A logo of a university

Description automatically generated

**Western Governor’s University**

Managing Information Security

C843

Joshua Lee

KOP1 – Task 1: Analysis Response

**Part I: Incident Analysis and Response**

1. **Determine why the attack on Azumer Water’s infrastructure was successful**

When viewing the case study for Azumer Water, there were many vulnerabilities that were apparent in the company. There were a couple specific vulnerabilities that allowed the attack to occur.

One of the vulnerabilities that likely attributed to the attack being successful was the reactive approach to infrastructure safety that Maria, the Pruhart Tech contact at Azumer Water, was employing. When employing a reactive approach, the security threats would be responded to after the occurred then managed and they wouldn’t have a procedure for it until then as well. Also, with the addition of Maria knowing the network vulnerable, this gap contributed to every issue that occurred such as the phishing attack and removal of the database. If a proactive approach was taken, Maria could have taken from standards, frameworks, and other known effective measures to have something in place that could have mitigated or prevented the phishing attacks and the missing database.

Another of the vulnerabilities that was a probable reason on why the attack on the infrastructure was successful was the lack of enforcement of the password policies that were stated in the handbook. With no enforcement of password changes and given the security posture, presumable lack of password complexity or length, it is highly likely someone was able to get a hold of John’s or one of his backups’ passwords who had access to the missing database. Another likelihood with this vulnerability is that the passwords were cracked due to no time, complexity, or logical requirements and could have been brute-forced or dictionary attacked to gain access to and remove the database.

1. **CIA Triad Compromised**

Confidentiality and PII were compromised similarly in the same fashion for multiple targets. The separate phishing attacks that occurred both with John and various volunteers are the example of the compromise. When John clicked the link in the phishing email that likely allowed a threat agent in to access their account, which in itself is a breach confidentiality, but also had access to the volunteer database which is a breach of confidentiality and compromise of PII. Examples of PII per the database include contact details and last 4 digits of their SSN. NIST SP 800-122 states, “Harm means any adverse effects that would be experienced by an individual whose PII was the subject of a loss of confidentiality, as well as any adverse effects experienced by the organization that maintains the PII” (McCallister et al., 2010). The other confidentiality and PII breach were with the phishing email that was sent to the volunteers. Anyone who provided their credit card, another form of PII, experienced a breach in confidentiality and PII

When the volunteer database was removed from the network, this was both a compromise of integrity and availability. With the database being deleted, it affected the availability of it as John nor other users with access no longer could access the data that was provided by it. The integrity part of this is that when the data was deleted, it was modified from its intended state and was altered without correct authorization. ISO/IEC 27000 states confidentiality as “property that information is not made available or disclosed to unauthorized individuals, entities, or processes” and integrity as “property of accuracy and completeness” in which the database was not available nor complete. This in turn is defined as Information Security “Information security involves the application and management of appropriate controls that involves consideration

of a wide range of threats, with the aim of ensuring sustained business success and continuity, and minimizing consequences of information security incidents.” (*ISO/IEC 27000:2018 - Information Technology — Security Techniques — Information Security Management Systems — Overview and Vocabulary*, n.d.)

1. **Identify violated Federal Regulation**

In the case study, it is stated that Azumer Water is part of the Federal Emergency Management Agency. Being that they are an organization affiliated with FEMA, that makes it subject to the Federal Information Security Management Act (FISMA) as it is a Federal Agency. FISMA provides “a comprehensive framework to protect government information, operations and assets against natural or man-made threats” (*WHAT IS FISMA | OLAO*, n.d.). A federal agency must follow information security standards developed by NIST to be compliant (Computer Security Division, 2016). Many of these controls are outlined in NIST 800-53.

Azumer Water violated FISMA in many ways. There was no apparent security training provided to members of Azumer Water which would have created an awareness for the phishing attacks that occurred and could have minimize the attack surface of this particular attack and others.

Another of these was that Azumer Water chose not to enforce the password policies that were outlined in the Employee Handbook, as well as they have not been updated which means they were also likely not in line with current standards.

1. **Immediate Steps for Mitigation**

First and foremost, would be mitigating how the threat agent was able to access the network. For John and all others who clicked the links in the two phishing emails, their computers should be quarantined and ran through a process to check for malware or security compromises that need to be mitigated and fixed. This should start with the ones who have elevated privileges first, as their accounts would cause the most damage if compromised, but all users who clicked the phishing link should be scanned and validated.

Next would be to configure the firewall and implement the proper settings in order to adequately. This would be lists for access control, doing research on what protocols need to be allowed and only allowing those that are needed for business, making sure those protocols are the secure versions of the protocols, and starting a blacklisting of URLs of known sites to be blocked in addition to the ones that were on the links from the phishing emails.

1. **Benefit of an Incident Response Plan**

Currently Maria of Pruhart Tech is exercising a reactive approach to infrastructure security. The problem is that they are responding to threats after they occur and focusing on detecting and containing these threats in progress. If there has been no experience with the security threat, the time it takes to mitigate could cause drastic damage.  
  
Having an incident response plan in place, would be the first step to having a proactive approach to security threats and help in developing a rounded strategy for incidents such as these. First would be the preparation of a plan which would include creating an incident response team and having their contact information and instructions on when to contact. This would allow for less confusion on who to contact, as well as keeping the information directed at the correct people who can assist with the incident. This team will be trained on how to react to incidents and use standards, best practices and frameworks in order to create an information base (along with mainlining it with new information as it arises) to help protect the information and infrastructure. The IRT team will also practice this to make it as seamless as possible.

An incident response plan also would provide information on how to detect and analyze threats to gauge whether or not the Incident Response Team needs to be notified. This might be able to be mitigated using the documentation provided in the preparation phase or if the incident is not able to be and validated to be an incident, the IRT can be called to intervene. Measures will also be put in place to prevent it.

The IRT team would then have a strategy on how to contain the issue, eradicate it and recover the affected systems. This would be in line with processes ahead of time prepared by the team in documentation or if it is an issue no conceived of or documented, they would follow a process on how to come up with a solution. No matter the incident, this would all be documented to go over and learn from after the incident has taken care of and the affected systems recovered back to operation standards.

By following the above information, it would change the approach to proactive one. Instead of waiting or issues to occur, the company would be able to react to incidents faster and even be able to prevent them.

**Part II: Risk Assessment and Management**

1. **Increasing Information Assurance**

There are many processes that would assist in bringing Azumer Water in compliance with FISMA. Since a federal agency must follow security standards developed by NIST as one of the steps to become compliant, here are a couple of processes from NIST 800-53 that would apply the referenced violations above to do so.

One of the processes that would help to increase information assurance levels is to implement an awareness and training program. This would be developing awareness and training policies along with onboarding and reoccurring training to educate the employees and have them know what to do in certain situations, as well as what to be aware of. “Policies and procedures contribute to security and privacy assurance. Therefore, it is important that security and privacy programs collaborate on the development of awareness and training policy and procedures” (Force, 2020).

Another of the processes that would help is in reference to the non-enforcement of password polices above. NIST does not require a periodic password change and complexity and only require a password of 8 characters or less. It would still be best practice to create a complexity requirement, enforce passwords of 15 characters or more, as well as a expiry on the password to prevent issues like this to happen again. This is not a way to become compliant but to be in line with best practices. To become compliant, NIST recommends that multi-factor authentication be implemented for access to privileged accounts. “Regardless of the type of access (i.e., local, network, remote), privileged accounts are authenticated using multi-factor options appropriate for the level of risk” (Force, 2020).

1. **Recommended Technical Solutions**

One of the technical solutions would be to do an Access Control Audit of affected accounts. Disabling the accounts and resetting all passwords associated with them. This would cut any access threat agents had to these accounts. Then apply the above best practices with stronger password policies and implementing MFA to assure this will not happen again.

The next technical solution would be to change the wireless to a WPA3 for a better encrypted protocol. It is possible the network was or could be breached by using WEP as an insecure protocol and this would make it that much harder to compromise. Also, it would be good to create a separate guest network segmented from the main network for volunteers to access the Internet without the possibility of a network compromise.

1. **Organizational Structure for IT and Security Management**

So first there would be the top leadership of the organization which would be the Chief Information Officer (CIO) and the Chief Information Security Officer (CISO). The CIO would oversee the IT planning and security management, where the CISO would be more of the enforcer of the two. The CISO would assess the risks to see which framework or policies, with an emphasis on discover and mitigation of future incidents, would be needed to be implemented and would establish that framework would be used and make sure those policies are enforced.

Under the CISO would be the Security Management group that would be proactive on security. Security Operations Center (SOC) Analysts would be the ones who monitor and try to prevent incidents. They would then escalate to the Incident Response Team members who would contain, eradicate, and recover from incidents and conduct the investigations into why the incidents occurred.

Then in another branch under the CIO, will be the IT Manager who would manage the IT group and coordinate all IT operations. They would be the System Administrators that would maintain and secure the systems of the company and the Network Administrators that would do the same for the networks and infrastructure. Lastly under this umbrella, would be the IT Support staff who would provide technical support and help to enforce all the policies and protocols.

1. **Risk Management Approach**

One of the risks that were apparent in the case study was the phishing attacks and other attacks similar such as spoofing or social engineering. The likelihood of this currently would be High as there is no information on employee security training and awareness. The severity would be High as well since already shown it could lead to unauthorized access to data, unauthorized access of accounts and could lead to even disruption of service or malware/ransomware attacks. Impact would be High as well since it could cause legal repercussions being a federal agency, disruption of service to provide emergency relief and the list could go on.

Another of the risks that show in the case study was the possibility of unauthorized access. The likeliness of this is High as the wireless was configured using am unsecure WEP protocol, no password policy, and the lack of Multi-Factor Authentication. The severity of this would be high as this would allow gained access to authorized systems and the impact would be high as well as this could constitute in data breaches and disruptions of service.

The risk management approach I would select for Azumer Water would be the one from NIST SP 800-53. Selecting this framework fits as Azumer Water needs to satisfy FISMA requirements and it fits those guidelines. The first step would be to prepare processes to get the organization ready to manage security/privacy risks. Next would be to categorize the system and what typed of data it handles through an impact analysis. Third would be selecting the correct set of NIST controls that would best suit the protection of the system. Then would be implementing the controls and document the process of deployment. After implementing, the controls that have been established would be evaluated to see if the are working as intended and providing the correct outcomes. The CIO or CISO would then decide to authorize the system or not. Then the final step would be to monitor the controls and monitor potential risks to the selected system (Force, 2018)**.**

**References**

McCallister, E., Grance, T., & Scarfone, K. A. (2010). Guide to protecting the confidentiality of Personally Identifiable Information (PII) (NIST SP 800-122; 0 ed., p. NIST SP 800-122). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-122>

ISO/IEC 27000:2018—Information technology—Security techniques—Information security management systems—Overview and vocabulary. (n.d.). Retrieved November 19, 2024, from <https://www.iso.org/standard/73906.html>

WHAT IS FISMA | OLAO. (n.d.). Retrieved November 20, 2024, from <https://olao.od.nih.gov/content/what-fisma>

Computer Security Division, I. T. L. (2016, November 30). FISMA Background—NIST Risk Management Framework | CSRC | CSRC. CSRC | NIST. <https://csrc.nist.gov/projects/risk-management/fisma-background>

Force, J. T. (2020). Security and Privacy Controls for Information Systems and Organizations (NIST Special Publication (SP) 800-53 Rev. 5). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-53r5>

Force, J. T. (2018). *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy* (NIST Special Publication (SP) 800-37 Rev. 2). National Institute of Standards and Technology. <https://doi.org/10.6028/NIST.SP.800-37r2>