Task 1

**## A. Success of the Attack**

1. Vulnerability 1 -

- Specific Example: Incorrectly configured email security

- Exploited / Attack Success: John from Azumer was phished by watersupp1y.int, The phish was successful due to lack of email security including SPF, DMARC, and DKIM. The Azumer email domain could be easily spoofed. In this situation however, spoofing the email domain was not necessary, due to a lack of warnings, flags, and security scanning by a correctly configured email security client or spam filters the attackers were able to redirect John to a credential harvesting site, giving them domain credentials.

2. Vulnerability 2

- Specific Example: Database security controls

- Exploited / Attack Success: On Monday's return to the office John proceeded to his desk and was unable to locate the volunteer database. The case study does not specify whether the database was digitally missing or physically missing. In this disussion we will speak to digitially missing. The exploit here is quite likely the pivot from email compromise to data theft. The same credentials from the phishing attack were likely used to attempt logging into the database at Johns desk. Upon successful login attempt the database was likely exfiltrated by the hacktavists.

**## B. CIA and PII**

Explain how the confidentiality integrity, and availability of Azumers operations and PII data have been compromised, using NIST, ISO 27002, or another industry standard framework to support your claims

- Explain how each was compromised

- When the Azumer database was compromised by the hacktivist, operational and PII data held Azumer was breached, this immediately negated the confidentiality of the both Operational and PII data. ISO IEC 27002, section 10.5 "Back-up", provides governance for Data Back-up. These measures are designed to address integrity and availability of information processing facilities. Upon breach of the Azumer database PII such as basic contact information, last 4 digits of social security numbers, and basic contact information, was immediately compromised. Further reaching the hacktivist deleted the Azumer database, thus preventing any restoration from back-up. This significantly impacts the availability. Lastly we compound the issue with there not being a physical copy of the database, while some Azumer employees may have copys taken at various stages, they do not guarantee a full replacement of the database, removing the integrity from Azumer.

**## C. Federal Regulation**

Task Requirement: Identify a federal regulation this NGO violated, providing a specific example from the case study as evidence of Azumer Water's noncompliance

Azumer violated the "Federal Privacy Act", when the data base for Azumer was breached PII was compromised. This is a direct violation of the Federal Privacy Act. As per the case study for Azumer, the mention of the database housing PII such as:

- basic contact information

- background checks

- last 4 digits of social security number for identity verification

**## D. Immediate Steps**

1. Recommendation 1

- The remedation steps I would take would be, change the passwords to John's accounts, making sure to change the password to his email/domain account.

2. Recommendation 2

- The second remediation step to take would be to isolate the database server to preserve any potential evidence and prevent further compromise. I would do this by taking the database server offline, still powered on, this will allow for full forensic capture and prevent further damage.

**## E. Incident Response Plan**

Task Requirement: Explain how having an incident response plan in place will benefit Azumer Water, using details from the case study to support your explanation.

- Tie in two or more elements of an incident response plan:

1. Mission

2. Strategies and goals

3. Senior Management approvals

4. Organizational approach to incident response

- Incident handling approach/incident reponse lifecycle

5. How the incident response team will communicate with the rest of the organization and with other organizations

6. Metrics for measuring the incident response capability and its effectiveness

7. Roadmap for maturing the incident response capability

8. How the program fits into the overall organization

1. Benefit 1:

- The first benefit of an incident response plan that I would chose is Communication, the need for secure immediate communications during an security incident is vital. This quickly hels to ensure no further information is being leaked, or that the communications being sent internally are not being monitored. A third party application for communications such as Signal, provides end-to-end encryption, quick access to AzumerWater employees that may be needed for incident response. This will help drive the containment and eradication phase as well. This would have been useful for initial investigation upon John's discovery of the missing database.

2. Benefit 2:

- Here I would recommend the NIST SP 800-61r Incident Response Life-Cycle this helps drive the overal response and provides a clear phased approach to incident response. Overall guidance to use during the breach. In the instance of the case study, had this been in place, those involved would have a known plan of action, individual steps to take, and assigned tasks to reduce confusion and hesitation.

**## F. Processes**

Task Requirements: Discuss two processes to increase information asssurance levels within the organization and bring Azumer Water into compliance with the violated federal regulation identified in part C

1. The first corrective action I would implement is an access control list of the database that restricts the access to Azumer IP addressing. While this could prove to be difficult for Azumer employees to access the database from an external IP address, it would limit the potential blast radius of a breach and prevent unwanted access to the database.

2. The second corrective measure I would implement would be to ensure that any PII stored on the database has been salted and hashed, identifiable numbers stored in a separate table from the last four digits of the social security number.

**## G. Technical Solutions**

Task Requirements: Recommend technical solutions to counter the remaining effects of the attack in the case study and to prevent future attacks

- Understand what contitutes "technical" vs "administrative"

- Address remaining effects (i.e two other effects you have not previously addressed in other sections of the task)

1. Technical Solutions #1: List a specific technical solution here:

- Access Control Lists (ACL), an ACL configured to only allow specific IP addresses or MAC addressing access to the AzumerWater database.

2. Technical Solutions #2: List a specific technical solution here:

- Anti-Virus software, active scanning of websites and applications.

**## H. Organization Structure**

Task Requirements: Recommend an organizational structure for IT and security management, including a logical delineation of roles and adequate coverage of responsibilities, to support the efficient discovery and mitigation of future incidents.

- Key Function: Maria Rodriguez. As an IT Manager, Maria's role would be to ensure all aspects of IT are covered, this includes working to ensure the contracts for Pruhart Tech include real-time security monitoring. This is the head of IT, all other actions roll up to this point.

- Coverage: IT Management

- Key Function: Pruhart Tech. Security Operations Center, the responsible party for ensuring devices are properly configured and maintained. This partner will report directly up the chain to Maria Rodriquez.

- Coverage: Security Management

- Key Function: Matt Lorenzen Cyber Security Analyst and Incident Response, reponsible for building monitoring and detection methods based on real-time logging. This role reports up to Maria Rodriguez as well.

- Coverage: Efficient Discovery and Mitigation of Incidents

**## I. Risk Management**

Task Requirements: Describe your risk management approach for Azumer Water based on the likelihood, severity, and impact of the risks in the case study.

- Risk selection

- Risk categorization

- Risk management approach formulation

1. Risk #1: The first risk I see here is the Wireless Access Point is configured to use WEP as an authentication mode. WEP is easily cracked, this will allow anyone to compromise the wireless network and access internal AzumerWater data. I believe the risk exists as AzumerWater does not have a dedicated team to manage in-house configuration of network equipment.

- Likelihood: Medium

- Severity: High

- Impact: High

2. Risk #2: AzumerWater Database redundancy. This risk exists at AzumerWater because the database is currently being hosted on a system under John's desk. This puts the database at risk of corruption, theft, or in this case, deletion by a malicious actor.

- Likelihood: High

- Severity: High

- Impact: Critical

Provide your risk management approach here. Be sure to discuss how categorization in terms of likelihood, severity and impact are considered. Discuss how the approach would help the company address future risks.

I would use the Risk Management Framework (RMF) provided by NIST 800-37. This framework covers the entire Risk Management life-cycle. The RMF uses the below steps:

1. Prepare: This is done via asset management and understand of the potential attack surface, likely attack vectors, and anticipated threat actor type.

2. Categorize: Using a low, medium, high, critical categorization reduces the need for forumulary work to apply a score or rating. This reduces the overhead and time for Risk Categorization.

3. Select: Selecting your highest impacting Risk as your priority for risk mitigation

4. Implement: Making the configuration changes or adding security measures, this is where the changes are made.

5. Assess: Review your work, during this phase we are checking to make sure the correct changes were made and configured correctly.

6. Authorize: Provide the authority to those needed to make changes to ensure they are able to protect the organization.

7. Monitor: Continuous monitoring to ensure new measures aren't needed, or detect anomolies as needed.

Using this process would significantly increase the security posture of AzumerWater because they would be able to mitigate risks faster and more accurately. This would also allow for communication back to Pruhart Tech to ensure they have the information needed to make the appropriate firewall configurations.