Botium Toys Audit 1/29/2024

1. **Scope and Objectives:**
   - **Scope:** The scope is defined as the entire security program at Botium Toys. This means all assets need to be assessed alongside internal processes and procedures related to the implementation of controls and compliance best practices.

   - **Goals:** Assess existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' security posture.

2. **Asset Inventory:**
   - 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
     *(items marked ** are of higher criticality)*

3. **Access Controls**:

   - **Admin/Managerial Controls:**
     - ☐ Least Privilege
     - ☐ Disaster recovery plans
     - ☑ Password policies
     - ✖ Separation of duties
   - **Technical Controls:**
     - ☑ Firewall
     - ✖ Intrusion detection system (IDS)
     - ✖ Backups
     - ☑ Antivirus software
     - ☑ Manual monitoring, maintenance, and intervention for legacy systems
     - ✖ Encryption
     - ✖ Password management system

   -

- **Physical controls:**
  - ☑ Locks (offices, storefront, warehouse)
  - ☑ Closed-circuit television (CCTV) surveillance
  - ☑ Fire detection/prevention (fire alarm, sprinkler system, etc.)

4. **Compliance Checklists:**

- **Payment Card Industry Data Security Standard (PCI DSS)**
  - ✖ Only authorized users have access to customers' credit card information.
  - ✖ Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
  - ✖ Implementation of data encryption procedures to better secure credit card transaction touchpoints and data.
  - ✖ Adopt secure password management policies.
- **General Data Protection Regulation (GDPR)**
  - ✖ E.U. customers' data is kept private/secured.
  - ☑ There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
  - ✖ Ensure data is properly classified and inventoried.
  - ☑ Enforce privacy policies, procedures, and processes to properly document and maintain data.
- **System and Organizations Controls (SOC type 1, SOC type 2)**
  - ✖ User access policies are established.
  - ✖ Sensitive data (PII/SPII) is confidential/private.
  - ☑ Data integrity ensures the data is consistent, complete, accurate, and has been validated.
  - ☑ Data is available to individuals authorized to access it.

5. **Security Awareness Training**:
- Currently no awareness training program exists
- Employees are potentially unaware of evolving social engineering tactics and mishandling of customer PII/SPI
- Simulated phishing exercises would be unintuitive as there is no training program available to base employee knowledge from

6. **Third-Party Assessments**:
- Currently no third party vendors or external partners exists with the company

7. **Documentation and Policies:**
- Company does have, maintain, and enforce a privacy policy, procedures, and processes, including a 72 hour timeframe of security breach notification for E.U. customers plan.

8. **Audit Report and Recommendations:**
   - Botium Toys has a current risk score of 8 which is significantly high due to lack of controls and adherence to compliance best practices
   - **Controls in compliance:**
     - Firewall is in place and in working conditions
     - Physical location has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.
     - Privacy policy and procedures are up to date and enforced to maintain and document data
     - A 72 hour Security breach notification system for E.U. customers is brilliant and complies with the PCI DSS

   - **Recommendations**:
     - A disaster recovery plan is extremely important to ensure proper management of a potential crisis
     - Backups of critical data is vital to business continuity and recovery
     - Introduce more complex password requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
     - Develop or outsource a centralized password management system that will enforce password requirements (this will potentially reduce frustrations due to password recovery/reset)
     - Set up **scheduled** legacy system monitoring/maintenance procedures and have clear methods for handling intervention and asset protection
     - An Intrusion Detection System (IDS) is a **vital** part of any internal network as they significantly mitigate risk
     - A system of least privilege and separation of duties is highly recommended due to the severe negative impact of free access to potentially sensitive customer data
     - An encryption system with salts to ensure confidentiality of customer data