Evan H. Yearwood

Internal Security Audit – Botium Toys

Assets, Risks, Audit, Mitigation Strategies and Impact Analysis

Context

Botium Toys is a mid-sized company that designs, manufactures, and sells toys. Their operations include an in-office headquarters where design, development, and administrative tasks are handled, a storefront for retail sales, and an adjoining warehouse for product storage and order fulfillment. The company is expanding its digital footprint through an e-commerce platform, which enables customers to purchase products online. This expansion has introduced a range of digital assets and increased the complexity of its IT infrastructure.

Given its involvement in the sale and handling of sensitive customer information (such as payment card data and personal information), Botium Toys is subject to stringent security requirements, including compliance with U.S. regulations and the European Union's GDPR, as it serves an international customer base. However, as a company undergoing growth, it has yet to fully implement many best practices and compliance standards to safeguard its assets and customer data. This audit's findings are intended to help Botium Toys strengthen its security posture, mitigate potential risks, and achieve compliance with relevant security standards to protect both the company and its customers.

1. Scope, Goals, and Assets

1.1 Scope:

The scope is defined as the entire security program at Botium Toys. All assets, physical, and network infrastructure will be assessed to identify potential vulnerabilities. Alongside the internal processes and procedures related to the implementation of controls and compliance best practices.

1.2 Goals:

Assess existing assets and complete controls and compliance checklist to determine which controls and compliance best practices need to be implemented to improve Botium Toys' Security Posture. Provide recommended mitigation strategies for found vulnerabilities.

1.3 Assets:

Assets managed by the IT Department include:

1. On-premises equipment for in-office business needs
2. Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
3. Storefront products available for retail sale on site and online; stored in the company's adjoining warehouse
4. Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
5. Internet access
6. Internal network
7. Data retention and storage
8. Legacy system maintenance: end-of-life systems that require human monitoring

2. Audit and Results

2.1 Risk Assessment Report

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.

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.

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, since 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 vulnerability bullet points for specific details:

Vulnerabilities

Low-risk | *Medium-risk* | *High-risk*

1. Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII. **10/10**

2. Encryption is currently not used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database. **10/10**
3. Access controls pertaining to least privilege and separation of duties have not been implemented. **9/10**

4. The IT department has ensured availability and integrated controls to ensure data integrity. **2/10**

5. The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules. **2/10**

6. Antivirus software is installed and monitored regularly by the IT department. **1/10**

7. The IT department has not installed an intrusion detection system (IDS). **6/10**

8. There are no disaster recovery plans currently in place, and the company does not have backups of critical data. **10/10**

9. 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. **1/10**

10. 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). **7/10**

11. 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. **6/10**

12. While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear. **5/10**

13. 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. **2/10**

2.2 Controls and Compliance Audit

Controls assessment checklist

Does Botium Toys currently have this control in place?

Yes	No	Control
☐	☑	Least Privilege
☐	☑	Disaster recovery plans
☑	☐	Password policies
☐	☑	Separation of duties
☑	☐	Firewall
☐	☑	Intrusion detection system (IDS)
☐	☑	Backups
☑	☐	Antivirus software
☐	☑	Manual monitoring, maintenance, and intervention for legacy systems
☐	☑	Encryption
☐	☑	Password management system
☑	☐	Locks (offices, storefront, warehouse)
☑	☐	Closed-circuit television (CCTV) surveillance
☑	☐	Fire detection/prevention (fire alarm, sprinkler system, etc.)

Compliance checklist

Does Botium Toys currently adhere to this compliance best practice?

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice
□	☑	Only authorized users have access to customers' credit card information.
□	☑	Credit card information is stored, accepted, processed, and transmitted internally, in a secure environment.
□	☑	Implement data encryption procedures to better secure credit card transaction touchpoints and data.
□	☑	Adopt secure password management policies.

General Data Protection Regulation (GDPR)

Yes	No	Best practice
□	☑	E.U. customers' data is kept private/secured.
☑	□	There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.
☑	□	Ensure data is properly classified and inventoried.
☑	□	Enforce privacy policies, procedures, and processes to properly document and maintain data.

System and Organizations Controls (SOC type 1, SOC type 2)

Yes	No	Best practice
☐	☑	User access policies are established.
☐	☑	Sensitive data (PII/SPII) is confidential/private.
☑	☐	Data integrity ensures the data is consistent, complete, accurate, and has been validated.
☑	☐	Data is available to individuals authorized to access it.

3. Potential Impact Analysis and Recommended Mitigation Strategies

3.1 Impact Analysis

#	Vulnerability	Risk Score	Potential Impact	Cost / Damages
1	There are no disaster recovery plans currently in place, and the company does not have backups of critical data.	10/10	In the potential event of a data breach, if systems are compromised, destroyed or encrypted the process of recovery can last several years or be impossible. Halting or ending business continuity.	Costs can be catastrophic, including regulatory fines, legal fees, remediation costs, loss of brand trust and disruption or ceasing of business continuity. *Estimated Financial Loss over 2 year* ~ **$750,000 - $2,000,000**
2	Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers' PII/SPII.	10/10	Disgruntled or exploited employees with access may steal cardholders and customers PII/SPII. Threat actors can use fewer lateral movements to breach databases.	Costs can be severe, including regulatory fines, legal fees, remediation costs, loss of brand trust and disruption in business continuity. *Estimated Financial Loss Over 2 Years ~* ***$500,000***
3	Encryption is currently not used to ensure confidentiality of customers' credit card information that is accepted, processed, transmitted, and stored locally in the company's internal database.	10/10	In the potential event of a data breach, there is no additional layer of security or control preventing threat actors from exploiting customers' PII/SPII.	Costs can be severe, including regulatory fines, legal fees, remediation costs, loss of brand trust and disruption in business continuity. *Estimated Financial Loss over 2 years ~* ***$375,000***
4	Access controls pertaining to least privilege and	9/10	Disgruntled or exploited employees with access may steal	Costs can be severe, including regulatory fines, legal fees, remediation

	separation of duties have not been implemented.		cardholders and customers PII/SPII. Threat actors can use fewer lateral movements to breach databases.	costs, loss of brand trust and disruption in business continuity. *Estimated Financial Loss Over 2 Years ~ **$500,000***
5	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).	7/10	Password spraying and brute force techniques using programs like 'John The Ripper' can easily gain access to critical user credentials, potentially resulting in a database breach or alteration of data integrity.	Cost can be severe, including regulatory fines, legal fees, and costs associated with credential recovery and system hardening post-breach, as well as potential data loss or alteration leading to operational inefficiencies. *Estimated Financial Loss Over 2 Years ~* **$300,000 - $600,000**
6	The IT department has not installed an intrusion detection system (IDS).	6/10	Without an IDS, the organization may not detect breaches in a timely manner, increasing the risk of prolonged unauthorized access and data theft.	Costs can be substantial, including potential data loss, regulatory fines, legal costs, and expenses for post-breach investigations and remediation. *Estimated Financial Loss Over 2 Years ~* **$250,000 - $500,000**
7	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.	6/10	Inefficient password management could lead to increased vulnerability to password attacks and potential security breaches. The time spent on recovering or resetting passwords can also affect productivity.	Costs can be significant, including potential data breaches due to weak password security, increased IT support workload, and reduced employee/vendor productivity. *Estimated Financial Loss Over 2 Years ~* **$150,000 - $300,000**

8	While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.	5/10	The lack of a regular schedule and clear intervention methods for legacy systems increases the risk of system failures or security breaches going undetected.	Costs can be considerable, including unexpected system downtimes, potential security incidents, and inefficiencies in maintenance. *Estimated Financial Loss Over 2 Years* ~ **$100,000 - $250,000**
9	The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.	2/10	The risk is mitigated by the firewall, which effectively blocks unauthorized traffic based on security rules. However, over-reliance on the firewall without additional layers of security could pose a risk.	Costs are minimal due to the protective measures provided by the firewall, but additional security layers may be required for comprehensive protection. *Estimated Financial Loss Over 2 Years* ~ **Minimal to Negligible**
10	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.	2/10	The risk of physical breaches or damage is mitigated due to effective locks, CCTV surveillance, and fire detection and prevention systems. However, continuous updates and maintenance are necessary.	Costs are relatively low due to robust physical security measures. Ongoing maintenance and potential upgrades may incur minimal expenses. *Estimated Financial Loss Over 2 Years* ~ **Minimal to Negligible**
11	The IT department has ensured availability and integrated controls to ensure data integrity	2/10	The risk of data loss or corruption is significantly reduced due to proactive measures in ensuring system availability and data integrity.	Costs are minimized due to the effective implementation of these controls. Future investments might be required for updates and continuous improvement.

3.2 Mitigation Recommendations - Controls

#	Vulnerability	NIST SP 800-53 Control Family	Selected Control(s)	Description/Implementation Notes
1	No disaster recovery plans; no backups of critical data	CP - Contingency Planning	CP-9 (Information System Backup), CP-10 (Information System Recovery and Reconstitution)	Implement regular data backup procedures; develop and test disaster recovery plans.
2	All employees have access to internally stored data, cardholder data, and customers' PII/SPII	AC - Access Control	AC-3 (Access Enforcement), AC-6 (Least Privilege)	Restrict data access based on roles; enforce least privilege principles.
3	No encryption for customers' credit card information	SC - System and Communications Protection	SC-28 (Protection of Information at Rest)	Encrypt sensitive data at rest using strong cryptographic methods.
4	No access controls for least privilege and separation of duties	AC - Access Control	AC-5 (Separation of Duties), AC-6 (Least Privilege)	Establish separation of duties; implement role-based access control.
5	Weak password policy	IA - Identification and Authentication	IA-5 (Authenticator Management)	Strengthen password policies; enforce complexity, change intervals, and secure management.
6	No intrusion detection system (IDS) installed	SI - System and Information Integrity	SI-4 (Information System Monitoring)	Install and configure IDS for network and system monitoring; regularly update signatures/rules.
7	Irregular monitoring and maintenance	CM - Configuration Management	CM-3 (Configuration Change Control), CM-5 (Access Restrictions for Change)	Standardize maintenance schedules; control changes and document interventions.

	of legacy systems			
8	Properly configured firewall in place	SC - System and Communications Protection	SC-7 (Boundary Protection)	Regularly review and update firewall rules; monitor firewall logs for anomalies.
9	Inefficient password management without centralized system	IA - Identification and Authentication	IA-2 (Identification and Authentication (Organizational Users))	Implement a centralized password management solution to enforce and monitor compliance.
10	Secure physical location with sufficient protective measures	PE - Physical and Environmental Protection	PE-3 (Physical Access Control), PE-6 (Monitoring Physical Access)	Regularly review and update physical security measures; ensure access control and surveillance.
11	Availability and data integrity controls in place	SC - System and Communications Protection	SC-5 (Denial of Service Protection), SC-8 (Transmission Integrity)	Continuously monitor system performance; implement redundancy and error-checking methods.
12	Established breach notification plan and privacy policies	IR - Incident Response	IR-4 (Incident Handling), IR-9 (Information Spillage Response)	Develop clear breach response protocols; maintain privacy policies in compliance with regulations.
13	Regularly monitored antivirus software	SI - System and Information Integrity	SI-3 (Malicious Code Protection)	Regularly update and monitor antivirus software; conduct periodic scans and review alerts.

Personal Notes

- I can understand the overwhelming nature of Nist RMF Step 3 - Select. After choosing the controls it can be overwhelming to see all the moving parts that go into a proper security posture.
- I can see why having effective senior leadership oversee the proper implementation, assessment, authorization and monitoring of the controls is important.
- Completing this assessment has given me a wider view of the security operations and what goes into developing and maintaining a strong security posture.