Botium Toys Internal IT Audit: Summary Report

Project Overview

This internal IT audit was conducted for Botium Toys, a fictional U.S.-based toy company experiencing rapid online growth. The audit assessed the company's cybersecurity posture, compliance with relevant standards, and identified risks, threats, and vulnerabilities to critical assets.

Audit Scope and Goals

- **Scope:** The audit encompasses Botium Toys' entire security program, including assets such as employee devices, the internal network, and company systems.
- **Goals:** To evaluate existing assets, complete the controls and compliance checklist, and identify gaps that need to be addressed to improve the company's security posture and ensure compliance with U.S. and international regulations.

Key Findings

1. **Strengths:**
    - Basic access controls are in place for employee systems.
    - Antivirus software is installed and monitored regularly.
    - The IT department has implemented firewalls with defined security rules.
    - Physical security measures, such as locks and CCTV, are effective.
2. **Weaknesses:**
    - **Data Security Risks:**
        - Encryption is not used for sensitive customer data, including credit card information.
        - Customer PII and SPII are accessible by all employees.
    - **Access Management Gaps:**
        - Lack of least privilege and separation of duties.
        - Outdated password policies and no centralized password management system.
    - **Incident Preparedness Gaps:**
        - No disaster recovery plans or data backups in place.
        - No intrusion detection system (IDS) installed.
    - **Compliance Issues:**
        - The company does not fully comply with GDPR or PCI DSS requirements.

Compliance Assessment

Based on the completed Controls and Compliance Checklist:

- **Compliant Areas:**

    - Antivirus management, firewalls, and physical security.
    - Policies to notify E.U. customers of breaches within 72 hours.
- **Non-Compliant Areas:**
    - Encryption, access controls, disaster recovery, and compliance documentation.

Recommendations

To address these issues and improve compliance:

1. **Implement Encryption:** Encrypt customer data at rest and in transit to ensure confidentiality.
2. **Enhance Access Controls:** Introduce least privilege principles and separation of duties.
3. **Strengthen Password Management:** Update the password policy to meet current complexity standards and deploy a centralized management system.
4. **Develop a Disaster Recovery Plan:** Establish regular data backups and detailed incident response procedures.
5. **Install Intrusion Detection Systems:** Deploy an IDS to monitor and mitigate unauthorized activity.
6. **Ensure Compliance with GDPR and PCI DSS:** Maintain clear documentation and enforce compliance practices.

Conclusion

Botium Toys has taken initial steps to secure its IT infrastructure, but significant gaps remain. Addressing these weaknesses will enhance the company's security posture, ensure compliance with relevant standards, and support future growth. Implementing the recommended actions is crucial to mitigating risks and protecting critical assets.