# KOP1 Task 1: Managing Information Security

## Part I: Incident Analysis and Response

### A. Vulnerabilities and Attack Success

The attack on Azumer Water's infrastructure succeeded due to several specific vulnerabilities identified in the case study. Azumer Water's main office used an outdated wireless security protocol called Wired Equivalent Privacy (WEP), which has been deprecated due to its weak encryption, making it vulnerable to attacks. This provided an attack vector for hacktivists to intercept and decrypt wireless traffic, gaining a foothold on the main office network.

The second vulnerability identified was Pruhart Tech's need to properly configure the public-facing enterprise firewall between the main office and the Internet Service Provider (ISP) ReadyNet. The unconfigured firewall exposed the main office's network to malicious traffic or unauthorized access attempts. A properly configured enterprise-level firewall integrates advanced threat protection, including email and web security protection. Email filtering and threat protection could have helped mitigate email phishing attacks by enabling firewalls to identify and block traffic to malicious phishing sites and drive-by downloads.

**B. CIA Compromises**

To explain how Azumer Water's operations were compromised will be accomplished using the ISO/IEC 27002 standard with the NIST Cybersecurity Framework (CSF). These frameworks provide best practices and security controls for managing information security related to protecting information confidentiality, integrity, and availability.

The email phishing incident compromised the confidentiality of Azumer Water's communication through a spear phishing attack designed to harvest credit cards and personally identifiable information targeting the personal emails of volunteers at Azumer Water. If the volunteers decided to complete the donation form, this would have compromised the volunteer's PII and payment information, including the potential exposure of the company's confidential data. ISO/IEC 27002:2022 states, "Information should be protected against unauthorized access and disclosure" (ISO/IEC, 2022). This industry standard emphasizes the need for adequate controls to reduce unauthorized access and data exposure risks. The phishing attack breached confidentiality by trying to collect PII through deception and social engineering.

Integrity and availability were compromised when John Smith discovered the volunteer's database was missing from Azumer Water. Data integrity is compromised when data is falsified or corrupted. This can lead to data falsification or misinformation in the volunteer database, compromising data integrity. ISO 27002 aligns with the NIST cybersecurity framework and provides controls designed to help protect data integrity. NIST CSF states, “Data integrity is maintained by ensuring that data is accurate and unaltered during storage, transmission, and processing” (NIST, 2018). The failure to

implement secure controls led to the compromise of data integrity due to misinformation or unauthorized modifications to the volunteer database.

The principle of availability ensures that data and systems are accessible to authorized users when needed. In this instance, availability was breached since John Smith could not access and retrieve critical data from the volunteer database. ISO/IEC 27002, Control 8.9, is a preventative control that addresses the importance of configuration management for maintaining availability. It recommends documenting, monitoring, and reviewing configurations of assets and data management systems. The failure to manage configurations led to the unavailability of their database, impacting Azumer Water's ability to access and retrieve critical information. Industry standards ISO/IEC 27002 and NIST CSF provide guidance to help organizations maintain operational resilience through security controls to protect sensitive information.

**C. Federal Regulation**

Azumer Water violated the Federal Information Security Modernization Act (FISMA). Azumer Water is an organization that's part of the Federal Emergency Management Agency (FEMA) and is responsible for providing clean drinking water for those affected by natural disasters. Azumer Water is required to protect federal information systems and adhere to FISMA standards.

A specific instance of non-compliance with FISMA was Azumer Water's lack of protection of its wireless network and insecure email practices. In the case study, Azumer Water used WEP, a deprecated wireless protocol known for its weak encryption and vulnerabilities. The failure to use updated wireless standards and encryption protocols makes Azumer Water non-compliant with FISMA requirements for failing to protect against unauthorized access to their information systems.

A second instance of non-compliance was the need for proper backup procedures and data protection. The volunteer database contains sensitive personal information, such as names, background checks, and social security numbers, backed up insecurely by employees on USB drives. FISMA requires organizations to implement adequate security controls to protect information management systems, including regular backups and secure data storage. The failure to regularly and securely maintain database backups violates FISMA's requirements. FISMA requires federal contractors and entities being contracted or supported by federal agencies to implement security controls to protect data and ensure authorized access to data.

**D. Immediate Steps**

The first action would be containment by isolating the affected systems and disconnecting the affected computers identified from the phishing attack. The email phishing incident exposed sensitive data and led to unauthorized access. Isolating the affected systems, such as the computers that opened the phishing emails, and segmenting the network can prevent the spread of malware or unauthorized access. These steps can prevent further damage or data exfiltration by isolating the affected systems through containment. Disconnecting the affected computers that interacted with the phishing email would help prevent the spread of potential malware or data loss. Isolating the computers or systems will limit the attack scope and protect other network segments.

Initiate a data recovery process and investigate the missing volunteer database. Investigating the missing database is crucial for restoring normal business operations and understanding the scope of the breach's impact. Begin by checking with any employees with storage media or USBs for recent backups. Then, a forensic investigation will be performed to identify how the database was lost or accessed. Checking recent employee backups can help recover the volunteer database. Then, a forensic investigation will be conducted by contacting the IT service team at Pruhart Tech to determine how the database was lost or if it was due to unauthorized access. Checking the database logs can help determine the scope of the data breach and prevent further incidents from occurring in the future.

**E. Incident Response Plans**

Having a defined and well-documented incident response plan (IRP) would greatly benefit Azumer Water by providing structured procedures to efficiently address, manage, and mitigate the impact of security incidents. IRPs provide clear procedures for detecting and reporting potential security incidents such as phishing attacks. In the case study, John Smith's failure to identify the phishing email led to unauthorized access and potential data breaches. An IRP provides steps to help employees verify the authenticity of emails and report any anomalies. This would have helped contain phishing attacks, reducing the potential risk of data exposure or disrupting business operations.

IRPs provide protocols that outline recovery procedures for regular backups to ensure data integrity and availability. In the case study, Azumer Water did not have any backup protocols, which led to the disruption of services and the potential loss of the volunteer database. An effective IRP would mandate regular backups and procedures for data recovery. This would have helped Azumer Water recover missing data and minimize service disruption.

## Part II: Risk Assessment and Management

### F. Processes

Azumer Water should correct violations of the Federal Information Modernization Act (FISMA) identified in part C by implementing specific processes to increase information assurance levels and improve its overall security posture.

The first violation was the lack of regular backup procedures and data protection, which led to the loss of their volunteer database, as identified in part C. Azumer Water should develop and enforce a formal backup policy that includes regular and systematic backup procedures. This policy should provide details on the backup type (full, incremental, differential) and frequency, based on their needs, to ensure secure storage practices for their backup data. FISMA requires the implementation of security controls to ensure data availability, including regular backup procedures and secure data storage practices. Maintaining a systematic backup procedure that includes encrypted storage solutions for backups and data at rest can help ensure the availability of critical data. These steps will help address the immediate issue of missing databases and meet long-term FISMA requirements while maintaining data availability and integrity.

Azumer Water can address the second violation in part C by upgrading its network security protocols from WEP to WPA3 and ensuring proper configuration of its firewalls. WPA3 offers improved security features such as more robust encryption and enhanced protection against unauthorized access and eavesdropping. In addition, proper configuration of their enterprise firewall will help secure their network perimeter against unauthorized access and attacks. These steps will help ensure Azumer Water corrects its non-compliance issues with FISMA by ensuring network security and data

protection. By implementing these processes, Azumer Water can address its specific violations with FISMA while improving its overall information assurance.

### G. Technical Controls

Implementing technical controls can help Azumer Water address the attack's immediate impact and prevent future attacks. Deploying an intrusion detection system (IDS) provides continuous monitoring of network traffic and can detect indicators of compromise, such as ongoing or new malicious activities. The IDS can be configured to provide continuous monitoring, alerts, and indicators of compromise, such as early identification of residual effects resulting from the phishing attack.

Installing endpoint detection and response (EDR) software agents on all endpoints, including the desktop computers in the main office. EDR solutions can address any remaining attack effects with tools containing and remediating threats through real-time monitoring, threat detection, and response. Implementing these technical controls can help Azumer Water counter any residual effects of the attack and remediate future attacks, improving its overall security posture.

**H. Organizational Structure**

Regular communication and reporting between the CISO, IT Manager, Security Manager, and Incident Response Coordinator ensure all levels of management are informed and prepared to handle security incidents efficiently. They also provide regular training and awareness for staff on security policies and incident reporting to maintain an effective security posture. By establishing this organizational structure, Azumer Water can efficiently manage and maintain IT and security operations to mitigate future incidents efficiently. The Chief Information Security Officer (CISO) is responsible for developing and overseeing IT security initiatives to meet business objectives and compliance requirements. The CISO supervises the IT and Security managers to ensure effective coordination and execution between IT and security-related operations. The CISO provides reporting directly to the CEO on IT security-related issues.

The IT manager manages daily IT operations, IT staff, system maintenance, and vendor management. The IT manager reports to the CISO on IT operational status and incidents affecting the IT infrastructure.

The Security Manager is responsible for developing and implementing security policies, risk assessments, and controls to protect the organization’s assets. This includes leading the incident response efforts, including the response activities and recovery efforts. The Security Manager reports to the CISO on security incidents, improvements, and their current security posture. The IT and Security managers often collaborate to ensure security controls are correctly integrated for effective incident response.

The Incident Response Coordinator coordinates response efforts between the IT staff and the Security manager to ensure a unified response to incidents. The Incident

Response coordinator facilitates communication between team members, documents incident response activities, and supports post-incident analysis. In addition, reports will be provided to the security manager, providing the status of ongoing incidents and response actions.

## I. Risk Management

Azumer Water's approach to risk management involves assessing and categorizing risks to develop a risk mitigation strategy by creating a risk register to evaluate specific risks based on their likelihood, severity, and impact.

**Risk 1: Email phishing attacks compromising email accounts**

**Likelihood:** High

- **Justification**: The case study showed that phishing attacks targeted volunteers and employees successfully. The absence of security measures increases the likelihood that the phishing attacks will successfully continue targeting Azumer Water staff.

**Severity**: Medium

- **Justification**: Phishing attacks can lead to unauthorized access to sensitive information and disrupt operations. The severity is considered medium since the impact can be contained by implementing proper security measures and controls.

**Impact**: Low

- **Justification**: The impact of phishing attacks can be limited by prompt incident response procedures and user education training. This can ensure that the overall impact can be limited and prevent significant disruption to operations.

**Risk 2**: **Data loss from lack of backups**

**Likelihood**: High

- **Justification**: Azumer Water does not have a formal backup policy and relies on manual methods (USB storage) for data backup, significantly increasing the risk of data loss. Due to unreliable backup practices, another attack or hardware failure will likely cause severe data loss.

**Severity**: Medium

- **Justification**: Loss of critical data can disrupt operations and service delivery. The severity is a medium since proper backup policies can mitigate the impact. Data loss severity can be reduced with proper backup policies and recovery procedures to restore any data loss.

**Impact**: Low

- **Justification**: The impact can be minimized if the backup data is partially intact or detected early. Even without a structured backup process, the impact and recovery process will delay operations temporarily.

**Mitigation strategy:** Risk 1 can be mitigated by email filtering, MFA, and user education, such as phishing awareness training. Risk 2 can be mitigated by implementing formal backup policies, including testing and automated backup procedures. By following these steps in identifying risks to the organization, Azumer

Water can improve its risk management practices, reducing the likelihood of security incidents and improving its overall security posture.

## References

ISO/IEC 27002:2022. (2022). *Information security, cybersecurity and privacy protection.* Retrieved from https://www.iso.org/standard/75652.html

NIST. (2018). *Framework for improving critical infrastructure cybersecurity*. Retrieved from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

U.S. Government Publishing Office. (2014). *Federal Information Security Modernization Act of 2014*. Retrieved from https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf