**CyberSecurity Audit Report**

Botium Toys company,

7th July 2024,

Prepared By:IT Department.

***This scenario is based on a fictional company:***

**Botium Toys is a small U.S. business that develops and sells toys. The business has a single physical location, which serves as their main office, a storefront, and warehouse for their products. However, Botium Toy’s online presence has grown, attracting customers in the U.S. and abroad. As a result, their information technology (IT) department is under increasing pressure to support their online market worldwide.**

**The manager of the IT department has decided that an internal IT audit needs to be conducted. She's worried about maintaining compliance and business operations as the company grows without a clear plan. She believes an internal audit can help better secure the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets. The manager is also interested in ensuring that they comply with regulations related to internally processing and accepting online payments and conducting business in the European Union (E.U.).**

**The IT manager starts by implementing the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), establishing an audit scope and goals, listing assets currently managed by the IT department, and completing a risk assessment. The goal of the audit is to provide an overview of the risks and/or fines that the company might experience due to the current state of their security posture.**

**Your task is to review the IT manager’s scope, goals, and risk assessment report. Then, perform an internal audit by completing a controls and compliance checklist.**

**Assets managed by the IT department**

● 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

**GOALS:**

* Identify and mitigate potential risks,threats and vulnerabilities to critical assets
* Ensure compliance with PCI-DSS and GDPR
* Improve overall security posture of the company's IT infrastructure

**SCOPE:**

Auditing the entire security program at Botium Toys including their assets like employee equipment and devices, internal network and their systems.

**RISK ASSESSMENT**

**findings**

After a thorough audit,we found out that Botium Toys does not have all of the proper controls in place and may not be fully compliant with the U.S and International regulations standards.

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.

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

**ACCESS CONTROL**

**findings:**

● 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

the 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.

**RECOMMENDATIONS**

Access control:

* Implementing the least privilege principle.
* Installing of the intrusion detection systems
* Implementing disaster recovery plans
* Ensuring the password policy meets the minimum password complexity requirements
* Introducing a centralized password management system.
* Installing CCTV surveillance and locks in the offices, storefront and warehouse.

### **Conclusion**

The audit reveals several areas for improvement in Botium Toys' cybersecurity framework. Addressing these issues will better secure the infrastructure, protect critical assets, and ensure compliance with regulatory requirements. Regular follow-up audits and continuous improvement are essential as the company grows and its online presence expands.