Botium Toys: Scope, goals, and risk assessment report

Goals of the Audit

1. **Asset Management**
   - Goal: Identify and classify all assets managed by Botium Toys, including on-premises equipment, employee devices, storefront products, management systems, and legacy systems.
   - Objective: Develop a comprehensive inventory of assets and establish a system for ongoing management and classification.

2. Compliance and Controls
   - Goal: Assess the current controls and compliance status of Botium Toys in relation to U.S. and international regulations and standards.
   - Objective: Complete a controls and compliance checklist, addressing areas such as data protection, encryption, access controls, and adherence to best practices.

3. NIST CSF Function - Identify
   - Goal: Implement the first function of the NIST Cybersecurity Framework (Identify) to enhance the overall security posture of Botium Toys.
   - Objective: Dedicate resources to identify and classify assets, as well as determine the impact of potential asset loss on business continuity.

4. Risk Mitigation
   - Goal: Mitigate the identified risks associated with inadequate asset management, lack of controls, and non-compliance.
   - Objective: Develop and implement measures to address specific risks, including improving access controls, implementing encryption, and establishing disaster recovery plans.

5. Security Awareness
   - Goal: Enhance security awareness among Botium Toys employees.
   - Objective: Provide training on security best practices, compliance requirements, and the importance of adhering to established controls.

Current assets

Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Data retention and storage
- Legacy system maintenance: end-of-life systems that require human monitoring

Risk assessment report

1. Risk Description

- Inadequate management of assets.
- Lack of proper controls and potential non-compliance with U.S. and international regulations.

2. Risk Score

- Score: 8 (fairly high) on a scale of 1 to 10.
- Justification: Lack of controls and adherence to compliance best practices.

3. Potential Impact

- Medium impact from the loss of an asset due to uncertainty about which assets are at risk.
- High risk of fines from governing bodies due to inadequate controls and non-adherence to compliance best practices.

4. Specific Risk Factors

- Unauthorized access to sensitive data by employees.
- Lack of encryption for credit card information.
- Absence of access controls based on least privilege.
- No intrusion detection system and inadequate disaster recovery plans.
- Non-compliance with password complexity requirements.

5. Additional Comments

- Privacy policies and procedures exist but need to be reinforced.
- Password policy is nominal and not in line with current standards.
- No centralized password management system.
- Legacy systems are monitored, but maintenance lacks a regular schedule.
- Physical security measures at the store's location are sufficient.

6. Recommendations

- Implement robust asset management processes.
- Enhance controls related to data protection, encryption, and access.
- Develop and test disaster recovery plans.
- Strengthen password policies and implement a centralized management system.
- Regularize maintenance tasks for legacy systems.
- Reinforce privacy policies and conduct periodic training for employees.

This report outlines the goals, risk assessment, and recommendations to improve the security posture of Botium Toys.