WK4: CYBERSECURITY PLAN

Part 4

Anila Naz

University of Phoenix

BSA-425: BSIT Capstone

Professor: Dr. Reid

25th July 2024

Introduction

This cybersecurity plan outlines the strategic approach to safeguarding the data, systems, and processes of the internet bank project in handling sensitive financial data and personal information. It is essential to ensure the security of this data is paramount. The plan is designed to mitigate risks, protect sensitive information, and ensure the continuity of operations. This Cybersecurity Plan outlines the measures and protocols that will be implemented to protect the data and processes from unauthorized access, breaches, and internal and external cybersecurity threats to the system.

1. Objectives:

- **Confidentiality**: Ensuring that the sensitive information is accessible only to those authorized to have access to the system.
- **Integrity**: Safeguarding the confidentiality, accuracy, and completeness of information and processing methods of the system.
- **Availability**: Ensuring the information and critical services are available to users when needed.

2. Security Policies and Procedures:

Access Control:

- **User Authentication**: Implementation of multi-factor authentication (MFA) for all user accounts and Role-Based Access Control (RBAC).
- **Account Management**: Regularly review and update user access rights and disable accounts that are no longer in use.

Risk Assessment

A comprehensive risk assessment will be conducted to identify potential threats and vulnerabilities. This assessment will cover:

- **Asset identification:** Determining critical assets, including customer data, financial transactions, and system infrastructure.
- **Threat identification:** Recognizing potential threats like cyberattacks, unauthorized access, and data breaches.
- **Vulnerability assessment:** Identifying weaknesses in systems, applications, and processes.
- **Risk analysis:** Evaluating the likelihood and impact of potential threats.

Security Controls

A robust set of security controls will be implemented to protect the internet banking system:

Technical Controls

- **Data Security:**
    - Access controls: Restricting access to data based on the need-to-know principle.
    - Data encryption: Encrypting sensitive data to protect its confidentiality, use strong encryption (AES-256) for data at rest and data in transit.
    - Data Masking: Mask sensitive information such as Social Security numbers, credit card numbers, and account numbers in logs and user interfaces.
    - Data loss prevention (DLP): Preventing unauthorized data transfer.
    - Data backup and recovery: Implementing regular backups and robust disaster recovery plans to ensure data availability.
- **Network Security:**
    - Firewalls: Implementing strong firewalls to protect the network perimeter.

    - Intrusion Detection and Prevention Systems (IDPS): Deploying IDPS to detect, monitor, and analyze network traffic for signs of suspicious activity and prevent unauthorized access.
    - Virtual Private Networks (VPNs): Providing secure remote access for authorized users.

- **Application Security:**
    - Secure coding practices: Enforcing secure coding standards, guidelines, and conducting code reviews to identify and mitigate vulnerabilities.
    - Regular Security Testing: Performing regular penetration testing and vulnerability assessment.
    - Input validation: Implementing input validation to protect against injection attacks.
    - Web Application Firewall (WAF): Using WAF to protect applications from common attacks such as SQL injection and cross-site-scripting (XSS).
    - Encryption: Encrypting sensitive data both at rest and in transit.

Endpoint Security:

- **Antivirus and Anti-Malware**: Ensuring all endpoints have updated antivirus and anti-malware software.
- **Patch Management**: Regularly update and parch all systems and applications to protect against known vulnerabilities.
- **Device Management**: Implement Mobile Device Management (MDM) for secure access and management of mobile devices.

Administrative Controls

- **Security policies and procedures:** Developing and enforcing clear security policies.
- **Access management:** Implementing strong access controls, defining roles and assigning permissions based on the principles of least privilege including role-based access control (RBAC).
- **Security awareness training:** Conducting regular security awareness training for employees.
- **Incident response plan:** Developing and testing an incident response plan for security breaches.
- **Business continuity and disaster recovery (BCDR):** Establishing BCDR plans to ensure business continuity.

Physical Controls

- **Physical access control:** Protecting physical access to facilities and equipment.
- **Environmental controls:** Maintaining appropriate environmental conditions for hardware.
- **Device security:** Implementing security measures for mobile devices and endpoint protection.

3. Security Monitoring and Compliance

Continuous monitoring and compliance activities will be essential:

- **Security monitoring:** Implementing security information and event management (SIEM) to monitor network traffic and system logs.
- **Vulnerability management:** Regularly scanning for vulnerabilities and patching systems promptly.

- **Compliance:** Ensuring adherence to relevant industry regulations and standards (e.g., PCI DSS, GDPR, CCPA).
- **Data Privacy**: Implement measures to protect customers' data privacy in accordance with applicable laws and regulations.

Security Testing

Regular security testing will be conducted to identify vulnerabilities:

- **Penetration testing:** Simulating attacks to identify weaknesses.
- **Vulnerability scanning:** Identifying vulnerabilities in systems and applications.
- **Security audits:** Assessing compliance with security policies and standards.

4. Incident Response Plan:

A comprehensive incident response plan will be in place to address security incidents:

- **Incident detection and Analysis:** Implementing systems to detect security incidents promptly. Monitor systems continuously for potential security incidents and analyze alerts to determine their validity.
- **Containment, Eradication, and Recovery:** Quickly contain and eradicate threats to prevent further damage and recover systems to their normal state.
- **Incident response team:** Establishing a dedicated incident response team.
- **Communication plan:** Developing a communication plan for stakeholders.
- **Post-incident analysis:** Conducting thorough investigations to identify root causes and prevent recurrence.

5. **Security Training and Awareness**:

- **Employee Training**: Regularly train employees on security policies, procedures, and best practices.

- **Phishing Awareness and Tabletop Exercises**: Conduct regular phishing awareness campaigns and simulated phishing attacks to educate employees.

6. **Continuous Improvement**

- **Threat Intelligence**: Technology security plan will be continuously reviewed and improved based on emerging threats, technology advancements, and regulatory changes. Update security measures accordingly.
- **Security Audits**: Conduct regular security audits to assess the effectiveness of security measures and identify areas for improvement.

7. **Collaboration and Communication**:

Effective collaboration and communication among stakeholders are crucial for the success of the Cybersecurity Plan. Regular communication channels will be established to share information and synchronize team efforts.

By implementing the measures outlined in this Cybersecurity Plan, the Internet Bank project will safeguard its data and processes against innumerable security threats, ensuring the confidentiality, integrity, and availability of critical information.

REFERENCES:

CISA (CYBERSECURITY & INFRASTRUCTURE SECURITY AGENCY). (n.d.). *Cybersecurity Best Practices*. https://www.cisa.gov/topics/cybersecurity-best-practices

CIS Center for Internet Security. (n.d.). *CIS Critical Security Controls*. https://www.cisecurity.org/controls

FINRA. (n.d.). *Cybersecurity*. https://www.finra.org/rules-guidance/key-topics/cybersecurity

MSRC. (n.d.). *Microsoft Security Response Center*. https://msrc.microsoft.com/

NIST. (n.d.). *CYBERSECURITY FRAMEWORK*. https://www.nist.gov/cyberframework

OWASP. (n.d.). *Explore the world of cyber security*. https://owasp.org/

SANS.org. (n.d.). *Empowering Cyber Security Practitioners & Teams*. https://www.sans.org/

Singer, P. W., & Friedman, A. (2014). *Cybersecurity and Cyberwar: What Everyone Needs to Know*. Oxford University Press. https://whateveryoneneedstoknow.com/display/10.1093/wentk/9780199918096.001.0001/isbn-9780199918096-book-part-1