**Incident report analysis**

|  |  |
| --- | --- |
| **Summary** | This morning, the IT department identified suspicious behavior on the network. Multiple failed login attempts were recorded in a short period of time and prompted an investigation by the incident response team. A network intrusion utilizing a zero-day vulnerability in a commonly used web application framework. The network intrusion resulted in a data breach to the client information database and exfiltration of names, addresses, social security numbers, and financial transaction details. This breach has the potential for financial loss and damage to the company’s reputation. |
| Identify | The incident response team investigated a possible intrusion and identified a network intrusion utilizing a zero-day vulnerability in a commonly used web application framework. The network intrusion resulted in a data breach to the client information database. It appears the attacker exfiltrated names, addresses, social security numbers, and financial transaction details. |
| Protect | The incident response team will patch the zero-day vulnerability, review and reconfigure the firewall, require employee password reset, and introduce multi-factor authentication to the customer database access protocol. |
| Detect | In order to prevent unauthorized access the firm will invest in an Intrusion Detection System (IDS) and utilize a firewall access logging tool to monitor access. |
| Respond | Client information cannot be recovered. Therefore, all affected clients must be made aware of the data breach and their risk exposure. All affected clients will be contacted to ensure client safety. In the future, the incident response team will use the IDS and firewall logging tool to identify unauthorized access prior to the data breach. The incident response team must take steps to ensure data breach does not occur. This may include shutting down the network services until the system is secure. |
| Recover | The team will ensure the accuracy and integrity of the data in relation to the last backup. If any data is missing or altered, the database may need to be reverted to the previous backup. The firm will need to invest in reputation management services in order to restore client confidence. In future incidents, we will notify clients of data breach promptly. |

|  |
| --- |
| Reflections/Notes: |