Redback Operations

Project 2: Elderly Wearable Technology Audit Report

SIT374 TEAM PROJECT A

ALESSANDRA DOMINIQUE COLMENARES
9-15-2024

Contents

Introduction

This report presents the findings from the audit of Project 2: Elderly Wearable Technology, which aims to improve the quality of life for elderly individuals through wearable devices that provide health monitoring, emergency alerts, and social connectivity. The audit focused on evaluating the project's compliance with Redback Operations' Information Security Management System (ISMS) policies, particularly regarding data handling, encryption, and security practices.

The audit interview took place on 12/09/2024 with Manan Purvish Gangar, the project lead. It was revealed that both the project team and the Data Warehousing Team were unaware of Redback's ISMS policies, resulting in several areas of non-compliance. This report outlines these findings, provides recommendations for improvement, and details the actions required to ensure compliance moving forward.

Audit

Policy Compliance

1. **Are the correct encryption methods being used for data in storage and transmission?**
    - No, encryption controls are not being adhered to as data is transmitted and stored in plaintext.
    - Action Required:
        - Implement AES-256 encryption for all sensitive data in storage and secure transmission protocols (TLS/SSL).
        - Train employees on encryption standards and conduct regular reviews.

2. **Are the related DLP Policies being adhered to?**
    - No, DLP policy requirements are not met.
    - Action Required:
        - Implement data classification per policy (public, internal use, confidential, restricted).
        - Apply role-based access and the least privilege principle.
        - Encrypt sensitive data in transit and storage using AES-256.
        - Introduce watermarking, screen-capture prevention, and clipboard controls.
        - Implement automated content scanning to detect unauthorized data leaks.
        - Conduct regular audits and reviews to ensure DLP compliance.

3. **Are the related Data Classification Policies being adhered to?**
    - No, data classification practices are not applied.
    - Action Required:
        - Classify all data per policy specifications and ensure encryption and access controls align with data sensitivity.
        - Regularly review data classifications.

4. **Have forms of physical security for data protection been implemented?**
    - No, adequate physical security measures are absent.
    - Action Required:
        - Secure devices containing sensitive data and restrict physical access to essential personnel only.
        - Implement automatic device lockouts after periods of inactivity.

5. **Have forms of digital security for data protection been implemented?**
    - No, essential digital security practices are not enforced.
    - Action Required:
        - Regularly update systems with security patches, deploy comprehensive malware protection, and enforce least privilege access.

6. **Have EASM risks been identified?**
    - No, there is no identification of EASM risks.
    - Action Required:
        - Perform EASM risk assessments and classify external risks.

7. **Have appropriate EASM risk management strategies been implemented?**
    - No, EASM risk management strategies are lacking.
    - Action Required:
        - Develop and implement EASM strategies, ensuring consistent monitoring and updating based on the latest threat intelligence.

8. **Have all employees undergone the appropriate User Awareness Training?**
    - No, employees have not completed required training.
    - Action Required:
        - Employees must read the Cybersecurity User Awareness Training document to ensure they are informed about security practices and policies.

Ethical Considerations and Requirements

1. **Are all forms of data collection briefed with customers and consent gathered?**
    - No, most of the data is gathered through public domains, but there is private data involved, and the ethical considerations for handling it are still under discussion.
    - Action Required:
        - Finalize the ethical considerations for the private data.
        - Ensure all forms of data collection, especially for private data, are clearly communicated to customers, and obtain explicit consent before proceeding with any data collection.

2. **Has all collected information and data been classified according to data classification requirements?**
    - No, collected data has not been properly classified.
    - Action Required:
        - Classify all collected data according to the company's data classification policy to ensure proper handling and protection of sensitive information.

3. **Is data anonymity used to protect the privacy of customers?**
    - No, data anonymization is still a work in progress.
    - Action Required:
        - Finalize and implement data anonymization protocols to ensure customer privacy is protected.

4. **Is the cryptography policy being adhered to?**
    - No, encryption standards are not being followed, as Fernet (128-bit encryption) is used instead of the required 256-bit encryption.
    - Action Required:
        - Follow the cryptography policy by implementing 256-bit encryption for sensitive data, both in transit and at rest.

5. **Is data minimization in place when collecting data?**
    - Yes, data minimization practices are being applied.
    - Action Required:
        - No action required.

6. **Are ISMS (Information Security Management System) policies being adhered to when required?**
    - No, ISMS policies are not being followed.
    - Action Required:
        - Review and ensure adherence to ISMS policies across all relevant areas of the organization, including data handling, encryption, and access control.

Governance

1. **Is the team adhering to the company's governance framework?**
    - No, the team is not aware of the company's governance framework.
    - Action Required:
        - Provide the team with training and documentation on the company's governance framework and ensure adherence through regular check-ins.

2. **Are team roles and responsibilities clearly defined and documented?**
    - Yes, team roles and responsibilities are defined and documented.
    - Action Required:
        - No action required.

3. **Is there a risk management plan in place?**
    - No, there is no formal risk management plan.
    - Action Required:
        - Develop and implement a comprehensive risk management plan that includes identifying, assessing, and mitigating potential risks.

4. **Is there an incident response plan in place?**
    - No, an incident response plan is not in place.
    - Action Required:
        - Create and implement an incident response plan to ensure prompt and efficient handling of any security incidents or breaches.

5. **Are incidents logged and reviewed for continuous improvement?**
    - No, incidents are not being logged.
    - Action Required:
        - Establish a process to log all incidents and regularly review them to improve security measures and prevent recurrence.

Overall Findings and Recommendations

The audit of Project 2: Elderly Wearable Technology uncovered significant non-compliance with Redback's ISMS policies. Both the Project 2 team and the Data Warehousing Team are unaware of the company's security policies, resulting in issues with encryption, data classification, and governance.

The lack of encryption is a major concern, as data is stored and transmitted in plaintext. Additionally, data classification has not been implemented, and DLP policies are not followed. There is no formal risk management or incident response plan, leaving the project vulnerable. Moreover, the required Cybersecurity User Awareness Training has not been completed, and there is no process for incident logging and review.

The first and most important step is for all team members to familiarize themselves with Redback's ISMS policies. This will ensure compliance with encryption standards, data classification, and DLP requirements. Implementing risk management and incident response plans is also essential. Regular audits should be conducted to reinforce compliance and ensure all security measures are properly applied.

Conclusion

The audit of Project 2: Elderly Wearable Technology revealed key gaps in compliance with Redback's ISMS policies, primarily due to a lack of awareness across both the Data Warehousing and project teams. Ensuring that all team members read and follow the ISMS policies is crucial for improving security practices. With the recommended actions in place, the project can move forward securely, aligned with company standards, and ensuring the protection of data and overall success.