CYBR373 Assignment 2 – Analysis of Incident Response Case Study
greenthom – 300536064

All observations and understanding of the Ministry of Social Development Security Breach came from Deloitte of Social Development Independent Review of Information Systems Security. Have not cited information or details written throughout from Review.

Question One

Who

The breach affected the Ministry of Social Development infrastructure of client kiosks located at Work and Income Service Centers across NZ. The kiosk project was overseen by the IT Governance Group, Leadership Team Board, Business and Strategy Teams, Online and Infrastructures Project Business Steering Group, MSD Desktop Upgrade Steering Group, and IT Security Team. These groups, and IT, Finance, Risk Assurance, and other sector representatives, were responsible for addressing security weaknesses leading to the breach and coordinating the response effect. Key decisions were overseen by MSD's Deputy Chief Executives and the Chief Executive.

What

The breach occurred due to poor network separation between kiosks and corporate network, allowing unauthorized access to shared drives and sensitive information. The kiosks, designed for job-seekers, were improperly configured, allowing users to map network drives and access internal systems. Inadequate monitoring, a lack of audit trails, insufficient kiosk access controls, and no alerting/notifications further worsened the issue.

When

The first breach was identified on October 10, 2011, by Ms. Brereton, reporting access vulnerabilities. The most critical breach occurred on October 5, 2012, when Mr. Bailey exploited the vulnerability. Delays in recognizing and responding to the vulnerability identified by both parties to the MSD prolonged the breach.

Where

The breach occurred within MSD's corporate network, specifically due to the kiosks' direct connection to internal systems, exposing sensitive network resources.

Why

The root cause was failure to implement security measures, such as network separation, access control, and risk management. The kiosks were connected to the corporate network as authenticated devices, allowing access to sensitive data without proper restrictions.

How

The lack of separation, with unaddressed security findings from penetration tests, facilitated the breach. The security elements of the project scope were lost during design and deployment processes. The findings in Dimension Data's report identified risks, due to lack of network separation and the ability to access potentially sensitive data on MSD's network. These findings were not appropriately followed up on, addressed, or escalated, enabling the breach to occur.

Question Two

a)

Mr. Ng's actions in revealing the MSD security breach can be seen as both ethical and questionable. He acted in the public interest by informing the Privacy Commissioner and RNZ about a serious vulnerability, bringing attention to an issue requiring urgent remediation, and aligning with transparency principles. He handed over all retrieved data to the Office of the Privacy Commissioner and signed a statutory declaration confirming he had removed the MSD data he obtained. He also discussed with MSD the servers he accessed, how he obtained the data, and how it was handled. However, his public disclosure on his blog before allowing MSD time to address the issue is questionable, as it exposed vulnerabilities to potential malicious actors, possibly leading to further exploitation. Ethical disclosure typically involves giving the affected organization time to resolve the issue before publicizing it, which Mr. Ng did not follow.

The MSD's initial response also raises ethical concerns. After Mr. Bailey reported the vulnerability, MSD misunderstood the issue, assuming it was web-based rather than kiosk-related, resulting in them going down an incorrect path for initial investigations. This delayed their response, allowing further unauthorized access. The lack of urgency and failure to address the breach could be viewed as a failure to ethically protect customer data. Once MSD fully understood the breach, they acted swiftly to disable kiosk services, engage authorities, and secure systems. Despite initial delays, their later actions were more aligned with ethical standards to protect customer data and address the breach.

b)

In New Zealand, responsible disclosure is guided by policies from the New Zealand Internet Task Force (NZITF) and CERT NZ. Key steps include publishing a coordinated disclosure policy on websites, providing clear contact points for reporting vulnerabilities, and secure communication methods like PGP[4]. Vulnerability reports should be acknowledged within two days, with regular updates every 7 days[4]. Organizations should commit to not taking legal action against finders who follow guidelines and cause no harm[4]. After resolving the vulnerability, organizations should collaborate with the finder to publish an advisory or notify affected parties[4]. It is crucial to check if the vulnerability has been exploited and ensure it is fully resolved before publicizing it[4].

MSD's information disclosure policy[3], written in alignment with NZITF guidelines[4], follows these best practices but could be improved. While MSD commits to confirming reports within seven days[3], best practice suggests a prompt initial response, ideally within two days[4]. Additionally, MSD could enhance trust by providing more frequent updates during the resolution process[4]. Finally, MSD excludes vulnerabilities involving third-party services and recommends CERT NZ[3]. However, it would be helpful for MSD to clarify how they coordinate with other government agencies when vulnerabilities affect broader systems.

Question Three

a) Containment Strategy

The containment strategy for MSD involved key actions initiated once the breach's severity was identified. They interviewed Mr. Ng and Mr. Bailey to understand how they accessed sensitive data and forensically analyzed USB device used. Together with the Privacy Commissioner, they reviewed the contents of the USB device to determine what information was accessed, and how individuals may be affected. Network logs were analyzed to trace viewed data to specific kiosks and servers; with this, 10 persons were uncovered who had high levels of risk. MSD isolated the kiosks from the corporate network and granted access only to highly necessary network shares, thereby reducing the residual risk. Delays in initiating these actions assumed web vulnerability, allowed data exposure.

b) Incident Response

Once the breach was escalated, the response from MSD was comprehensive. They established a "war room" to coordinate actions including, disablement of kiosks, communication with Privacy Commissioner, and engagement of external experts. MSD was focused on assessing the extent of potential harm to clients, having its legal team review files to determine how serious the breach was. MSD highlighted privacy law, more specifically Principle 5 of the Privacy Act, to ensure appropriate follow-up action was taken and individuals concerned were treated accordingly.

c) Disaster Recovery

MSD took immediate steps in both short-term and long-term remediation. Concerning first steps, MSD disconnected the kiosks and allowed access only to network shares to minimize risk of further unauthorized access. Then they implemented a cyclic scanning and remediation process to identify and fix vulnerabilities at different places in their network; due to this, they had to shut down or restrict access to 40 network shares. The above-mentioned technical measures were key to eliminating any scope of future breaches from kiosks. The longer-term focus of MSD was restoration of service capabilities for Work and Income clients to compensate for the loss of kiosk functionality. They also commissioned a review of lessons learned about the incident and an immediate independent review to realize root causes and make sure that similar breaches could be avoided.

Question Four

Control	Detail	Chapter & Topic	Summarized Objective
1.Least Privilege Access	Limits kiosk users' access to MSD's corporate network, ensuring they only access the minimum necessary information.	16.Access Control and Passwords 16.4.Privileged Access Management	16.4.21. Enforcing least privilege reduces the attack surface, improves audit visibility and compliance, and lowers risk, complexity, and costs for agencies. 16.4.31.R.02. Implementing least privilege requires limiting the number of privileged accounts and reducing user access to them.
2.Log Monitoring	Logs high-privilege user activities, such as kiosk users, to detect unauthorized network access.	16. Access Control and Passwords 16.6. Event Logging and Auditing	16.6.8.R.01. Event logging boosts security by increasing user accountability. 16.6.8.R.02. Event logging Improves detection of malicious behavior. 16.6.8.R.03. Well-configured event logging enables easier and more effective auditing and forensic analysis during security incidents.
3.Intrusion Detection and Prevention	Uses IDS/IPS to detect and respond to network threats	18.Network Security 18.4.Intrusion Detection and Prevention	18.4.7.R.01. A properly configured, updated IDS/IPS with the right processes effectively identifies, responds to, and contains known attack types, profiles, and suspicious network activities. 18.4.7.C.02. Agencies should develop, implement, and maintain an intrusion detection strategy that includes auditing event logs, including IDS/IPS logs. 18.4.9.C.01.Agencies must select IDS/IPS that monitor uncharacteristic and suspicious activities. 18.4.8.C.02.Agencies should deploy IDS/IPS at all gateways between the agency's networks and any network not managed by the agency.

4.Network Separation and Segmentation	Implements logical separation between public kiosks and sensitive internal networks to limit user access to confidential information.	10.Infrastructure 10.8.Network Design, Architecture and IP Address Management	10.8.6. Separation and segregation are based on system function and data sensitivity, such as placing internet-facing systems in a DMZ, isolated from sensitive systems. 10.8.7. Separation and segregation limit an intruder's ability to exploit vulnerabilities and elevate privileges to access more sensitive internal systems. 10.8.8. Network segmentation effectively protects key data assets and prevents the lateral movement of faults, threats, and malicious activity.
5.Network Access Control	Manages access to MSD's network by enforcing strict policies, authentication, and encryption to prevent unauthorized access.	18.Network Security 18.1.Network Management	18.1.13.R.01. Limiting an attacker's opportunities to connect to a network reduces chances of attacking it. Network access controls prevent attackers from traversing the network and stop users from carelessly connecting to networks of different classifications. 18.1.13.R.02.Their use is primarily aimed at the protection they provide against accidental connection to another network.
6.Data Loss Prevention	Monitors, detects, blocks unauthorized access or exfiltration of sensitive data from kiosks to prevent improper downloads or transfers.	22.Enterprise Systems Security 22.1.Cloud Computing	22.1.24.R.03. Data Loss Prevention (DLP) technologies safeguard sensitive information by identifying unauthorized access and exfiltration attempts, taking action to monitor, detect, and block them. For effectiveness, all data states must be monitored.

References

[1] Deloitte, Independent Review of the Ministry of Social Development's Information Systems Security Phase 1, 1-Nov-2012.
[2] Deloitte, Independent Review of the Ministry of Social Development's Information Systems Security Phase 1, 1-Nov-2012.
[3] webcoordinator@msd.govt.nz, "Responsible Disclosure guidelines - Ministry of Social Development," Govt.nz, 2024. https://www.msd.govt.nz/about-msd-and-our-work/tools/responsible-disclosure-guidelines.html
[4] NZITF_Disclosure_Guidelines_2014.pdf, "NZITF_Disclosure_Guidelines_2014.pdf," Google Docs, 2014. https://drive.google.com/file/d/1hbr8XEyn2o18Zfq6xeTrJerCx34bjinz/view (accessed Sep. 17, 2024).
[5] Govt.nz, 2024. https://nzism.gcsb.govt.nz/ism-document

ChatGPT for editing. Got it to shorten analysis/answers done on questions two and three to get below 300- and 400-word count set.