Scenario: Network Intrusion and Data Breach

You are a cybersecurity analyst working at XYZ Financial Services, a large financial  
institution that offers a wide range of financial products and services, including online  
banking, investment management, and mortgage lending. The company holds sensitive  
financial data for millions of clients, making cybersecurity a top priority.  
One morning, the IT department at XYZ Financial Services detects unusual activity on the  
network. Multiple failed login attempts are recorded on several employee accounts within a  
short period. Suspecting a possible intrusion, the incident response team is activated to  
investigate further.  
Upon further analysis, it is discovered that a sophisticated attacker has gained unauthorized  
access to the network by exploiting a zero-day vulnerability in a commonly used web  
application framework. This vulnerability allowed the attacker to bypass the web application  
firewall and gain access to an internal database server containing sensitive customer data.  
The attacker exfiltrated a significant amount of client information, including names,  
addresses, Social Security numbers, and financial transaction details. It is evident that this is  
a data breach with the potential for severe repercussions, including financial loss and  
damage to the company's reputation.  
The incident management team, in collaboration with the cybersecurity team, is now tasked  
with responding to this breach using the NIST Cybersecurity Framework (CSF) as a guide to  
effectively manage and mitigate the incident. The new guide NIST has developed provides  
practical implementation examples of the CSF.

**Type of Attack:** Network Intrusion and Data Breach

**Impacted Systems:**

1. Compromised Web Application
2. Internal Database Server
3. Employee Accounts (multiple)

**Immediate Action Plan:**

1. Patch the Zero-Day Vulnerability:
   * Work with the software vendor or developers to obtain and apply a patch that addresses the zero-day vulnerability in the web application framework.
2. Enhance Access Controls:
   * Review and strengthen access controls for both the web application and the internal database server.
   * Implement the principle of least privilege to ensure that employees have the minimum level of access required for their roles.
3. Review Firewall Configurations:
   * Conduct a thorough review of firewall configurations to identify and close any unnecessary open ports or services.
   * Consider implementing application-layer filtering to control application-specific traffic.

**Continuous Monitoring Strategies:**

1. Implement Intrusion Detection Systems (IDS):
   * Deploy IDS to monitor network traffic for suspicious patterns, known attack signatures, or anomalies indicating potential unauthorized access.
2. Analyze Access Logs:
   * Regularly analyze access logs for the web application, database server, and network devices to detect unusual login patterns or suspicious activities.

**Response Plan for Future Incidents:**

1. Incident Containment:
   * Develop clear and detailed procedures for containing incidents swiftly to prevent further unauthorized access or data exfiltration.
2. Neutralization Strategies:
   * Define strategies to neutralize threats, including isolating compromised systems, disabling compromised accounts, and implementing network segmentation.
3. Post-Incident Analysis:
   * Establish a thorough post-incident analysis process to identify the root cause, tactics, techniques, and procedures (TTPs) used by the attacker.

**Recovery Steps:**

1. Data Restoration:
   * Prioritize the restoration of critical client data and financial transaction details.
   * Ensure the integrity of restored data through verification processes.
2. Process Restoration:
   * Identify essential processes that were disrupted and develop a plan for their swift restoration.
3. Improvement Assessment:
   * Evaluate the incident response and recovery processes to identify areas for improvement.
   * Incorporate lessons learned into updated incident response plans.