## **Security audit for Botium Toys Company**

## Scope and goals of the audit

**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.

## 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 description

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of 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 will need to dedicate resources to identify assets so they can appropriately manage them. Additionally, they will need to classify existing assets and determine the impact of the loss of existing assets, including systems, on business continuity.

Controls assessment checklist

|  |  |  |
| --- | --- | --- |
| Yes | No | Control |
|  | # | Least Privilege |
|  | # | Disaster recovery plans |
|  | # | Password policies |
|  | # | Separation of duties |
| # |  | Firewall |
|  | # | Intrusion detection system (IDS) |
|  | # | Backups |
| # |  | Antivirus software |
|  | # | Manual monitoring, maintenance, and intervention for legacy systems |
|  | # | Encryption |
|  | # | Password management system |
| # |  | Locks (offices, storefront, warehouse) |
| # |  | Closed-circuit television (CCTV) surveillance |
| # |  | Fire detection/prevention (fire alarm, sprinkler system, etc.) |

**Compliance checklist**

Payment Card Industry Data Security Standard (PCI DSS)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | # | Only authorized users have access to customers’ credit card information. |
|  | # | Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment. |
|  | # | Implement data encryption procedures to better secure credit card transaction touchpoints and data. |
|  | # | Adopt secure password management policies. |

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | # | 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)

|  |  |  |
| --- | --- | --- |
| **Yes** | **No** | **Best practice** |
|  | # | 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. |

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.

# **Recommendations:**

First of all, it is recommended to develop a plan in case of a potential threat based on the recommendations of the NIST CSF.

It is recommended to study the principle of operation of the CIA TRIADA, and the basic principles of the frameworks that relate to the use of bank-cards, such as PSI DSS.

It is recommended to familiarize yourself with the principles of encryption and cryptography to reduce the risk of theft and compromise of confidential data and.

It is recommended to set up a more advanced and complex type of identification, for example, change the password system and add more special characters to reduce the risk of compromise of the password and data.

It is also recommended to limit and separate employee access from all confidential data, and minimize the amount of data for work that all employees in the company perform. For review: The principle of least privilege.

Yevhenii Moskalenko.