Section 1 – Incident Overview

The date/time of detection was December 11th. Shortly after, service disruptions began.

The date/time of resolution was December 17th. This is when the investigation process and resolution were completed.

The duration of the incident was approximately six days (from December 11th to December 17th).

The incident severity was high, due to the extensive impact on services and the significant breach of data.

The incident classification would be a data breach along with a ransomware attack.

Section 2 – Executive Summary

Donovan, a senior member of MOVR's Operations team, approved a sign-in prompt that was posing as a valid IT request on October 10th, unintentionally giving access to a threat actor. Using Donovan's credentials, the attacker obtained sensitive customer data and on December 11th, started two significant operations: erasing live database records and initiating a phishing campaign that infected more than 150 business PCs with ransomware. Customers and staff alike experienced severe service disruptions as a result of these actions.

For MOVR, the incident had a significant impact. The company's ability to fairly recompense workers and contractors was hampered by the loss of operating data and records, and they were subject to a ransom demand of $1000 per impacted device. Significant reputational harm resulted from the breach and service interruptions that undermined consumer confidence. Operationally, the incident greatly hampered productivity and service delivery by causing an 8-hour service outage and rendering many employee devices unusable.

After a comprehensive investigation, the IT and security professionals at MOVR determined that Donovan's account was the source of the breach and took appropriate action. By resetting the passwords and ending the active sessions, they were able to secure the hacked accounts. Notwithstanding practical difficulties, the business chose to pay the ransom to get back access to the systems infected by the ransomware. Customers and stakeholders were updated and given compensation by MOVR for the inconveniences. In order to stop similar incidents in the future, they also instituted bi-annual security training and engaged a security consulting firm to do a thorough examination.

Section 3 – Incident Timeline

Detection Phase: The first warning or alert was sent when records in the database were removed, resulting in instant service interruptions for MOVR clients. Customer service received reports about this incident, and IT was notified. The operations staff was the victim of a widespread phishing campaign that encouraged them to install ransomware pretended to be a brand-new internal tool. User lockouts and ransom demands resulted from this being carried out via Teams and email. Database deletions caused eight hours' worth of disruptions while different teams tried to figure out what was wrong and fix it. After receiving complaints of ransomware attacks and conducting an investigation into service outages, IT and security professionals found the ransomware. There were then database restoration delays as restoring the database from backups was delayed due to technical issues, leading to a partial loss of records, transactions, and accounts for some users.

In terms of what went wrong, several things were involved. There were no alarms that came on immediately. It appears that improved real-time monitoring and alert mechanisms are required because the security team was not promptly notified of any unsuspected activity or illegal access. The training was inadequate. Because of his recent employment and the company's yearly training regimen, Donovan, the account that was hacked in the breach, had not yet completed the required cybersecurity training. Because of his inexperience, he was more vulnerable to phishing scams. Inadequate authentication procedures were also present. Even though multi-factor authentication (MFA) was implemented, Donovan rarely got MFA prompts because he was typically already signed in to the majority of the items, which diminished the efficacy of this security mechanism. There were misleading phishing tactics as well. The phishing email was crafted to appear as an urgent directive from MOVR's IT department, exploiting a sense of urgency to bypass critical thinking among employees. The investigation process to trace the source of the breach and resolve the issues took an extended period, highlighting the need for more efficient incident response protocols.

Containment Phase: Donovan's email password was changed right away, as his account was used to access the master account. This was one of the key events and actions taken to contain the incident. To stop more illegal access, all sessions for the master account and Donovan's account were deleted. After conducting interviews and looking into the computer resources of every user who had access to the password manager export, it was possible to link the breach to Donovan's account.

Eradication Phase: The goal of the eradication phase was to eliminate the threat from systems that were impacted. The ransomware problem was attempted to be fixed by IT personnel, but the logistics of obtaining remote employee devices caused a delay in the process. In the end, MOVR chose to pay the ransom to regain access to more than 150 business laptops that the ransomware had rendered useless.

Recovery Phase: In the recovery stage, ransomware problems were fixed and unauthorized access was eliminated in order to resume regular operations and services. In order to notify customers, the company posted follow-up messages and declared the restoration of services. Those impacted, such as MOVR couriers and contractors, encountered difficulties getting paid because of interruptions and incomplete trip records.

Section 4 - Root Cause Analysis

Initial Attack Vector: The compromised credentials of Donovan were purchased by the attacker from the dark web, granting them access to the system. A phishing email posing as MOVR IT support was sent to Donovan, a senior operations manager, directing him to approve a sign-in prompt that purported to be an installation prompt for new IT services. Lacking digital literacy and cybersecurity training, Donovan accepted the prompt without checking its validity, giving the attacker access to his account.

Weaknesses and Vulnerabilities: Cybersecurity training was lacking. Since joining the company, Donovan has not been required to undergo cybersecurity training, which leaves him vulnerable to phishing scams. The implementation of multi-factor authentication was insufficient. Despite the presence of MFA, Donovan rarely received prompts because of infrequent logouts, which diminished the efficacy of this security measure. Credentials were stored in an unsecured or invalid manner. Once Donovan's account was compromised, the development team left a password manager export in an unencrypted shared OneDrive folder, giving the attacker access to vital login information. Mismanagement of role-based access control (RBAC) was present. The attack surface was increased because Donovan continued to have access to the software development OneDrive space even after the project was finished.

Human Factors: The use of a phishing prompt was approved. Due to a lack of cybersecurity awareness and training, Donovan accepted the phishing prompt without checking its legitimacy. Insufficient knowledge was available about security. The incident was caused in part by Donovan's low level of digital literacy and the company's lack of emphasis on regular cybersecurity training. Security procedures were met with complacency. After the project was finished, the development team did not remove Donovan's access to the OneDrive account and improperly encrypted sensitive data.

Recommendations: It is crucial to establish regular and required cybersecurity training for all staff members to raise awareness of phishing attacks and other threats in order to improve security and stop similar incidents. Employees should be encouraged to log out when not in use and regular MFA prompts should be enforced as part of improved MFA procedures. Encrypting all sensitive credentials and reducing the amount of shared credentials must be the top priorities for secure credential storage. To guarantee that staff members only have access to resources that

are absolutely necessary and are promptly rescinded when no longer required, strict access controls should be periodically reviewed and updated. Lastly, to find and fix weaknesses in the system and procedures, regular security audits and penetration tests should be carried out.

Section 5 - Lessons Learned

Key Takeaways: The incident has primarily taught us the value of comprehensive and ongoing cybersecurity training for all staff members, the necessity of strict access control procedures, and the crucial role that monitoring and logging play in identifying and addressing security breaches.

Improvements: Through the implementation of mandatory and frequent training sessions, the enforcement of stringent access control policies, frequent security audits, and improved multi-factor authentication (MFA) procedures, the organization will strengthen its cybersecurity posture.

Training and Awareness: New training and awareness programs will be introduced to ensure that all employees are well-versed in identifying and mitigating phishing attacks and other security threats.

Policy and Procedure Updates: The incident will be used to inform future updates to security policies and procedures, which will include stronger protocols for credential storage, access control, and incident response.

Section 6 - Response & Recovery Assessment

Effectiveness of Response: There were a number of advantages and disadvantages to MOVR's incident response procedure. Although the service disruptions were quickly detected and responded to, a number of factors limited the response's overall efficacy. Logistical difficulties impeded the containment, eradication, and recovery efforts, especially when it came to responding promptly to the ransomware attack on multiple remote employee devices. The choice to pay the ransom emphasizes how urgent it is to get operations back up and also shows how unprepared they may have been for this kind of thing.

Timeliness: The IT and security teams were commended for their promptness in identifying ransomware reports and service disruptions during the detection phase. However, technical problems and logistical difficulties—particularly in returning remote employee devices to the office for remediation—caused a delay in the containment and eradication phases. Due to

this delay, there were prolonged service disruptions and user annoyance as the recovery phase was prolonged.

Communication: Results of communication during the incident were not uniform. MOVR managed customer expectations by promptly notifying customers via social media about the service disruptions and by providing frequent updates. But trust may have been damaged by the initial lack of specifics and the postponed announcement of the ransomware attack and breach. Teams worked together to identify and resolve problems, so internal communication was more effective, but there were still some gaps that could have sped up the response.

Resource Allocation: During the incident, resources were allocated in a reactive manner. The overall response was slowed by the lack of preparation and logistical planning for remote device management, even though the IT staff and security teams were quickly mobilized. The hiring of a security consulting firm after the fact shows that more knowledge is needed, but it would have been better if these resources had been available earlier.

Section 7 – Next Steps

Short-term Actions: A number of quick actions need to be taken in order to address the current incident and stop it from happening again. First and foremost, the IT Security Team needs to improve and adjust its password management procedures. This entails implementing encrypted password managers, frequent changes, and stricter password policies. Second, it is imperative that all employee and customer accounts be equipped with Two-Factor Authentication (2FA). The IT Security Team bears the responsibility of ensuring both comprehensive coverage and enforcement. It is also essential for the Operations Team and IT Security Team to conduct a comprehensive evaluation of access controls. To lessen future violations, this review should remove excess/unneeded access and uphold the least privilege principle. Encrypting confidential information is another essential immediate step. Encryption of sensitive data is a must for the IT Security Team and Data Management Team, especially when it comes to shared spaces like OneDrive. Improving phishing awareness and training is also crucial. It is recommended that HR and the IT Security Team promptly hold training sessions aimed at recognizing and addressing social engineering techniques. It is also essential to review and update the incident response plan (IRP). The IT Security Team and the Legal Team are working on this project, which includes protocols for dealing with ransomware attacks and data breaches in particular. Finally, it's essential to conduct frequent penetration tests and security audits. These audits should be carried out by the IT Security Team in order to proactively find vulnerabilities and bolster defenses against potential attacks.

Long-term: A number of long-term tactics should be put into practice in the future to improve cybersecurity resilience. First, a thorough cybersecurity training program should be created by HR and the IT Security Team. Regular, required sessions catered to various employee roles and technical proficiency levels should be part of this program. Second, it's critical to improve threat detection and monitoring capabilities. Real-time detection and reaction to anomalous activity will be made possible by investing in cutting-edge tools and systems that are supervised by the Security Operations Center (SOC) and IT Security Team. Another crucial step is to put Data Loss Prevention (DLP) procedures into place. DLP solutions should be used by the IT Security Team and Data Management Team to monitor and shield confidential information from illegal access and eavesdropping. It's also crucial to improve third-party and vendor risk management. The IT Security Team and Procurement Team are accountable for enforcing strict security regulations and carrying out frequent audits. It is essential to deploy and update endpoint security measures on a regular basis. To defend against malware and ransomware, the IT Security Team should supervise the installation of antivirus and endpoint detection and response software. It is equally important to establish a strong governance framework and security culture. A culture of cybersecurity awareness should be promoted throughout the company by the IT Security Team and executive leadership, and it should be backed by distinct governance and accountability frameworks. Lastly, continuous improvement and adaptation are necessary. The IT Security Team and Risk Management Team should regularly review and update cybersecurity strategies and policies based on emerging threats, industry best practices, and lessons learned from incidents. This adaptive approach ensures ongoing protection against evolving cyber threats.

Section 8 – Reflection

1. Data Classification Analysis:

DATA	CATEGORY	CLASSIFICATION
Location & Location History (IP, etc.)	Customer	Sensitive
Personal Identifiable Information	Customer, Employee	Highly Sensitive / Confidential
Payment Information	Customer	Highly Sensitive / Confidential
Passwords	Customer, Employee	Highly Sensitive / Confidential
Device Data	Customer	Sensitive
Social Security Number, Banking Information	Employee	Highly Sensitive / Confidential
Email Addresses	Customer, Employee	Sensitive

2. It seems that more than one point is the primary source of weakness. These flaws were mostly related to people and processes. Access controls and password management procedures, for example, were not properly updated or enforced. Vulnerability was also a result of staff members' lack of cybersecurity training, particularly recent hires like Donovan. One of Donovan's people-based weaknesses was his lack of awareness and training, which made him vulnerable to phishing attacks.

3. The way MOVR handles data privacy and breach disclosure raises ethical questions. Inadequate cybersecurity training, a delayed and opaque disclosure of the breach, and a decision to pay ransom in secret are among the flaws. The rationale behind sharing data with advertising partners and the effectiveness of security measures in light of the sensitive nature of the data collected are two areas of uncertainty.

4. Although MOVR eventually revealed the breach, their disclosure strategy was not transparent at first. Ethical questions are raised by holding off on confirming the breach for a month and keeping the ransom payment private. In an ideal world, MOVR would have revealed the breach sooner, given more information about its extent, and been open and honest about its response plans.

5. The decision of whether or not to pay the ransom is divisive. In MOVR's instance, the choice to pay was made in order to minimize disruption and swiftly regain access. Paying the ransom does not ensure that the data will be recovered, and it may even encourage more attacks. Personally, I wouldn't consent to a ransom because there is no assurance and it may encourage more attacks in the future if it is successful. There may have been other options like negotiating with cybercriminals or recovering from backups.

6. The scenario exposes MOVR and other big tech companies to a number of cybersecurity risks. One instance is when sensitive employee and customer data is compromised by data breaches, allowing for illegal access and exfiltration. Another is ransomware attacks that result in lost data, interrupted services, and monetary losses. Additionally, insufficient access controls and a deficiency of frequent security audits contribute to insider threats.

7. MOVR should take a proactive stance when it comes to cybersecurity risk, placing a high value on ongoing development and spending money on strong security measures. This entails providing workers with frequent cybersecurity training, strictly enforcing password management and access controls, conducting regular security audits, and being open and honest about data breaches. Proactive action lowers risks, upholds consumer confidence, and guarantees regulatory compliance.