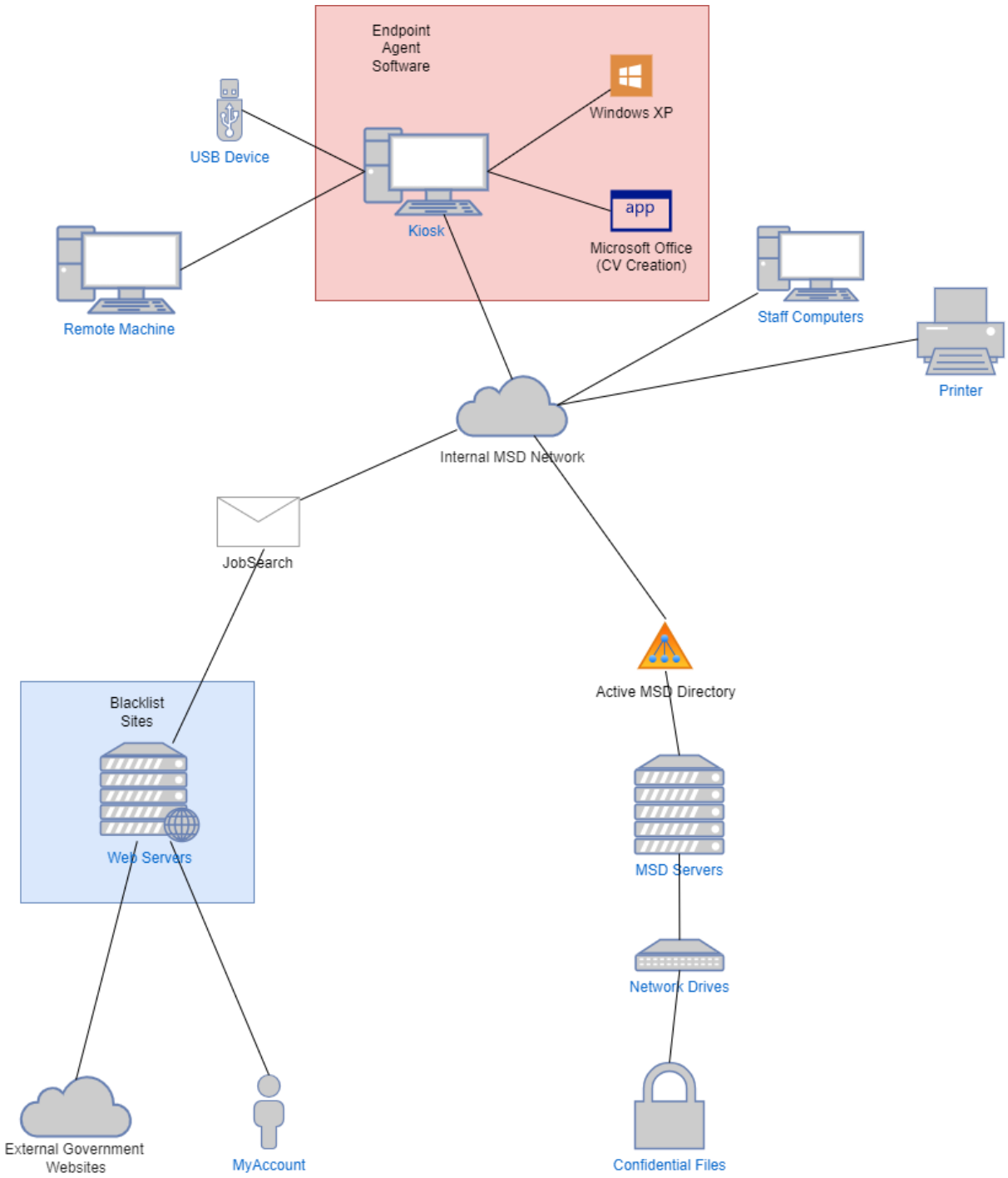
Cam Olssen
300492582
cam.olssen@gmail.com

1. Network Topology



Cam Olssen
300492582
cam.olssen@gmail.com

2.

An Incident Response (IR) strategy is used by organisations to plan their response to security breaches. Containment strategy and Disaster Recovery (DR) are part of the 'Eradication and Recovery' stage of an IR (NIST 61). The containment strategy is implemented after an incident occurs, in order to mitigate further damage. The specifics of this strategy will change based on the nature and severity of a potential breach – it includes both immediate response and investigation to ascertain the source and nature of a breach. Disaster Recovery is a plan to return to "normal operations" and "remediate vulnerabilities to prevent similar incidents" following an incident – in essence, assuring that an incident disrupts the normal business of an organization in as limited and for as short a time as possible.

Category	Description	Handlers
Containment Strategy	Interviewed Ira Bailey and Keith Ng to gain a better understanding of the incident.	Ministry of Social Dev., Deloitte
Containment Strategy	Obtained USB analysis to see what was taken.	Office of Privacy Commissioner, Ministry of Social Dev., Deloitte
Containment Strategy	Obtained image of USB device	Ministry of Social Dev.
Containment Strategy	Reviewed digital forensics of USB device to understand specific files and servers accessed. From this, the files were divided into groups – invoices, recorded phone calls, screenshots showing Ministry and client information, files from the file store and a report on the load balancing of the Ministry's email system.	Ministry of Social Dev.
Containment Strategy	Reviewed network log to discover which kiosk PCs had been used in the breach.	Ministry of Social Dev.
Containment Strategy	Shut down kiosk service temporarily to remove a point of entry for threats.	Ministry of Social Dev.
Containment Strategy	Initial incident information collection via a phone call with Keith Ng.	Ministry of Social Dev.
Containment Strategy	War room set up in order to investigate the breach and mitigate its effects on normal operations.	Ministry of Social Dev.
Containment Strategy	Identified privacy impacts and potential legal liabilities associated with the breach.	Ministry of Social Dev., legal team

Cam Olssen
300492582
cam.olssen@gmail.com

Containment Strategy	Restricted access to the servers which were breached and identified by Ng	Ministry of Social Dev.
Containment Strategy	Identified all other network shares containing Ministry data or client information. When one was found, stricter access controls were implemented or it was removed if unnecessary to normal operations.	Ministry of Social Dev.
Disaster Recovery	Keith Ng signed a declaration that he removed all Ministry data accessed from the kiosk. Bailey gave verbal confirmation but refused to sign.	Ministry of Social Dev., legal team
Disaster Recovery	Worked with clients and stakeholders to try and mitigate potential harm to them.	Ministry of Social Dev., Office of the Privacy Commissioner, State Services Commission, Govt. Chief Digital Officer (GCIO)
Disaster Recovery	Established a service process to give clients the same functionalities that the kiosk system had while the system is shut down.	Ministry of Social Dev.
Disaster Recovery	Obtained an independent third-party review of the security situation from Deloitte.	Ministry of Social Dev., Deloitte

3. Risk Controls:

Deterrent and Preventive Controls

1. According to the guidelines provided in NIST SP.800-53r5, video surveillance defines the necessity to monitor physical access. While it is not necessary, video surveillance would potentially have acted as a deterrent as individuals are less likely to commit illegal acts when monitored/when they believe they are monitored. *(NIST Control PE-6)*
2. According to the guidelines provided in NIST SP.800-53r5, remote access requires protection of confidentiality and integrity using encryption. Encryption can be used to protect sensitive data during remote sessions such as those used by the kiosk system. With encrypted sessions, Ng and Bailey would have found it harder to access the restricted files on the network. *(NIST Control AC-17)*
3. A multi-factor authentication system could have been used to authenticate kiosk users. This could be done using mobile phones or possibly community services cards, as the latter would have made sure that users were WINZ clients – minimising the range of users and as a result decreasing the risk of brute force or dictionary attacks.

Cam Olssen
300492582
cam.olssen@gmail.com

4. Including a time limit on kiosk services could have lessened the risk of attack, as they would have less time in which to launch an attack on the system. This restriction is defined in NIST SP.800-53r5 as a way of controlling sessions. *(NIST Control AC-12)*
5. A code of conduct should have been shown to users when logging into the kiosks. The NZSIM-V.3.2-2018 report classifies this as a MUST – stating that *"Agencies MUST develop and implement a policy governing appropriate Web usage." (NZSIM 14.3.5 – Web Usage Policy)*
6. Banners or other popups on the kiosk PCs reminding users that they are under surveillance could have a deterring effect, as individuals are less likely to commit illegal acts when they believe they are being monitored.
7. The NZSIM report states that *"Agencies SHOULD perform antivirus scans on all content, using up-to-date engines and signatures, using multiple different scanning engines" (NZSIM 20.3.10 – Antivirus Scans)*. These scans can detect malware before it can harm a system. The antivirus MSD was using was not up-to-date, and usage of up-to-date antivirus software in accordance with NZSIM recommendations could have prevented this breach from occurring.
8. According to the NIST SP-800.53r5 guidelines external system connections should use a "deny-all, permit-by-exception" policy – in other words, a whitelist system where only specifically permitted connections are allowed. This would protect against access of threat websites better than the blacklist system used by MSD *(NIST Control CA-3)*. This is also recommended in the NZSIM report which states that *"Agencies SHOULD implement whitelisting for all HTTP traffic being communicated through their gateways". (NZSIM 14.3.10 – Whitelisting/Blacklisting Websites)* This acts as a preventative control as potentially malicious websites cannot be accessed by users.
9. The NZSIM report states that *"Agencies SHOULD monitor relevant sources for information about new vulnerabilities and security patches for software and IT equipment used by the agency." (NZSIM 12.4.3 – Vulnerabilities and Patch Availability Awareness).* This was not done at MSD, and much of their software was out of date and in need of updating and patching, as explained in the Deloitte report.
10. According to the NIST SP-800.53r5 guidelines the direct connection of an internal network should be protected by the use of firewalls. Firewalls control connection and information flow, reducing the risk of malicious activity. (NIST Control CA-3) The NZSIM report also encourages the use of firewalls, stating that *"All gateways MUST contain a firewall in both physical and virtual environments." (NZSIM 19.3.8 - Firewall Assurance Levels).* Use of firewalls is also suggested in the Deloitte report.
11. The network should have had stricter access controls implemented on all necessary internal servers and network shares. The NZSIM report recommends that users are uniquely identifiable and authenticated every time they access a system. *(NZSIM 16.1.16 – System User Identification)* This reduces the risk of unauthorised individuals gaining access to confidential information, as occurred with Ng and Bailey.
12. According to the NIST SP-800.53r5 guidelines, external system connections should be protected by the use of routers, which was not done by the MSD for the kiosk system *(NIST Control CA-3)*. This minimises unwanted traffic.

Cam Olssen
300492582
cam.olssen@gmail.com

Detective Controls

1. The NZSIM report states that *"Agencies SHOULD install host-based IDS/IPSs on authentication, DNS, email, Web, and other high-value services." (NZSIM 18.4 – Intrusion Detection and Prevention Strategy).* This should have been implemented by MSD to detect suspicious activity within the network. This is also supported by the NIST SP-800.53r5 guidelines *(NIST Control SC-7).*
2. MSD should also have installed network-based IDS/IPS tools to detect suspicious activity, according to NIST guidelines which state that agencies should employ automated tools to support real-time analysis of network activity *(NIST Control SC-7).* This is supported by the NZSIM report, which states that *"Agencies MUST develop, implement and maintain an intrusion detection strategy that includes appropriate intrusion detection mechanisms, including network-based IDSs/IPSs and host-based IDSs/IPSs as necessary." (NZSIM 18.4 – Intrusion Detection and Prevention Strategy)* Use of network-based IDS/IPS tools is a valuable part of an intrusion detection strategy and should have been implemented.
3. The NZSIM report states that "Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken." The Ministry should have implemented fraud detection monitoring to find suspicious activity.
4. The NZSIM report recommends *"Agencies SHOULD ensure information security monitoring, logging and auditing is conducted on all accredited systems." (NZSIM 4.4 – Accreditation Framework)* MSD should have practiced regular auditing of their systems to prevent vulnerabilities such as that discovered by Ng and Bailey from being exploited.
5. The NZSIM report states that *"Agencies MUST develop, implement and maintain tools and procedures covering the detection of potential information security incidents, including… audit analysis." (NZSIM 7.1 – Detecting Information Security Incidents).* MSD could use this as a potential detective tool, as audit analysis involves analysing logs in order to check for potentially suspicious activity.

Responsive and Corrective Controls

1. The MSD should have had an Incident Response plan ready to have an established protocol for what to do in the event of an incident. They did not have one to follow ahead of time, and when Bailey and Ng first contacted them, they disregarded information of the breach. As stated in the NZSIM report, *"Agencies MUST develop an Incident Response Plan and supporting procedures"* and *"Agency personnel MUST be trained in and periodically exercise the Incident Response Plan"*. (NZSIM 5.1 – Documentation Fundamentals) Going forward, it will be important for MSD to have a comprehensive plan for incident response, and to ensure personnel are trained in what to do in the case of another incident.
2. A Disaster Recovery plan should have been ready and implemented. MSD had some set steps which were followed – contacting an independent third-party and running internal analysis. However, they did not have a plan for maintaining normal operations, and a lot of time was spent planning a backup system to the kiosks as one was not already in place. In the NZSIM report, it details that developing a DR plan ahead of time will reduce the time spent between the disaster and returning to normal operations, recommending that *"Agencies SHOULD*

Cam Olssen
300492582
cam.olssen@gmail.com

develop and document a Disaster Recovery plan." (NZSIM 6.4 – Business Continuity and Data Recovery).

3. The same section of the NZSIM report states that organisations should develop a business continuity plan, so that critical systems can continue to operate with constraint. In MSD's case, when the vulnerable servers were identified they restricted access to them, removing network shares. When this was occurring, nothing would have changed for their internal staff, allowing them to continue operations. NIST also recommends this and states that organisations should *"Plan for the continuance of essential missions and business functions with little to no loss of operational continuity." (NIST Control CP-2, NZSIM 6.4 – Business Continuity and Data Recovery)*
4. MSD should regularly run automated 'clean-ups' of the kiosk PCs to wipe history and cache files, preventing users from accessing previous users' personal or account information. This is recommended by the Deloitte report. *(Deloitte, "Development of the 'kiosks'", p14)*
5. The kiosk PCs should have end point protection software installed which prevents them from being booted with a USB drive and is able to check for installed malware. This will assist in preventing kiosk PCs from being compromised in future and is recommended by the Deloitte report. *(Deloitte, "Development of the 'kiosks'", p14)*
6.
7. The kiosk PCs should have an automated and regularly scheduled rebuild procedure to ensure that no malicious software is installed. This will also help with the issue addressed by the 'clean-up' suggestion by wiping user history and cached data, ensuring that clients' personal data is not at risk. This is recommended by the Deloitte report. *(Deloitte, "Development of the 'kiosks'", p14)*