**Cybersecurity Audit Report for Botium Toys**

**Scope and Goals of the Audit**

**Scope:** The scope of this audit encompasses the entire security program at Botium Toys. This includes evaluating their assets, such as employee equipment and devices, internal network, and systems. The audit aims to review the existing assets and assess the controls and compliance practices in place.

**Goals:** The primary goals are to assess the existing assets and complete the controls and compliance checklist to determine which controls and compliance best practices need to be implemented to enhance Botium Toys’ security posture.

**Current Assets**

The IT Department manages the following assets:

* **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**

**Risk Description:** Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all the proper controls in place and may not be fully compliant with U.S. and international regulations and standards.

**Control Best Practices:** The first of the five functions of the NIST CSF is Identify. Botium Toys needs to dedicate resources to identify assets so they can be managed appropriately. Additionally, classifying existing assets and determining the impact of the loss of these assets on business continuity is crucial.

**Risk Score:** On a scale of 1 to 10, the risk score is 8, which is fairly high. This is due to a lack of controls and adherence to compliance best practices.

**Additional Comments:** The potential impact from the loss of an asset is rated as medium, primarily because the IT department does not have a clear understanding of which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all necessary controls in place and is not fully adhering to best practices related to compliance regulations that ensure critical data privacy and security. Specific details include:

* All employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not used to ensure the confidentiality of customers’ credit card information.
* Access controls related to least privilege and separation of duties have not been implemented.
* IT department ensures availability and integrated controls to ensure data integrity.
* A firewall is in place that blocks traffic based on a defined set of security rules.
* Antivirus software is installed and monitored regularly.
* No intrusion detection system (IDS) is installed.
* No disaster recovery plans or backups of critical data exist.
* A plan is in place to notify E.U. customers within 72 hours of a security breach.
* Privacy policies, procedures, and processes are enforced among IT department members and other employees.
* Existing password policy requirements are nominal and not in line with current minimum complexity requirements.
* No centralized password management system is in place.
* Legacy systems are monitored and maintained without a regular schedule.
* The physical store location has sufficient locks, CCTV surveillance, and fire detection/prevention systems.

**Control Categories and Types**

**Administrative/Managerial Controls:**

| **Control Name** | **Control Type** | **Control Purpose** |
| --- | --- | --- |
| Least Privilege | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts |
| Disaster Recovery Plans | Corrective | Provide business continuity |
| Password Policies | Preventative | Reduce likelihood of account compromise |
| Access Control Policies | Preventative | Bolster confidentiality and integrity by defining access/modification permissions |
| Account Management Policies | Preventative | Manage account lifecycle, reducing attack surface |
| Separation of Duties | Preventative | Reduce risk and impact of malicious insider or compromised accounts |

**Technical Controls:**

| **Control Name** | **Control Type** | **Control Purpose** |
| --- | --- | --- |
| Firewall | Preventative | Filter unwanted or malicious traffic |
| IDS/IPS | Detective | Detect and prevent anomalous traffic |
| Encryption | Deterrent | Provide confidentiality to sensitive information |
| Backups | Corrective | Restore/recover from an event |
| Password Management System | Preventative | Reduce password fatigue |
| Antivirus Software | Preventative | Detect and quarantine known threats |
| Manual Monitoring/Maintenance | Preventative | Identify and manage threats, risks, or vulnerabilities in legacy systems |

**Physical/Operational Controls:**

| **Control Name** | **Control Type** | **Control Purpose** |
| --- | --- | --- |
| Locks (Offices, Storefront, Warehouse) | Preventative | Limit physical access to physical assets |
| CCTV Surveillance | Detective | Monitor physical premises |
| Fire Detection/Prevention Systems | Preventative | Detect and prevent fire-related incidents |

**Controls Assessment Checklist**

| **Control** | **Yes** | **No** |
| --- | --- | --- |
| Least Privilege |  | X |
| Disaster Recovery Plans |  | X |
| Password Policies |  | X |
| Separation of Duties |  | X |
| Firewall | X |  |
| Intrusion Detection System (IDS) |  | X |
| Backups |  | X |
| Antivirus Software | X |  |
| Manual Monitoring/Maintenance for Legacy Systems | X |  |
| Encryption |  | X |
| Password Management System |  | X |
| Locks (Offices, Storefront, Warehouse) | X |  |
| CCTV Surveillance | X |  |
| Fire Detection/Prevention Systems | X |  |

**Compliance Checklist**

**Payment Card Industry Data Security Standard (PCI DSS)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| Only authorized users have access to customers’ credit card information |  | X |
| Credit card information is stored, accepted, processed, and transmitted securely |  | X |
| Implement data encryption procedures |  | X |
| Adopt secure password management policies |  | X |

**General Data Protection Regulation (GDPR)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| E.U. customers’ data is kept private/secured |  | X |
| Plan to notify E.U. customers within 72 hours of data breach | X |  |
| Ensure data is properly classified and inventoried |  | X |
| Enforce privacy policies, procedures, and processes | X |  |

**System and Organizations Controls (SOC Type 1, SOC Type 2)**

| **Best Practice** | **Yes** | **No** |
| --- | --- | --- |
| User access policies are established |  | X |
| Sensitive data (PII/SPII) is confidential/private |  | X |
| Data integrity is ensured | X |  |
| Data is available to authorized individuals |  | X |

**Recommendations**

To enhance Botium Toys' security posture and reduce risks, the following recommendations should be communicated to stakeholders:

1. **Implement Least Privilege Access Controls:**
   * Limit access to data based on job roles and responsibilities to reduce the risk of malicious insiders and compromised accounts.
2. **Develop and Implement Disaster Recovery Plans:**
   * Establish a comprehensive disaster recovery plan to ensure business continuity in case of an incident.
3. **Enhance Password Policies and Management:**
   * Update password policies to meet current complexity requirements and implement a centralized password management system to enforce these policies.
4. **Install an Intrusion Detection System (IDS):**
   * Deploy IDS to detect and respond to potential security breaches.
5. **Implement Regular Backups:**
   * Ensure regular backups of critical data to enable recovery in the event of data loss.
6. **Encrypt Sensitive Data:**
   * Implement encryption for sensitive data, including customer credit card information, to ensure data confidentiality.
7. **Regularly Monitor and Maintain Legacy Systems:**
   * Establish a regular schedule for monitoring and maintaining legacy systems to manage risks associated with out-of-date systems.
8. **Adhere to Compliance Best Practices:**
   * Ensure compliance with PCI DSS by restricting access to credit card information and implementing secure data storage and transmission practices.
   * Ensure compliance with GDPR by properly classifying and inventorying data, and consistently enforcing privacy policies.

Implementing these recommendations will significantly improve the security posture of Botium Toys, ensuring better protection of assets and compliance with relevant regulations.