**Step 1: Review of Assets**

The following assets are managed by Botium Toys' IT department:

1. **Physical Equipment**
   * On-premises office devices: desktops, laptops, smartphones, remote workstations, peripherals (keyboards, headsets, docking stations).
   * Surveillance systems and CCTV.
   * Storefront products and warehouse inventory.
2. **Systems and Software**
   * Accounting, telecommunication, database management, security, ecommerce, and inventory systems.
3. **Networks and Connectivity**
   * Internal network and internet access.
4. **Data Management**
   * Data retention and storage systems.
   * Legacy systems requiring manual maintenance.

**Step 2: Risk Assessment Review**

**Key Risks Identified**

* **Inadequate Asset Management**: Assets are poorly classified and not systematically tracked.
* **Lack of Encryption**: No encryption mechanisms are implemented to secure customer PII and credit card data.
* **Access Control Issues**:
  + No least privilege or separation of duties policies.
  + All employees have unrestricted data access.
* **No Intrusion Detection System (IDS)**: No mechanism to monitor and detect potential security breaches.
* **Lack of Backups and Disaster Recovery Plans**: Critical data is not backed up, and there is no recovery strategy.
* **Non-compliance with GDPR (E.U. Regulations)**: Potential regulatory violations due to inadequate privacy controls and security measures.
* **Weak Password Policy**: Current password policy is outdated and lacks enforcement mechanisms.
* **Legacy Systems Maintenance Gaps**: No scheduled updates or clear intervention procedures.

**Risk Score: 8/10**

* **Potential Impact**: Medium for asset loss but **high for regulatory penalties and reputational damage**.
* **Step 3: Controls and Compliance Checklist**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **Control** | **Status** | **Recommendations** | | **Asset Management** | Inadequate | Implement a centralized asset tracking system. Classify assets based on criticality and assign ownership. | | **Encryption** | Not in place | Deploy end-to-end encryption for sensitive data storage and transmission, especially for payment card information. | | **Access Controls** | Lacking | Enforce least privilege policies and role-based access controls. Implement separation of duties. | | **Intrusion Detection System (IDS)** | Not installed | Install and configure an IDS to monitor network activity and detect unauthorized access. | | **Data Backup & Disaster Recovery** | Missing | Develop and implement a backup strategy with automated backups and regular tests of disaster recovery plans. | | **GDPR Compliance** | Partially compliant | Improve compliance with GDPR by encrypting E.U. customer data, documenting all data processing activities, and ensuring appropriate data breach notification processes. | | **Password Policy** | Weak | Update password policy to require 12-character minimums with complexity (uppercase, lowercase, numbers, symbols). Deploy a centralized password management system. | | **Legacy Systems Maintenance** | Ad hoc | Establish a regular maintenance schedule and document intervention methods for legacy systems. | | **Firewall** | Adequate | Regularly review and update firewall rules to address evolving threats. | | **Antivirus Software** | Adequate | Continue monitoring and updating antivirus software to address new vulnerabilities. | |

**Step 4: Key Recommendations**

1. **Address High-Priority Risks**:
   * Implement encryption for all sensitive data.
   * Establish role-based access controls.
   * Create a robust disaster recovery plan.
2. **Enhance Compliance Measures**:
   * Conduct regular audits to ensure adherence to GDPR and other regulatory requirements.
   * Train employees on compliance best practices.
3. **Strengthen IT Security**:
   * Install IDS and schedule routine penetration testing.
   * Update the password policy and enforce it using automated systems.
4. **Improve Asset Management**:
   * Centralize asset management to track and classify assets effectively.
5. **Document and Standardize Procedures**:
   * Develop clear, documented procedures for maintenance, data management, and incident response.

**Audit Conclusion**

Botium Toys has a solid foundation for IT security but faces significant risks due to weak controls and compliance gaps. Addressing these issues will improve their security posture, reduce risks, and ensure compliance with U.S. and international regulations. Implementing the above recommendations should be a priority for the IT department.