the *MSD Desktop Upgrade Steering group*.

Online and Infrastructures Projects Business Steering group The steering group which provided business advice and oversight across all Work and Income projects related to online and infrastructure services. This structure was set up in December 2010 and continues to be operating.

Penetration Testing Security testing of a system or network by replicating the types of actions a malicious attacker would conduct.

Reference Architecture Reference architecture is typically a document that provides a template solution with possible options to achieve business objectives. A reference architecture is used as an input when developing a high level design of a proposed system..

Risk Register A documented list of risks identified by a project or organisation. It typically acts as a central location of identified risks to be monitored and tracked to assist with managing identified risks before become problems. A risk register details information about the risk, how likely it is to occur, the impact if the risk occurs, what controls if any are in place to remediate the risk, and individual or role responsible for monitoring the risk and keeping the risk register updated in relation to the latest information about the risk.

Router A network device which directs and transmits traffic to and from different parts of a network. Some routers have the ability to also filter and restrict the network traffic that it transmits but does not have the same complete functionality of *firewalls*.

SecurityAssessment.com A subsidiary of Dimension Data.

The Ministry of Social Development Is New Zealand's largest government department and is tasked with providing social policy advice to the government as well as social services to New Zealand.

Independent Review of the Ministry of Social Development's Information Systems Security Phase 1

© 2012 Deloitte. A member of Deloitte Touche Tohmatsu Limited.

Term

Explanation

Tier 1 Applications

Major applications and systems used to support the Ministry's delivery of key services to clients such as payments of benefits, pensions, student loans and allowances as well as internal Ministry services such as accounting, debt collection and financial management. These are the applications that contain the bulk of the client personal information held by the Ministry.

Whitelist

A whitelist approach is when access is only given to a preapproved list of acceptable actions. For example, a website whitelist on a "kiosk" is a predefined list of websites that a user can visit. The user is prevented from accessing any website that is not on the approved list. This allows for better security than compared to a *blacklist* approach.

Work and Income New Zealand

A service of the Ministry of Social Development that provides financial assistance and employment services throughout New Zealand.

Worktrack PC

PCs which the Ministry made available to the public to assist in job searches since 1998. *Worktrack PCs* are the predecessor of the "kiosks".

About Deloitte

Deloitte refers to one or more of Deloitte Touche Tohmatsu Limited, a UK private company limited by guarantee, and its network of member firms, each of which is a legally separate and independent entity. Please see www.deloitte.com/nz/about for a detailed description of the legal structure of Deloitte Touche Tohmatsu Limited and its member firms.

Deloitte provides audit, tax, consulting, and financial advisory services to public and private clients spanning multiple industries. With a globally connected network of member firms in more than 140 countries, Deloitte brings world-class capabilities and deep local expertise to help clients succeed wherever they operate. Deloitte's approximately 170,000 professionals are committed to becoming the standard of excellence.

Deloitte New Zealand brings together more than 900 specialists providing audit, tax, technology and systems, strategy and performance improvement, risk management, corporate finance, business recovery, forensic and accounting services. Our people are based in Auckland, Hamilton, Wellington, Christchurch and Dunedin, serving clients that range from New Zealand's largest companies and public sector organisations to smaller businesses with ambition to grow. For more information about Deloitte in New Zealand, look to our website www.deloitte.co.nz

© 2012 Deloitte. A member of Deloitte Touche Tohmatsu Limited