Internal Security Audit Report: Botium Toys

Date: June 19, 2025
Prepared by: Rhys Hill, Cybersecurity Analyst

1. Introduction

This report outlines the findings of an internal security audit for Botium Toys. As the company continues to grow its online presence, it's important to pause and check if our security defenses are keeping up. The main goal of this audit was to get a clear picture of our current security setup, identify any gaps that could put the company at risk, and create a straightforward plan to strengthen our protections.

This review was guided by the National Institute of Standards and Technology (NIST) Cybersecurity Framework, focusing on the core need to identify and protect the company's critical assets.

2. Audit Findings: A Snapshot of Our Current Security

I reviewed the company's assets, policies, and technical systems to see which security controls are in place and which are missing. Below is a summary of what I found.

Controls Checklist

This checklist answers the question: "Do we currently have this security measure in place?"

Control	In Place?	Notes
Least Privilege	No	Currently, all employees have access to all data.
Disaster Recovery Plan	No	There is no formal plan to recover from a major incident.
Password Policies	No	Although a document exists, its requirements are not enforced and fall below minimum standards, making it non-functional as a control.
Separation of Duties	No	No controls to prevent a single person from controlling a process.
Firewall	Yes	A network firewall is active

		and configured.
Intrusion Detection System	No	We are not currently monitoring the network for active threats.
Backups	No	Critical company and customer data is not being backed up.
Antivirus Software	Yes	Antivirus is installed and monitored on company devices.
Manual monitoring, maintenance, and intervention for legacy systems	No	While some monitoring occurs, it lacks a regular schedule and clear intervention procedures, making it an unreliable and incomplete control.
Encryption	No	Sensitive data, like customer credit card info, is not encrypted.
Password Management System	No	No central tool to enforce a password policy.
Physical Locks	Yes	Doors to offices, the storefront, and warehouse are secure.
CCTV Surveillance	Yes	The physical location is monitored by CCTV.
Fire Detection	Yes	Fire alarms and prevention systems are in place.

Compliance Checklist

This checklist looks at whether we're following the rules for handling sensitive data, especially for online payments (PCI DSS) and our E.U. customers (GDPR).

Compliance Best Practice	Followed?
PCI DSS: Only authorized users can access credit card data.	No
PCI DSS: Credit card data is handled in a secure environment.	No
PCI DSS: Encryption is used to protect credit card data.	No
PCI DSS: Secure password policies are adopted.	No
GDPR: E.U. customer data is kept private and secured.	No
GDPR: A plan exists to notify E.U. customers of a breach.	Yes
GDPR: Data is properly classified and inventoried.	No
GDPR: Privacy policies are enforced to protect data.	Yes

3. Discussion: What These Gaps Mean for Botium Toys

Based on the review, I rated the company's overall risk score as **8 out of 10**. This is high, and it's driven by a few critical issues. A high risk score means there is a significant chance of a security incident that could lead to financial loss, damage to our reputation, or legal fines.

Here are the three biggest concerns:

1. **Unprotected Customer Payment Information:** Right now, we are storing customer credit card details without encryption. This is our most urgent problem. It's a direct violation of the Payment Card Industry Data Security Standard (PCI DSS). If this data were stolen, it would likely result in significant fines, loss of our

ability to accept credit card payments, and a complete loss of customer trust.

2. **No Safety Net for Disasters:** We currently have no backups of our critical data and no disaster recovery plan. If a fire, flood, or a major cyberattack like ransomware happened today, we could lose everything—our accounting records, customer lists, and inventory data—with no way to get it back. This is a threat to the company's survival.
3. **Everyone Has Access to Everything:** By allowing all employees access to all company data, we are operating on trust alone. This violates a core security principle called "least privilege." It makes us very vulnerable to both accidental data leaks and intentional damage from a disgruntled employee. It also fails key requirements for both PCI DSS and GDPR.

4. Recommendations: A Plan to Secure Our Business

Here is a straightforward, prioritized plan to fix these issues. I've grouped them into three categories to show what we need to tackle first.

Priority 1: Critical (Fix These Immediately)

These issues pose a direct and immediate threat to the company.

- **Implement Access Controls:** We need to immediately ensure that only specific, authorized employees can access sensitive customer data and financial information. This involves creating user roles and restricting access based on job responsibilities.
- **Encrypt Sensitive Data:** We must encrypt the database that stores customer credit card information. This is non-negotiable for PCI DSS compliance and for protecting our customers.
- **Set Up Data Backups:** We need to implement a daily backup system for all critical business data. These backups should be stored securely and tested regularly to make sure we can rely on them in an emergency.

Priority 2: High (Address These Next)

These are significant security gaps that need to be addressed quickly to build on our critical fixes.

- **Create a Disaster Recovery Plan:** Once we have backups, we need a written plan that details, step-by-step, how we would restore our operations after a major incident.
- **Strengthen Our Password Policy:** We need to create a new password policy that meets modern standards (e.g., length, complexity) and deploy a password management tool to enforce it across the company.
- **Install an Intrusion Detection System (IDS):** This will act like a burglar alarm for

our network, actively monitoring for suspicious activity and alerting us to potential attacks in real-time.

Priority 3: Medium (Important Improvements)

These actions will strengthen the company's overall security and put formal processes in place.

- **Formalize a Maintenance Schedule:** Create a fixed schedule for checking and maintaining our legacy systems to ensure they don't become a security risk.
- **Conduct a Data Inventory:** We need to go through our systems and formally document what data we have, where it's stored, and who owns it. This is a foundational step for good data governance and GDPR compliance.

5. Conclusion

Botium Toys is at an exciting stage of growth, but our current security practices have not kept pace with the risks we now face. The issues identified in this audit are significant, but they are all fixable.

By taking decisive action and following the recommendations in this report, we can protect our customers, our reputation, and our business. I am confident that by working together, we can build a strong and resilient security foundation for the company's future.