**[[1]](#footnote-0)BOTIUM TOYS AUDIT REPORT**

**1.0 Summary**

This internal audit aligns with industry standards and best practices. The audit is done to provide mitigation recommendations for vulnerabilities found and classified as ‘high risk’ and present an overall strategy to improve the Botium Toys security posture The Audit team has documented their findings and provided remedial efforts and plan and communicated the same to all stakeholders.

**Scope: The internal IT audit will assess the following:**

* Identify existing controls, policies and procedures
* Assess user’s permissions
* Account for technology currently in use at BOT Toys

**Goals: The goals for the internal audit are:**

* Assess existing assets
* Improve system controls
* Assess compliance effort
* Adhere to the NIST Cybersecurity framework

**2.0 RISK ASSESSMENT**

Current Asset

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 is not fully compliant with U.S. and international regulations and standards.

**Vulnerabilities and Threats:**

During the risk assessment phase, a thorough examination of Botium Toys' IT infrastructure identified a range of vulnerabilities and potential threats to the company's operations. These vulnerabilities included but were not limited to:

**Outdated Software and Hardware:** Many of the systems and software applications currently in use at Botium Toys are running outdated versions. These can expose the company to known security vulnerabilities that can be exploited by malicious actors.

**Insufficient Data Backups:** A lack of comprehensive data backup procedures was observed. In the event of data loss, there might be significant downtime and potential loss of critical information.

**Inadequate Employee Training:** Employee cybersecurity training and awareness programs appeared to be limited. This leaves the company susceptible to social engineering attacks and unintentional security breaches.

Weak Password Policies: The review also noted the absence of strong password policies, increasing the risk of unauthorized access due to weak or easily guessable passwords.

**Lack of Intrusion Detection Systems:** Botium Toys lacks robust intrusion detection systems, which makes it challenging to detect and respond promptly to potential security breaches.

**Data Access Controls:** Inadequate access controls and permissions within the organisation's network might lead to unauthorised data access and manipulation.

**Phishing and Social Engineering Risks:** The absence of comprehensive training and awareness programs increases the susceptibility of employees to phishing and social engineering attacks.

**Identified Risks:**

The vulnerabilities listed above pose significant risks to Botium Toys, potentially impacting the confidentiality, integrity, and availability of data and IT resources. The identified risks include:

Data Breaches: Outdated software and weak password policies may lead to data breaches, exposing sensitive customer information.

Operational Disruptions: Insufficient data backups and lack of intrusion detection systems may result in operational disruptions due to data loss or cyberattacks.

Regulatory Non-Compliance: Weak data access controls can lead to non-compliance with data protection regulations, especially those related to processing online payments and operating within the European Union.

Reputation Damage: Falling victim to phishing or social engineering attacks could damage the company's reputation, causing a loss of customer trust.

Financial Loss: Any of the above risks, if realised, could lead to financial losses, including potential fines and legal fees.

**3.0 Control Assessment**

### **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.

Here are the administrative controls, technical controls, and physical controls for Botium Toys with priority levels (8 being the highest priority and 1 being the lowest):

| **Administrative Control** | | | |
| --- | --- | --- | --- |
| **Control Name** | **Control Type** | **Needs to be implemented** | **Priority** |
| Security Policy and Procedures | Reduce risk and overall impact of it on the business, and reduce the likelihood of compromise | X | High: 8 |
| Employee Training and Awareness Programs | essential for enhancing the overall security posture of an organization by ensuring that employees are informed about potential risks and know how to respond to security threats and incidents. | X | 7 |
| Incident Response and Recovery Plan | provides guidance on how to mitigate the impact of incidents, such as data breaches, natural disasters, or other disruptions | X | 8 |
| **Technical Control** | | | |
| Firewalls and Intrusion Detection Systems (IDS) | To filter unwanted or malicious traffic from entering the network. Implementing and allow and deny list and to detect and prevent anomalous traffic that matches a signature or rule | X | 8 |
| Data Encryption for Online Transactions | Provide confidentiality to sensitive information such as customer PII and credit cards infromation | X | 8 |
| Regular Software Patching and Updates |  | X | 7 |
| **Physical Control** | | | |
| Access Control System (e.g., Keycard Entry) | Bolster integrity by deterring and preventing unauthorized personnel, individuals from physically accessing assets | X | 8 |
| Surveillance Cameras | Closed circuit television is both a preventative and detective control because it’s presence can reduce risk of certain types of events from occurring, and can be used after an event to inform on event conditions | X | 7 |
| Data Center Environmental Controls (e.g., Temperature and Humidity Monitoring) | Detect fire in the data centre and prevent damage to physical assets such as inventory, servers, etc. | X | 6 |

**4.0 Assessing Compliance**

**Compliance checklist**

* **Payment Card Industry Data Security Standard:**

It is a set of security standards and requirements designed to ensure the safe handling of sensitive payment card data. These standards were developed to protect cardholder data and are typically applicable to businesses and organizations that handle credit card transactions.

**Explanation:**

Botium Toys need to adhere to PCI-DSS because we accept, store, process and transmit credit card information of our customers

* **General Data Protection Regulation (GDPR)**

It is a comprehensive data protection law that was implemented by the European Union (EU) in May 2018. The GDPR replaced the Data Protection Directive 95/46/EC and introduced new rules and regulations regarding the privacy and protection of personal data of EU citizens.

**Explanation:**

Botium Toys need to adhere to GDPR because we conduct business in the european union and we collect PII fro people in the EU.

**5.0 Stakeholder Communication**

### 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, because the IT department does not know which assets would be at risk. The risk to assets or fines from governing bodies is high because Botium Toys does not have all of the necessary controls in place and is not fully adhering to best practices related to compliance regulations that keep critical data private/secure. Review the following bullet points for specific details:

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Additionally, privacy policies, procedures, and processes have been developed and are enforced among IT department members/other employees, to properly document and maintain data.
* Although a password policy exists, its requirements are nominal and not in line with current minimum password complexity requirements (e.g., at least eight characters, a combination of letters and at least one number; special characters).
* There is no centralized password management system that enforces the password policy’s minimum requirements, which sometimes affects productivity when employees/vendors submit a ticket to the IT department to recover or reset a password.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* The store’s physical location, which includes Botium Toys’ main offices, store front, and warehouse of products, has sufficient locks, up-to-date closed-circuit television (CCTV) surveillance, as well as functioning fire detection and prevention systems.

1. Olajide Usman 10-24-2023 [↑](#footnote-ref-0)