Scenario:

You are the Chief Information Security Officer of the accounting firm, and you have been notified of a potential data breach. You immediately activate the incident response plan and gather the relevant team members, including the head of IT, HR manager, and managing partner to respond to the incident.

Upon further investigation, it is discovered that sensitive client data, including financial information, may have been compromised. The team works quickly to contain the breach and notify affected clients.

However, soon after the breach is discovered, news of the incident breaks out in the media, causing a scandal and damaging the firm's reputation. The managing partner requests the PR team to handle the situation promptly and transparently to mitigate the damage.

Additionally, the potential legal consequences of the breach are also significant, and the managing partner suggests bringing in a legal team to assess and manage the legal implications. The legal team advises the firm on the best course of action to ensure compliance with relevant regulations, such as data protection regulations, and to minimize legal and financial risks.

Step 1: Preparation

* To prepare for any potential attacks, the well known and acclaimed Risk Management tool Logic Manager will be used to analyze, protect and monitor company, user and employee related data and to keep track of potential anomalies while also limiting access to certain data without proper permissions. Norton Antivirus will also be employed as an additional defensive layer. Sophos Firewall will be employed as our firewall.
* Information will be structured on a tier basis, with higher tier information only being available to employees granted access. If the right access level isn’t possessed, the information should not be accessible.
* Regular training sessions and mock breaches will be conducted to help employees identify potential attacks, anomalies in data and also to give them greater understanding of best practices as well as how to utilize company software. If a breach or something suspicious is detected, employees will be taught how to respond as well as their roles in this response.
* The IT team will also be tasked with keeping regular communication with the physical Security teams to ensure that physical systems, servers, premises and individuals are all regularly checked and secured. If anything suspicious is detected, both teams should immediately contact each other and a sweep should be done to ensure safety is maintained.
* A team will be prepared specifically to handle attacks and related procedures following a chain of command with the CISO as the leader:
  + An Operations Team will be developed comprising of select programmers, ethical hackers and framework designers in order to control and mitigate damage as well as manage updates.
  + The IT team in charge of maintenance and managing of devices will be required to make checks on systems as well as working closely with Operations Team to ensure proper updates are made.
  + Technical Analysts will be in charge of detecting and relaying information about attacks
  + Media team will be tasked with controlling how potential information about any attacks is presented to the public.
  + The HR Manager as well as his selected HR team will be in charge of scheduling training sessions as well as working closely with the IT and Operations’ teams to communicate updates about systems and potential attacks that affect the functionality of the business to the employees where necessary.
  + Database Administrators will be in charge of managing the database, ensuring safety of the information and providing any relevant updates or leading any defensive measures that need to be taken.
  + A team of legal counselors is also required in order to stay ahead of potential legal matters that may arise as well as what measures we’ll be allowed to take in regards to the type of attack suffered and what data it targets.
  + Outsourced consultants and experts will also be required in order to provide additional assistance in detection of any potential follow up attacks or high level attacks using the current breach as a decoy.
  + The board will also need to stay in regular contact to ensure required budgets are met as well as giving approval of the measures that need to be taken.

Step 2: Identification

The IT team identifies that the attacker has bypassed the firewall. They also identify that the attacker has been active within the network for the past week, and has exfiltrated sensitive client data.

Step 3: Containment

The operations team isolates the affected systems and disables network access to limit the attacker's ability to spread the attack. They also shut down the firewall to prevent further access by the attacker.

Step 4: Investigation

The operations team and technical analysts conduct a forensic analysis of the systems to determine the extent of the damage and the source of the attack. They identify that the attacker used a vulnerability in the firewall to gain access to the network and that the attack originated from a foreign IP address. They also review the firewall configuration and identify areas where it was not properly configured or updated.

Step 5: Remediation

Based on the results of the investigation, the security team (Operations, IT, TAs and cyber security experts) takes steps to remediate the damage caused by the attack. They update the firewall to the latest version, configure it with appropriate security policies, and implement intrusion detection and prevention software to monitor for any further attacks.

Step 6: Recovery

Once the remediation steps have been taken, the security team works to restore the affected systems and data. They restore data from backups, reconfigure systems, and install new security controls to prevent similar attacks in the future.

Step 7: Post-Incident Analysis

After the incident has been fully resolved, the security team conducts a post-incident analysis to identify any areas for improvement in the incident response plan, security controls, or other aspects of the organization's security posture. They review the incident response plan and update it as necessary.

Step 8: Reporting and Communication

Throughout the incident response process, the security team keeps stakeholders informed of the incident's status and the actions being taken to address it. The media team is fully briefed on the relevant details and a campaign is created to address the media scandal as well as to alleviate potential worries related to the attack following the recovery. The legal team analyzes the facts related to the breach and compiles a legal opinion. Should any cases or issues arise related to the breach onward, the team is ready to adopt a pre-prepared defense. After the incident has been fully resolved, a final report is generated and shared with relevant stakeholders to ensure that all parties are aware of the incident and its resolution.