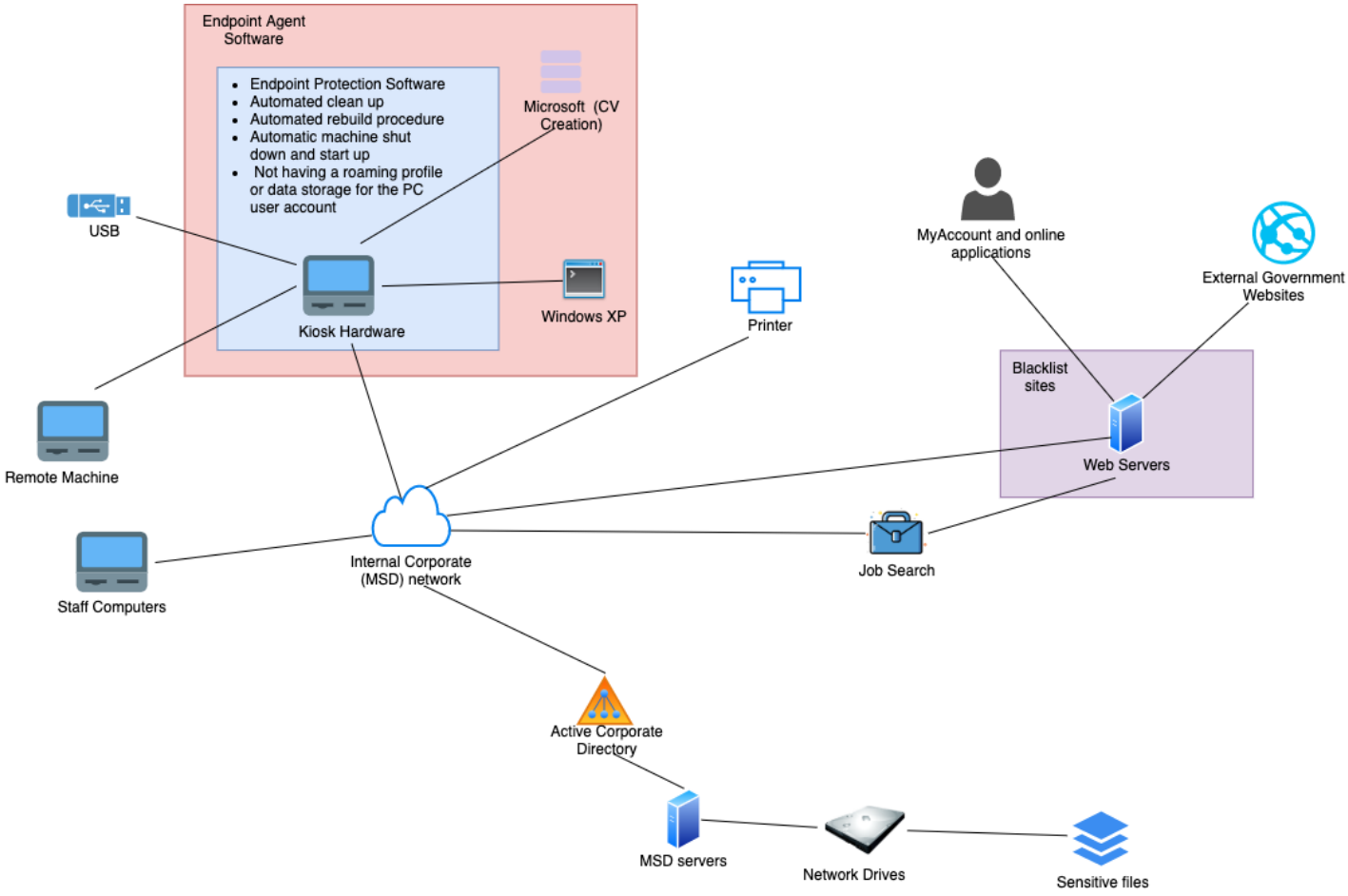
Lavanya Sajwan
300381661
ENGR440 – DIS

DIS - Assignment Two

1. **[5 Marks]**
   The Ministry of Social Development's (MSD), Work and Income Kiosk's network topology.



2. **[10 Marks]**
   Vulnerabilities are exposures that can lead to a threat being realised; a weakness in a system. Shortcomings are a design feature that has been missed which result in a failure to meet a certain standard of security-best-practice. Threats are anyone or anything that can intentionally or unintentionally exploit a vulnerability/shortcoming to manipulate company assets in any way.

Category	Description	Threat
Vulnerability	The kiosk was within the internal corporate MSD network. There was no network separation.	A threat actor would be able to move through the network with minimal security controls → espionage or trespass (Deliberate Threat).
Shortcoming	There was a lack of adequate security monitoring and alerting on the kiosk system.	A threat actor could easily manipulate the kiosk without any outright covert means. → theft and fraud (Deliberate Threat).
Shortcoming	Lack of kiosk logs outside of trends of patterns.	A lack of logging makes malicious activity harder to detect. → espionage or trespass (Deliberate Threat)

Shortcoming	Lack of security patching.	A lack of patching makes the security more vulnerable to evolved threats and easier for malicious bodies to exploit. → software attacks (Deliberate Threat)
Shortcoming	Updates associated with the end point software protection such as anti-virus signature updates were only updated once a week.	A lack of software updates make the security more vulnerable to evolved malware threats and easier for malicious bodies to exploit. → software attacks (Deliberate Threat)
Shortcoming	Insufficient use of routers as this was merged with the wider-organisation update on routers, instead of its own sub-entity.	A threat actor would be able to move through the network with minimal security controls. → espionage or trespass (Deliberate threat)
Shortcoming	Insufficient use of firewalls within the entire network.	A threat actor would be able to move through the network with minimal security controls. → espionage or trespass (Deliberate threat)
Shortcoming	Lack of focussing of security in the design of this product.	Thinking about security as an after-thought meant that some aspects of security would be missing and open to threats. → Missing, Inadequate or incomplete organisational policy or planning (Accidental Threat)
Vulnerability	Whitelist websites would have been more efficient rather than the use of a blacklist as it gave a free reign.	Blacklisting a few websites meant that a threat actor could have accessed a potentially "dangerous" site which could have issues and only afterwards is it classed a problem and blacklisted. A whitelist would have worked better for an open tool as only approved websites could be used. → Missing, inadequate or incomplete controls (Deliberate/Accidental Threat)
Vulnerability	USB's allowed to be plugged into the internal network by an external party.	USB's can have many different types of malware which paired with the lack of end-point security updates, this could have proved to be extremely dangerous oversight as malware could have infected the corporate network. Data is able to uploaded and downloaded as well which is potentially sensitive. → missing, inadequate or incomplete controls (Deliberate/Accidental Threat)
Vulnerability	Kiosks access to the active directory.	Active Directory is often used by persons with broader privileges on a network. By having the kiosks access the active directory this made it so that potential threat actors could manipulate the privilege user rights. → Missing, inadequate or incomplete organisational policy or planning (Accidental threat)
Shortcoming	Clients had no code of conduct to follow when using the kiosk services.	This meant there was no professional conduct in how to use the services appropriately which allowed for less of an incentive for threat actors to respect the tools provided. →

		missing, inadequate or incomplete controls (Deliberate/Accidental threat)
Shortcoming	Clients are able to use kiosk services for an unlimited amount of time between the set operation hours.	The lack of a time limit meant that threat actors could use the services for an unspecified amount of time to copy the sensitive information. → Missing, inadequate or incomplete controls (Deliberate/Accidental Threat)
Vulnerability	Kiosk located in front-of-house without appropriate physical security controls.	The lack of security guards near the devices or CCTV meant that anyone could walk in and use the services despite being illegitimate users. → Missing, inadequate or incomplete controls (Deliberate/Accidental Threat)
Shortcoming	Any penetration testing was not undergone.	This meant that vulnerabilities were not found and fixed, consequently making it open to threat actors brute forcing the system. → Technological Obsolescence (Deliberate/Accidental Threat)

3. **[10 Marks]**

An Incidence Response (IR) strategy is a plan used by organisations to plan their response capabilities to security breaches (NIST 61). Containment strategy and Disaster Recovery (DR) are part of the Containment Eradication and Recovery strategy stage in the IR lifecycle (NIST 61). The containment strategy is the tasks taken after an incident in order to mitigate propagating negative effects. This strategy changes based on the severity of a breach. In DR, the organisation aims to return to "normal operations" and "remediate vulnerabilities to prevent similar incidents". Incident handlers are those who manage the containment and recovery.

Category	Description	Incident Handlers
Containment Strategy	Interviewed Mr Ng and Mr Bailey to gain a deeper understanding of the situation.	Ministry of Social Development, Deloitte
Containment Strategy	Obtained USB analysis to see what was taken and if anything was removed.	Office of the Privacy Commissioner, Ministry of Social Development
Containment Strategy	Obtained image of USB device.	Ministry of Social Development
Containment Strategy	Reviewed files on USB forensically to understand what types of data were accessed and to identify what internal network servers had been accessed. From this the files were divided into groups; invoices, files from a file store, recorded phone calls, a report on the load balancing email system and screenshots showing Ministry and client information.	Office of the Privacy Commissioner, Ministry of Social Development
Containment Strategy	Reviewed network log information to compare with the servers that had been accessed to understand what kiosk PC's had been used in the breach.	Ministry of Social Development

Containment Strategy	Kiosk service was shut-down. This removed a major point-of entry for malignant threats.	Ministry of Social Development (Work and Income)
Disaster Recovery	Mr Ng signed a statutory declaration confirming he had removed all information. Mr Bailey gave verbal confirmation, but refused to sign any legal documents.	Ministry of Social Development, lawyers
Containment Strategy	War-room commenced in order to effectively mitigate the effects of the breach.	Ministry of Social Development
Disaster Recovery	Worked with clients to try and mitigate any harm that it might have caused them. This was done with stakeholders as well.	Ministry of Social Development, Minister, Government Chief Digital Officer (GCIO), Office of the Privacy Commissioner, State Services Commission
Disaster Recovery	Initiated technical implementation measures to respond to the vulnerability and breach. This was done to research more ways of working.	Ministry of Social Development
Containment Strategy/Disaster Recovery	Identified all other network shares by the use of automated and manual testing. When one was found, it was removed if it was unnecessary to the BAU (business as usual) of the organisation. If one found was necessary, then stricter user controls were added. This overall reduced the data on the Ministry's corporate network.	Ministry of Social Development
Containment Strategy/Disaster Recovery	Restricted access to the servers that were breached and identified by Mr Ng.	Ministry of Social Development
Disaster Recovery	Established a service process to give clients the same functionalities that the Kiosk provided.	Ministry of Social Development (Work and Income)
Containment Strategy	Identified privacy impacts and potential legal ramifications associated with the types of data exposed which included, personal details and health information.	Ministry of Social Development, Minister, Lawyers
Disaster Recovery	Obtained an independent third-party overview of the security breach situation.	Deloitte, Ministry of Social Development, Minister
Containment Strategy	Initial incident information gathering by a phone call with Mr Ng.	Ministry of Social Development

4. **[10 Marks]**

Category	Identification
Shortcoming	No defined incidence response plan was set in place. This meant that there was no preparation for the possibility of any security incident.
Vulnerability	Only obtaining verbal affirmation from Mr Bailey instead of legal at the time that this report was published. This is because he declined to sign the statement.
Vulnerability	Initially only secured the servers that Mr Ng said he accessed. The rest of the securing was done as an afterthought.

5. **[30 Marks]**
   a. **Deterrent and Preventive controls**
      i. According to the guideline provided in NIST SP.800-53r5, video surveillance (NIST SP.800-53r5 Section 3.13 control number PE-6) defines the necessity to monitor physical access. However, while it is stated that video surveillance is not necessary, on-premise this would have acted as a deterrence as individuals are less likely to commit illegal acts when under watch.
      ii. According to the guidelines provided in NIST SP.800-53r5, remote access – protection of confidentiality and integrity using encryption (NIST SP.800-53r5 Section 3.1 control number AC-17) explains the necessity to use encryption to protect data during remote sessions like the remote login process exhibited by the Kiosk system. This is also instructed in the NZISM section 17.1, cryptography functions, as they outline that "Encryption of data at rest can be used to reduce the physical protection of storage and handling requirements of the media or systems." With encrypted sessions and rest data, Mr Ng and Mr Bailey would have found it more challenging to access the sensitive files on the network.
      iii. A two-factor authentication system should have been used to authenticate the kiosk user. This could have been paired with community services cards as in 2011, mobile devices were still more seen as a privilege rather than a necessity. Making community services cards, the second factor of authentication would have also ensured that users were clients of Work and Income (unless they shared their details). This would have significantly minimised the range of users and consequently minimise the risk of brute force and dictionary attacks.
      iv. The use of security guards a deterrence as they are a physical reminder of authority and protection of assets [1].
      v. Including a time limit on services would mean that the risk of malignant attackers exploiting services lessen as there is not enough time to manipulate a system. This restriction is defined in NIST SP.800-53r5, session termination (NIST SP.800-53r5 Section 3.1 control number AC-12) as a way of controlling sessions.
      vi. A code of conduct should have been shown to users when logging into the Kiosks to provide them with a user policy that they have to follow. This outlines ethics that they have to follow and also provides them with unappealing implications of their activities [2]. This is classified as MUST in the NZISM-V.3.2-2018 report in Section 14.3 – Web

Applications where “Agencies MUST develop and implement a policy governing appropriate Web usage” (14.3.5. Web usage policy).

vii. According to the guideline provided in NIST SP.800-53r5, restrictions on external system connections (NIST SP.800-53r5 Section 3.4 control number CA-3), when a connection to external systems like external web servers is defined in the topology, a “deny-all, permit-by exception policy” should have been in place. This is a whitelist system. This protects against accessing threat websites that are unknown to a blacklist like the one used by MSD and defined in the Deloitte report. This is also defined in NZISM-V.3.2-2018 report in Section 14.3 – Web Applications where “Agencies SHOULD implement whitelisting for all HTTP traffic being communicated through their gateways” (14.3.10. Whitelisting / Blacklisting websites). This acts as a preventative control as potentially malicious sites cannot be accessed.

viii. Banners reminding users that they are under surveillance act as a deterrence as individuals are less likely to commit illegal acts when they are under watch.

ix. According to the guideline provided in NIST SP.800-53r5, restrictions on external system connections (NIST SP.800-53r5 Section 3.4 control number CA-3), unclassed national system connections (NIST SP.800-53r5 Section 3.4 control number CA-3) the direct connection of an internal network should have been protected by the use of firewalls. Firewalls mediate connections and control information flow; consequently, preventing any inward malicious activity. NZISM-V.3.2-2018 also outlines the use of firewalls in Section 19.3 – Firewalls where “All gateways MUST contain a firewall in both physical and virtual environments.” (19.3.8. Firewall assurance levels). This is also suggested in the conclusion of the independent review conducted by Deloitte.

x. According to the guideline provided in NIST SP.800-53r5, restrictions on external system connections (NIST SP.800-53r5 Section 3.4 control number CA-3), unclassed national system connections (NIST SP.800-53r5 Section 3.4 control number CA-3) the direct connection of an internal network should have been protected by the use of routers. This prevents any unwanted traffic.

xi. The NZISM-V.3.2-2018 report in Section 20.3 – Content Filtering, define that “Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines” (20.3.10. Antivirus scans). These are preventative measures as they can remove malware that can harm a system. These should have been up-to-date, unlike the dated-antivirus that the MSD was using.

xii. According to the NZISM-V.3.2-2018 report in Section 12.4 – Product Patching and Updating, there is the utmost importance that agencies keep up-to-date with trends and update any vulnerabilities and security patches. This prevents any risks due to technological obsolesce. The 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” (12.4.3. Vulnerabilities and patch availability awareness). This was not done at MSD, as explained in the Deloitte report.

xiii. Stricter access control should have been in place in the network. This should have been implemented on all necessary internal servers and networks shares. In the NZISM-V.3.2-2018 report in Section 16 – Access Control, “identification and authentication requirements are implemented in order to provide a secure means of access to information and systems.” This is based on the need-to-know principle, which reduces the risk of many individuals gaining access to highly confidential information.

b. Detective Controls

i. According to the guideline provided in NIST SP.800-53r5, video surveillance (NIST SP.800-53r5 Section 3.13 control number PE-6) defines the necessity to monitor physical access. However, while it is stated that video surveillance is not necessary,

on-premise this would act as proof to any wrongdoing and exploitation of Kiosk services by Mr Ng and Mr Bailey.

ii. A two-factor authentication system should have been used to authenticate the kiosk user. This could have been paired with community services cards as in 2011, mobile devices were more seen as a privilege rather than a necessity. Making community services cards, the second factor of authentication would have also ensured that users were clients of Work and Income (unless they shared their details). This would mean that when alerted of a security incident, the agency could have easily located the person(s) involved with their client information available as provided by the community services card.

iii. As stated in the NZISM-V.3.2-2018 report, accountable material includes regular auditing. In section 4.4 – Accreditation Framework, "Agencies SHOULD ensure information security monitoring, logging and auditing are conducted on all accredited systems" (4.4.4. Accreditation framework).

iv. According to NIST SP.800-53r5, system-wide and time-correlated audit trail (NIST SP.800-53r5 Section 3.3 control number AU-12) can provide a timestamp which can provide a time ordering of records within an audit and analysis to find discrepancies in events of an incident.

v. The NZISM-V.3.2-2018 report, Section 20.3 – Content Filtering, defines that "Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines" (20.3.10. Antivirus scans). This can be a detective tool as it provides a record of when malware-infected or tried to infect a system.

vi. The NZISM-V.3.2-2018 report in Section 7.1 - Detecting Information Security Incidents, defines that Log Analysis MUST be a potential detective tool used by agencies to find any potential security threats. This could be adopted by MSD as it "Involves collecting and analysing event logs using pattern recognition to detect anomalous activities."

vii. In the NZISM-V.3.2-2018 report in Section 16 – Access Control, "Agencies SHOULD implement fraud detection monitoring to identify suspicious activity and provide alerting so that remedial action can be taken." This should have been implemented by MSD as a detective tool to find any suspicious activity. In NIST SP.800-53r5, it is again mentioned that alerting monitoring tools should be used to announce that anomaly behaviour has occurred (NIST SP.800-53r5 Section 3.20 control number SI-15).

viii. NZISM-V.3.2-2018 states that "Agencies SHOULD install host-based IDS/IPS's on authentication, DNS, email, Web and other high-value servers" in Section 18 – Network Security. This should have been implemented by MSD assist in the detection of anomalous activity as it is a behaviour based detective control. This is also supported in NIST SP.800-53r5 (NIST SP.800-53r5 Section 18.1 control number SC-7).

ix. Network-based IDS/IPS detection tools should have been used by MSD to find any real-time anomalies in the network. This is stated in the NIST SP.800-53r5 report, and it is shown that agencies should employ automated tools and mechanisms to support real-time analysis (NIST SP.800-53r5 Section 18.1 control number SC-7). In NZISM-V.3.2-2018, Section 18 – Network Security it states that, "Agencies SHOULD develop, implement and maintain an intrusion detection strategy". A part of the strategy is the use of network-based IDS/IPS's.

c. Responsive and Corrective Controls

i. An incidence Response Plan should have been comprehensively formulated in order to have set plans on what to do in case of an incident. MSD did not have one that they stringently followed as when Mr Ng and Bailey contacted them initially – they disregarded information of any breach. As stated in NZISM-V.3.2-2018, "Agencies MUST develop an Incident Response Plan and supporting procedures" and "Agency personnel MUST be trained in and periodically exercise the Incident Response Plan".

NIST SP.800-53r5 also outlines a subsection on the importance and actions that an organisation must follow in regards to their incidence response (NIST SP.800-53R5 Section 5.1 control number 5.1.12).

ii. A Disaster Recovery Plan should be planned for and implemented in an organisation. In MSD's place, they had set steps which they followed well like their internal analysis and also reaching out to an independent third-party. However, they did not have an appropriate backup service similar to what the kiosks provided so after the incident, a lot of time was spent planning an alternative. With a robust disaster recovery plan, this would have been mitigated. This is outlined in NZISM-V.3.2-2018, in Section 6.4 and it states that developing this plan will reduce the time spent between the disaster and going back to normal business as usual. It recommends that "Agencies SHOULD develop and document a disaster recovery plan." NIST SP.800-53r5 also supports this as they emphasise the importance of a contingency plan; "Contingency planning for systems is part of an overall organizational program for achieving continuity of operations for mission/business functions." (NIST SP.800-53R5 Section 3.1 control number CP-2).

iii. NZISM-V.3.2-2018, in Section 6.4 outlines that organisations should develop a business continuity plan. This is so that critical systems and data functions can be maintained and used when operating with constraint. In MSD's case, this constraint was that when the vulnerable servers were identified, they restricted and network shares were removed or more access controls were added. However, when this was occurring, nothing should have changed in terms of ways-of-working for their internal staff. NIST SP.800-53r5 also references this by stating "Plan for the continuance of essential missions and business functions with little or no loss of operational continuity and sustains that continuity until full system restoration at primary processing and/or storage sites" (NIST SP.800-53R5 Section 3.1 control number CP-2).

iv. Organisations should perform file "sanitation" as a way to remediate any insecure files and content. NZISM-V.3.2-2018, states this in Section 20.4; "Agencies SHOULD perform antivirus scans on all content using up-to-date engines and signatures, using multiple different scanning engines."

v. Throughout the kiosk project planning, delivery and updates, security was neglected. MSD would have been benefitted if they involved the security team throughout this process; a Devops style of management [1].

Works Cited

[1] Champion National Security, "WHY ARE SECURITY GUARDS NEEDED?," [Online]. Available: https://www.champ.net/security-services/security-guard-needed/#:~:text=The%20Importance%20of%20a%20Security%20Guard&text=Security%20guards%20provide%20a%20visible,professional%20protection%20for%20your%20assets.&text=These%20areas%20can%20be%20targets,the. [Accessed 30 September 2020].

[2] WeLiveSecurity, "Cybercrime deterrence: 6 important steps," ESET, 20 January 2015. [Online]. Available: https://www.welivesecurity.com/2015/01/20/cybercrime-deterrence-6-important-steps/. [Accessed 30 September 2020].