MANAGING INFORMATION SECURITY – C843

KOP1 TASK 1: ANALYSIS RESPONSE

Shane Deitle

Western Governors University

010577487

*Part I: Incident Analysis and Response*

**A. Determine why the attack on Azumer Water's infrastructure was successful, including the specific vulnerabilities that allowed the attack to occur. Provide details from the case study to support your claims.**

The attack on Azumer Water's infrastructure was successful because the organization had several vulnerabilities in its network and security practices. These vulnerabilities included the lack of a properly configured enterprise firewall, the use of the weak Wired Equivalent Privacy (WEP) Protocol for its wireless network, the lack of password change policies for employees, and the use of personal devices for accessing the network without proper security controls. Additionally, the organization did not have regular vulnerability assessments or proactive risk mitigation measures in place, and it relied on a reactive approach to security. All of these factors likely contributed to the success of the attack on Azumer Water's infrastructure.

**B. Explain how the confidentiality, integrity, and availability of Azumer Water's operations and PII (personally identifying information) data have been compromised, using NIST, ISO 27002, or another industry-standard framework to support two claims of compromise.**

The NIST Cybersecurity Framework is an outline for managing security risk of cyber threats in organizations (National Institute of Standards and Technology, 2018). The ISO 27002 is an international standard that provides guidelines and general principles for initiating, implementing, maintaining, and improving information security management in an organization (International Organization for Standardization, 2022). According to the NIST Cybersecurity Framework and the ISO 27002 standard, the confidentiality, integrity, and availability of Azumer Water's operations and personally identifying information (PII) data have been compromised in the following ways:

- Confidentiality: The organization's network was vulnerable to attack due to the lack of a properly configured enterprise firewall and the use of the weak WEP Protocol for its wireless network. This allowed an attacker to gain unauthorized access to the network and potentially compromise sensitive data, such as the PII of volunteers and employees.
- Integrity: The organization's security practices were insufficient, as evidenced by the lack of password change policies and the use of personal devices for accessing the network without proper security controls. This made it easier for an attacker to manipulate or alter data on the network, potentially leading to corruption of important information or disruption of operations.
- Availability: The organization's lack of regular vulnerability assessments and proactive risk mitigation measures made it more likely that vulnerabilities in its network and security practices would go undetected and unmitigated, increasing the likelihood of a

successful attack. This could have disrupted operations or made PII data unavailable to authorized users.

These claims are supported by the NIST Cybersecurity Framework and the ISO 27002 standard, which provide guidance on best practices for protecting the confidentiality, integrity, and availability of sensitive information and systems. By failing to implement these measures, Azumer Water left itself open to potential attacks that could compromise its operations and PII data.

**C. Identify a federal regulation this NGO violated, providing a specific example from the case study as evidence of Azumer Water's noncompliance.**

One federal regulation that Azumer Water has violated is the Federal Information Security and Modernization Act (FISMA). FISMA is a federal law that establishes requirements for organizations that work with federal agencies to have an effective information security program in place (113th U.S. Congress, 2014). According to FISMA, organizations that work with federal agencies, such as FEMA, are required to have an effective information security program in place. This program should include protocols for responding to, detecting, and reporting security events, as well as the effectiveness of information security policies, procedures, and practices being periodically evaluated and tested. The regularity of these evaluations and tests should be based on risk, but should be performed at least annually. Azumer Water, as an organization working with FEMA, is expected to be FISMA compliant and to have an effective information security program in place.

**D. Recommend immediate steps to mitigate the impact of the incident, using specific examples from the case study to justify how these steps would mitigate the impact.**

To mitigate the impact of the incident, Azumer Water should take the following immediate steps:

1. Implement a properly configured enterprise firewall solution to prevent unauthorized access to the network and protect against potential attacks.
2. Replace the weak WEP Protocol with a stronger wireless security protocol, such as WPA2, to enhance the security of the wireless network.
3. Implement password change policies to ensure that employees regularly update their access credentials and prevent unauthorized access to the network.
4. Implement security controls for personal devices used to access the network, such as requiring encryption and implementing a mobile device management solution.
5. Conduct regular vulnerability assessments and proactively mitigate or resolve identified risks to prevent potential attacks on the network and PII data.

6. Develop and implement an incident response plan to quickly and effectively respond to any future security incidents, including methods for restoring operations and PII data availability.

These steps would help to mitigate the impact of the incident by enhancing the security of the network and protecting against potential attacks. By implementing these measures, Azumer Water can better protect its operations and PII data from future incidents and ensure the continued availability of its services.

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

Having an incident response plan in place will benefit Azumer Water by providing a clear and structured approach for responding to security incidents. This will help the organization to quickly and effectively contain the incident, minimize any potential damage, and restore operations and PII data availability.

For example, an incident response plan could provide guidance on how to identify and report security incidents, such as unauthorized access to the network or PII data. It could also outline steps for containing the incident, such as disconnecting affected systems from the network or implementing temporary security measures to prevent further damage. Additionally, the plan could provide guidance on how to assess the impact of the incident and develop a plan for restoring operations and PII data availability.

By having an incident response plan in place, Azumer Water can better prepare for and respond to security incidents, reducing the potential impact on its operations and PII data. This can help to maintain the organization's reputation and trust with its stakeholders, and ensure the continued availability of its services.

*Part II: Risk Assessment and Management*

**F. Discuss two processes to increase information assurance levels within the organization and bring Azumer Water into compliance with the violated federal regulation identified in part C.**

To increase information assurance levels and bring Azumer Water into compliance with FISMA, the organization can implement the following processes:

1. Develop an information security program: FISMA requires organizations to have an effective information security program in place. This program should include policies and procedures for responding to, detecting, and reporting security events, as well as the effectiveness of information security practices being periodically evaluated and tested. The organization can work with an IT company, such as Pruhart Tech, or an internal team

to develop a comprehensive information security program that meets FISMA requirements.

2. Conduct regular security assessments: FISMA requires organizations to periodically evaluate and test the effectiveness of their information security policies and practices. This can be done through regular security assessments, such as vulnerability assessments, penetration testing, and audits. These assessments can help identify any potential vulnerabilities or weaknesses in the organization's security posture and provide recommendations for remediation. The organization should conduct these assessments at least annually, based on risk, to ensure compliance with FISMA.

Additionally, the organization can consider implementing additional security measures, such as encryption, password policies, and training for employees and volunteers, to further increase its information assurance levels and protect against security breaches. By implementing these processes, Azumer Water can increase its information assurance levels and better protect its operations and passwords guarding its sensitive information. This can help the organization to maintain its reputation and trust with its stakeholders, and ensure compliance with FISMA requirements.

**G. Recommend technical solutions to counter the remaining effects of the attack in the case study and to prevent future attacks.**

To counter the remaining effects of the attack and prevent future attacks, Azumer Water should implement the following technical solutions:

- Enterprise firewall solution: To prevent unauthorized access to the network, Azumer Water should implement a properly configured enterprise firewall solution. This can provide a protective barrier between the organization's network and the Internet, and help to prevent potential attacks from reaching the network.

- Stronger wireless security protocol: To enhance the security of the wireless network, Azumer Water should replace the weak WEP Protocol with a stronger wireless security protocol, such as WPA2. This can help to prevent unauthorized access to the network via the wireless network and protect against potential attacks.

- Security controls for personal devices: To ensure that personal devices used to access the network are secure, Azumer Water should implement security controls, such as requiring encryption and implementing a mobile device management solution. This can help to prevent unauthorized access to the network and protect against potential attacks.

- Regular vulnerability assessments: To proactively identify and mitigate potential risks to the network and PII data, Azumer Water should conduct regular vulnerability assessments. This can help the organization to identify and prioritize potential vulnerabilities, and implement appropriate mitigation measures to prevent potential attacks.

By implementing these technical solutions, Azumer Water can counter the remaining effects of the attack and better protect its network and PII data from future attacks. This can help the organization to maintain the availability of its operations and services, and ensure the continued trust and confidence of its stakeholders.

**H. 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.**

To support the efficient discovery and mitigation of future incidents, Azumer Water should implement the following organizational structure for IT and security management:

- Chief Information Security Officer (CISO): The CISO would be responsible for overseeing the organization's overall information security strategy and policies. This would include developing and implementing security standards and procedures, conducting regular risk assessments, and coordinating the response to security incidents.
- Information Security Manager: The Information Security Manager would be responsible for implementing and maintaining the organization's security controls and policies. This would include implementing technical solutions, such as enterprise firewalls and security protocols, and monitoring the network for potential vulnerabilities and threats.
- IT Manager: The IT Manager would be responsible for managing the organization's IT infrastructure and ensuring that it is secure and available. This would include maintaining the servers, networks, and other IT systems, and coordinating with the Information Security Manager to ensure that appropriate security measures are in place.

By implementing this organizational structure, Azumer Water can ensure that there is clear and logical delineation of roles and responsibilities for IT and security management. This can help the organization to efficiently discover and mitigate future incidents, and maintain the availability and security of its operations and PII data.

**I. Describe your risk management approach for Azumer Water based on the likelihood, severity, and impact categorization of two risks in the case study.**

My risk management approach for Azumer Water would be based on the likelihood, severity, and impact of potential risks. This approach would involve identifying and evaluating potential risks to the organization's network and PII data, and implementing appropriate mitigation measures to prevent or reduce their impact.

For example, one risk that Azumer Water faces is the likelihood of a security incident due to the organization's lack of proper security controls and practices. This risk is likely to occur with moderate likelihood, given the organization's vulnerabilities, such as the lack of a properly configured enterprise firewall and the use of the weak WEP Protocol for its wireless network. The severity of this risk is high, as a successful attack could compromise the confidentiality,

integrity, and availability of the organization's operations and PII data. The impact of this risk would be significant, as it could damage the organization's reputation and trust with its stakeholders, and disrupt the availability of its services.

To mitigate this risk, Azumer Water should implement appropriate security controls and practices, such as implementing a properly configured enterprise firewall solution and stronger wireless security protocols, conducting regular vulnerability assessments, and implementing incident response plans. These measures can help to prevent or reduce the likelihood of a security incident, and minimize its potential impact on the organization.

Another risk that Azumer Water faces is the likelihood of a data breach due to the organization's lack of proper protection for its PII data. This risk is likely to occur with low likelihood, given the organization's limited use of PII data and the fact that it is not stored in a cloud-based system. However, the severity of this risk is high, as a data breach could compromise the privacy of volunteers and employees and expose the organization to legal and regulatory penalties. The impact of this risk would be significant, as it could damage the organization's reputation and trust with its stakeholders, and potentially result in financial losses.

To mitigate this risk, Azumer Water should implement appropriate security controls and practices for protecting its PII data, such as implementing encryption and access controls, conducting regular risk assessments, and implementing incident response plans. These measures can help to prevent or reduce the likelihood of a data breach, and minimize its potential impact on the organization.

**J. Acknowledge sources, using in-text citations and references, for content that is quoted, paraphrased, or summarized.**

National Institute of Standards and Technology. (2018, April 16). *NIST Framework for Improving Critical Infrastructure Cybersecurity*. National Institute of Standards and Technology. Retrieved December 9, 2022, from https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf

International Organization for Standardization. (2022, March 1). *ISO/IEC 27002:2022*. International Organization for Standardization (ISO) Standards. Retrieved December 9, 2022, from https://www.iso.org/standard/75652.html

113th U.S. Congress. (2014, December 18). *S.2521 - 113th Congress (2013-2014): Federal Information Security Modernization Act of 2014*. Federal Information Security Modernization Act (FISMA). Retrieved December 9, 2022, from https://www.congress.gov/bill/113th-congress/senate-bill/2521

**K. Demonstrate professional communication in the content and presentation of your submission.**