Cybersecurity Audit Report – Botium Toys

# Executive Summary

This project reviews the current cybersecurity posture of Botium Toys. The audit focused on assets, risks, and existing controls. Findings show that while basic protections (firewalls, antivirus, and physical security) are in place, there are critical weaknesses in data protection, access management, and recovery planning. The overall risk score is high (8/10) due to missing controls and lack of compliance with industry standards.

# Audit Scope and Goals

Scope: The entire security program of Botium Toys, including IT systems, employee devices, networks, customer data, warehouse, and physical store operations.

Goals:

1. Identify and review all assets.
2. Assess compliance with cybersecurity best practices.
3. Recommend improvements to strengthen overall security.

# Key Findings

* Unrestricted Data Access – All employees can access sensitive data, including customer credit card details.
* Lack of Encryption – Customer and payment information is stored without encryption.
* Weak Password Controls – Current policies are outdated, not enforced, and no multi-factor authentication is in place.
* No Recovery Plan – There are no backups or disaster recovery procedures for critical data.
* No Monitoring Systems – An Intrusion Detection/Prevention System (IDS/IPS) has not been deployed.
* Legacy Systems Risk – Old systems are monitored irregularly, creating vulnerabilities.
* Physical Security – Locks, CCTV, and fire prevention systems are adequate and well maintained.

# Risk Assessment

Overall Risk Score: 8/10 (High)

Potential Business Impact:

• Medium: Loss of assets could disrupt operations.

• High: Non-compliance could lead to fines, reputational damage, and customer trust issues.

# Control Categories & Gaps

Administrative (policies & procedures): Missing or outdated policies for passwords, access control, disaster recovery, and account management.

Technical (IT systems): Missing IDS/IPS, no encryption, no backups, weak authentication controls.

Physical (facilities): Adequate physical safeguards, but improvements such as a time-controlled safe for backup storage are recommended.

# Recommendations to the Business Owner

* Protect Customer Data – Encrypt all stored and transmitted customer and payment information to meet compliance requirements (e.g., PCI DSS, GDPR).
* Restrict Access – Enforce least privilege, role-based access, and separation of duties so employees only see the data they need.
* Strengthen Authentication – Update password policies, deploy centralized password management, and add multi-factor authentication (MFA).
* Plan for Recovery – Implement regular data backups and create a disaster recovery plan to ensure business continuity.
* Improve Monitoring – Deploy an IDS/IPS to detect and stop suspicious activity in real time.
* Manage Legacy Systems – Establish a monitoring and maintenance schedule, and plan for eventual replacement of outdated systems.
* Employee Training – Train staff regularly on cybersecurity best practices and reinforce awareness of policies.
* Enhance Physical Safeguards – Consider using a secure time-controlled safe for critical backup media

.

# Conclusion

Botium Toys has strong physical security and some basic IT protections, but the company faces high risk due to missing technical and administrative controls. Immediate attention is needed in areas of data encryption, access control, backup and recovery, and compliance. By implementing the recommendations outlined above, Botium Toys can reduce its exposure, safeguard customer trust, and build a more resilient cybersecurity posture.