Post-Mortem Analysis Report for Movr Cybersecurity Breach

April 6, 2024

Oyindamola Olayiwola

Incident Overview

Date and time of Detection: The breach was discovered on the 11th of December, but the time was not stated.
Date and time of Resolution: December 17th.
Duration of Incident: Exactly 2 months
Incident Severity: High
Incident Classification: High

Briefly describe what happened during the incident, highlighting key events.

The assailant utilized the obtained credentials to duplicate more than 20 million pieces of customer data, encompassing their personally identifiable information (PII). With these credentials, the attacker also eradicated a live production database record, resulting in service disruptions. Furthermore, they exploited Donovan's compromised credentials to orchestrate a widespread phishing campaign aimed at the operations team, masquerading as emails from Donovan himself. These emails contained a ransomware application, which, upon being clicked, infected over 150 computers.

Explain the impact of the incident on the organization, including financial, reputational, and operational impacts.

The incident, which involved the deletion of the database, had several repercussions: users were unable to book or manage upcoming flights, leading to revenue loss for the company; customers couldn't fulfil planned trips, damaging the company's reputation; payment to service providers was delayed, affecting operations; the loss of customer data eroded trust, potentially driving customers away, further contributing to revenue loss and customer attrition.

High-level actions taken were:

- Identifying the incident when the disruption happened as well as when the ransom was reported.
- Assessing the extent of the breach and systems that were affected.
- Attempt to restore from backup.
- Investigating to determine the cause of the breach and understand how the breach occurred i.e. identifying the attack vector, in this case, an unprotected document that consists of a password to
- Interviewing staff with access to the password manager export.
- Mitigating the risk by changing the password of the senior manager and removing all sessions for both Donovan’s account and his master account
- Addressing affected clients by offering compensation to them.
- Communicating the event of the breach to all necessary stakeholders and the actions that were taken to mitigate the breach.
- The company implement more efficient controls such as enhancing security protocol, updating access controls, and improving the backup and recovery process to prevent similar incidents from happening in the future.

Incident Timeline

Detection Phase

a.)

List of Events and Actions	How it Contributed to the actions
Login attempt	This early intrusion was not detected until two months later after the account was used to cause breach.
Phishing email	The lack of cyber security awareness among employee left them vulnerable to social engineering attacks
Unauthorized data access	There was no proper control in place to detect and prevent privileged escalation.
Deletion of live production database record	This was successful because there was lack of proactive monitoring to identify the breach before the deletion took place
Distribution of ransomware	It increased the attack surface and infected devices were rendered unusable which led to the company incurring additional cost to recover them

b.) In the absence of an initial alert, organizations can adopt proactive measures based on cybersecurity principles like role-based access control (RBAC) and least privilege. This involves granting access permissions according to job roles and limiting access to only what is necessary. For example, once a project is completed, access should be revoked or restricted. By adhering to these principles, organizations can mitigate the risk of unauthorized access and detect anomalies early on. It's possible to miss this from the onset if access permissions are not regularly reviewed and if there is no centralized access management system in place to effectively manage permission.

Containment Phase

The incident was contained through the efforts of the security team, which involved changing the passwords of senior manager Donovan, whose account was used to access sensitive data, deleting live production database records, and retrieving over 150 laptops infected by ransomware to decrease the attack surface, they investigated the source of disruption and identified the ransomware attack.

Eradication Phase

1. Identifying the root cause
2. Changing the password of the compromised account
3. Retrieving Infected Laptops

Recovery Phase

1. Identification of breach
2. Isolation and containment
3. Database restoration
4. Investigation and resolution
5. Ransomware mitigation
6. Communication and disclosure

Root cause Analysis

a.) Before the attack, the perpetrator obtained Donovan’s login credentials through a phishing campaign and sold them on the dark web. They meticulously researched Donovan's background on social media and LinkedIn, noting his previous roles in less digitally focused companies. Donovan's recent move to a larger company and his senior position made him a prime target due to perceived gaps in digital literacy compared to his colleagues. The attacker then attempted to access Donovan’s account using the compromised credentials.

b.) Here are some of the cybersecurity weaknesses and vulnerabilities within the organization's processes or policies that contributed to the incident. These include unclear access control and data governance practices, which leave the company open to various risks. For instance, without clearly defined access control policies, employees may have excessive permissions, leading to unauthorized access to sensitive information. This can result in data breaches, insider threats, or inadvertent data leaks. Similarly, inadequate data governance practices may result in data inconsistencies, inaccuracies, or loss of data integrity, compromising the reliability and trustworthiness of organizational data. Furthermore, unclear data classification and handling procedures can make it challenging for employees to determine the appropriate level of protection required for different types of data, increasing the likelihood of mishandling or exposure to sensitive information. Inadequate documentation of data access and usage can also hinder incident response efforts and forensic investigations in the event of a security breach. Overall, the lack of clarity in access control and data governance practices undermines the organization's ability to effectively manage and protect its data assets, posing significant cybersecurity risks.

c.) The human errors contributing to this incident include the failure of IT security to organize frequent cybersecurity training for both new and existing staff. Such training would have covered topics like phishing attacks, enabling employees like Donovan to recognize suspicious emails and question their legitimacy. Additionally, there was a vulnerability in not regularly authenticating and logging off from accounts when not in use. Donovan's reluctance to seek help due to fear of embarrassment or inconveniencing others also played a role, as it prevented him from verifying the authenticity of the urgent message he received.

d.) Regular cybersecurity training sessions should be provided to ensure that all staff members attend and are adequately prepared to handle security threats. Conduct simulation exercises to test employees' responses to potential cyber-attacks and provide constructive feedback based on the results. Designate a point person to drive the implementation of these initiatives and ensure their effectiveness. Raise awareness about the importance of using multifactor authentication and the necessity of logging off when accounts are not in use. Educate employees on the risks associated with failing to do so, while emphasizing the benefits of these security measures. Enforce the use of multifactor authentication for all company resources to enhance overall security. Create an environment where employees feel confident speaking up when they need clarification or assistance. Foster open communication channels and make employees comfortable discussing their needs, concerns, and questions related to cybersecurity practices.

Lesson Learned

a)

This case study emphasizes the importance of maintaining a robust security awareness program and the need for regular cybersecurity training to empower employees to safeguard against cyber threats. It advocates for swift action in response to breaches and highlights the significance of implementing policies containing a comprehensive incident response plan. Testing the effectiveness of this plan through simulations, including backup testing, is recommended. Additionally, the importance of transparent communication with stakeholders to keep them informed during security incidents is emphasized. Overall, the study stresses the necessity of proactive cybersecurity practices over-reactive approaches to effectively protect against and mitigate the impact of breaches.

b)

General Security Awareness Training
Phishing Simulation Exercises
Data Protection and Privacy Training
Secure Remote Work Training
Incident Response Training
Social Engineering Awareness
Mobile Device Security Training
Role-Based Training

c)

Acceptable use Policy
Data classification Policy
Access control Policy
Password Policy
Remote Access Policy
Incident response plan
Security Awareness train
Encryption Policy
Compliance policy
Employee Responsibilities and Code of Conduct
Backup and Disaster Recovery Policy
Monitoring and Logging policy and conducting Audit activities.

Response and Recovery Assessment

Effectiveness of Response: Evaluate the effectiveness of the incident response process.

The company identified and assessed the nature of the breach, taking immediate action to contain it and mitigate further damage. Once the source of the breach was identified, appropriate solutions were implemented to address vulnerabilities and strengthen security measures. Effective communication with stakeholders was maintained, ensuring transparency and trust throughout the process. Additionally, the company proactively engaged a security company to monitor for any appearance of stolen data records on the dark web, demonstrating a commitment to ongoing vigilance and protection of customer information. Overall, while there were challenges in the initial detection of the breach, the company's response was comprehensive and effective in minimizing the impact and safeguarding against future threats.

Timeliness: Assess the timeliness of detection, containment, eradication, and recovery efforts.

Initially, the breach went unnoticed for two months, attributed to the lack of sophisticated monitoring mechanisms and the attacker's strategy of maintaining discreet access and exfiltrating data in small batches. Once discovered, it took approximately one week to contain the breach, involving identifying the compromised account, revoking access, and investigating the scope of the attack. Eradication efforts also spanned about one week, focusing on removing the attacker's access from the system and addressing vulnerabilities. Despite efforts, the recovery process was only partially successful, with some customer data permanently lost due to database deletion. Additionally, costs were incurred for remediation efforts related to the ransomware attack. Overall, the MOVR breach response was hindered by the slow detection timeframe, allowing the attacker to compromise significant data and escalate disruptions. A prompt response could have potentially minimized the breach's impact.

Communication: Analyze the effectiveness of communication during the incident.

Delayed communication occurred one month after the incident, providing vague details to customers. While demonstrating some transparency, the communication lacked sufficient information about the incident's cause and resolution, leading to customer confusion. This lack of clarity may have portrayed a lack of confidence in the company's response. However, notifying customers promptly once services were restored was commendable, despite the delay.

Resource Allocation: Review the allocation of resources (personnel, tools, etc.) during the incident.

- **People**: The IT and security teams swiftly investigated service disruptions and ransomware reports. Donovan received specialized support and training post-breach. An internal team traced the breach's source and identified vulnerabilities. MOVR hired a security consulting firm to uncover the incident's chain of events. A security company was contracted to monitor data records on the dark web.
- **Technology**: The IT infrastructure was used to review access logs and account activities. Backup tools were used to restore the database, although there were delays due to technical issues. Social media platforms were used to notify customers of disruptions. Dark web monitoring tools were used to detect compromised data records.

- **Training and support Process**: Donovan received customized IT assistance and training to address security risks linked to his account. The company now conducts security training twice a year to boost employee awareness and readiness.

Next Steps

Short-term: List immediate actions to be taken to address the incident and prevent recurrence. With every action, list the team(s) that would be accountable for leading the implementation of this action.

Employee training: IT security Team, HR
Implementation of MFA: IT Administrator
Security and Network Monitoring: IT security Team and IT Administrator
Robust incident response plan and simulation: IT Security Personnel/ CSIRT, System Administrator and IT Manager CISO, Senior Management
Access Review and Restriction: IT security Team and Auditors (Internal and External)
Regular security audit: Auditors (Internal and External)
Dark Web Management: IT security team
Backup and Disaster Recovery Testing: System Administrator and IT Security Team

Long-term: Provide long-term strategies and improvements for enhancing Cybersecurity. For each point, list the team(s) or individual(s) that would be accountable for leading the implementation of this action.

- Implement a security awareness and training program (Security and HR)
- Enforce the principle of least privilege Access Control (Security and IT Team)
- Strengthen Password Management Practice (Security and IT Team)
- Secure Sensitive data by identifying, classifying, and implementing the appropriate control to protect the data in transit and at rest. (Security and IT Team)
- Continuous Monitoring and Vulnerability Management (Security and IT Team)
- Incident Response Plan and testing (Security Team and Senior Management)
- Disclosure Policy (Management and Legal Team).

Reflection

1.

DATA	CATEGORY	CLASSIFICATION
Name (First and Last)	Customer	PII (Personally Identifiable Information)
Profile photo (Optional)	Customer	Sensitive
Phone Number	Customer	PII (Personally Identifiable Information)
Location	Customer	Sensitive
Location History	Customer	Sensitive

Payment information	Customer	Highly Sensitive
Transaction amounts	Customer	Sensitive
Merchant information (if applicable)	Customer	Sensitive
Driver's licenses	Customer	Highly Sensitive
License plates	Customer	Sensitive
History of the types of services requested (e.g. Package Delivery, Food Delivery, Personal Transportation)	Customer	PII (Personally Identifiable Information)
Delivery data	Customer	Sensitive
IP addresses	Customer	Sensitive
Device Data:	Customer	Sensitive
Name	Employee	PII (Personally Identifiable Information)
Address	Employee	PII (Personally Identifiable Information)
Phone number	Employee	PII (Personally Identifiable Information)
Date of birth	Employee	PII (Personally Identifiable Information)
Social security number	Employee	Highly Sensitive
Salary / pay stubs	Employee	Highly Sensitive
Benefits	Employee	Sensitive
Banking information	Employee	Highly Sensitive

Having performed a recap of the case events and identified key issues, what do you believe the main source of weakness was? Is it a single point or multiple points? Were they people-based, process-based, or technology-based?

This Event had multiple sources of weaknesses that included both people-based and process-based.

2. **Provide your analysis and commentary on the ethics presented throughout the case. Were there any shortcomings, ethical issues, or areas of ambiguity?** Movr acknowledges the collection of personally identifiable information (PII) but neglects to adequately safeguard it. Moreover, for a company handling such sensitive data, it is imperative to ensure all staff members are well-informed about security issues and equipped to respond to potential threats effectively, which Movr failed to do. Additionally, resorting to paying a cybercriminal is deemed unethical due to the lack of guarantee for data retrieval and the inadvertent support for future attacks, reflecting a reward for their actions. This raises ethical concerns regarding the company's response to the breach.
3. **Given the unknown extent of the breach, do you think that MOVR's disclosure approach was justified? What could or should have been done differently if anything?** While MOVR's communication with clients was timely, it lacked specificity, potentially causing confusion among clients. They were left uncertain about the extent of the impact and whether individual actions were necessary. Additionally, the communication provided later did little to clarify the situation, leaving clients unsure about the actions taken during the one-month attack period and the measures implemented to address the breach.
4. **Would you have paid the ransom? Why or why not**?

   Yes, given the significant loss of valuable assets and its impact on business operations, it is evident that the company lacks backup data for restoration. Consequently, the inability to access sensitive information, particularly for over 20 million clients, poses challenges for maintaining customer trust and conducting business continuity. Without this crucial data, the business's viability is compromised. Additionally, evaluating the cost of recovering this data prompts the question: Is the expense incurred justifiable?

5. **In Unit 1, we discussed the concept of risk in Cybersecurity. Given what you know about the scenario, what Cybersecurity risks exist for MOVR and other large technology companies?** The risk is Social Engineering Attack

   What do you think MOVR's attitude towards Cybersecurity risk should be? Why should they hold this attitude towards risk?
   The company's attitude toward cybersecure risk should be proactive. Adopting a proactive approach enables organizations to utilize existing resources and knowledge of risks and vulnerabilities to implement safeguards and controls, preparing them for potential events in the future. This approach is cost-effective and demonstrates the organization's exercise of due care and due diligence. By proactively addressing risks, companies can mitigate legal consequences, financial losses, and reputational damage that may arise from incidents. Overall, proactive risk management helps organizations safeguard their assets, maintain compliance with regulations, and preserve their reputation and financial stability.