Cybersecurity Audit Report: Botium Toys

Cybersecurity Audit Report: Botium Toys

1. Introduction

Botium Toys is a U.S.-based toy company that operates both physical retail outlets and a growing e-commerce platform. As the company expands its digital footprint to serve a broader customer base, including international markets, its reliance on technology, data systems, and online operations has increased significantly. This growth demands a strong focus on cybersecurity to protect sensitive customer information, ensure regulatory compliance, and maintain uninterrupted business operations.

Purpose of the Audit

The primary purpose of this internal cybersecurity audit is to assess the current state of Botium Toys’ IT security program, identify any vulnerabilities, evaluate risk exposure, and ensure that appropriate security controls and compliance practices are in place. This audit aims to:

- Review existing assets and infrastructure
- Evaluate the effectiveness of current security controls
- Identify non-compliance with security standards and regulations
- Provide actionable recommendations to strengthen Botium Toys’ cybersecurity posture.

Audit Framework Used (NIST CSF)

This audit is conducted using the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). NIST CSF provides a structured approach for identifying, protecting, detecting, responding to, and recovering from cybersecurity threats. It is a widely accepted framework that ensures organizations adopt industry best practices for managing and reducing cybersecurity risk.

---

2. Scope & Goals

Scope

For this audit, I looked at everything related to Botium Toys’ security setup. That includes employee devices, internal systems, network infrastructure, and any tools or software used by the company. I also reviewed their policies, access controls, and how they handle sensitive data like customer info and payments.

Goals

The goal was to spot any security risks, check how well their current controls are working, and see if they’re following key regulations like GDPR and PCI DSS. I used the NIST Cybersecurity Framework as a guide throughout the process.

---

3. Assets Reviewed

I reviewed the following key assets used by Botium Toys:

- On-premises equipment used for daily business operations in the office
- Employee devices, including desktops, laptops, smartphones, and other accessories

- Storefront and warehouse inventory, both physical and listed for online sale
- Software and services like accounting tools, security systems, ecommerce platforms, and databases
- Internal network and internet access setup and infrastructure
- Data storage systems and legacy systems still in use that require manual oversight

4. Risk Assessment Summary

Risk Score: 8/10 (High)

During the audit, I found several major security gaps that could put Botium Toys at risk:

- There's no encryption in place to protect sensitive customer data
- Access control is missing — all employees can access internal data
- There's no intrusion detection system (IDS) and no backup or disaster recovery plan
- The password policy is weak and doesn't meet current standards

These issues raise serious concerns about data security and regulatory compliance.

5. Control Checklist Summary

Control Area	Status	Recommendation
Employee access to sensitive data	❌	Apply least privilege & restrict PII access
Encryption of card data	❌	Implement AES-256 / TLS encryption
Intrusion Detection System (IDS)	❌	Install IDS like Snort or Suricata
Backup / Disaster recovery	❌	Set up and test regular backups
Password policy	⚠️	Enforce strong passwords + enable MFA
Firewall	✅	Continue monitoring and refining rules
Antivirus	✅	Keep updated and monitored
GDPR breach response	✅	Train staff and test breach response
Physical security	✅	Maintain CCTV, fire systems, and locks

6. Compliance Check

GDPR: Partially Compliant

- Staff breach notification plan is in place

- Needs stronger data access controls and better data handling policies

PCI DSS: Partially Compliant

- Currently missing encryption for cardholder data
- Secure access policies (like least privilege) still need to be implemented

7. Recommendations

Based on the audit findings, I recommend the following steps:

- Prioritize access controls and encrypt all sensitive data, especially customer and payment info
- Deploy an Intrusion Detection System (IDS) and set up a centralized password manager
- Implement regular backups and build a proper disaster recovery plan
- Review and enforce a stronger password policy, including complexity and multi-factor authentication
- Schedule periodic security audits to stay compliant and address new risks

8. Conclusion

Botium Toys needs to take immediate action to fix several critical security issues, especially around data protection and system monitoring.

By applying industry best practices—like access control, encryption, backups, and regular audits—the company can significantly reduce its legal and cybersecurity risks while building a stronger, safer environment for its operations and customers.