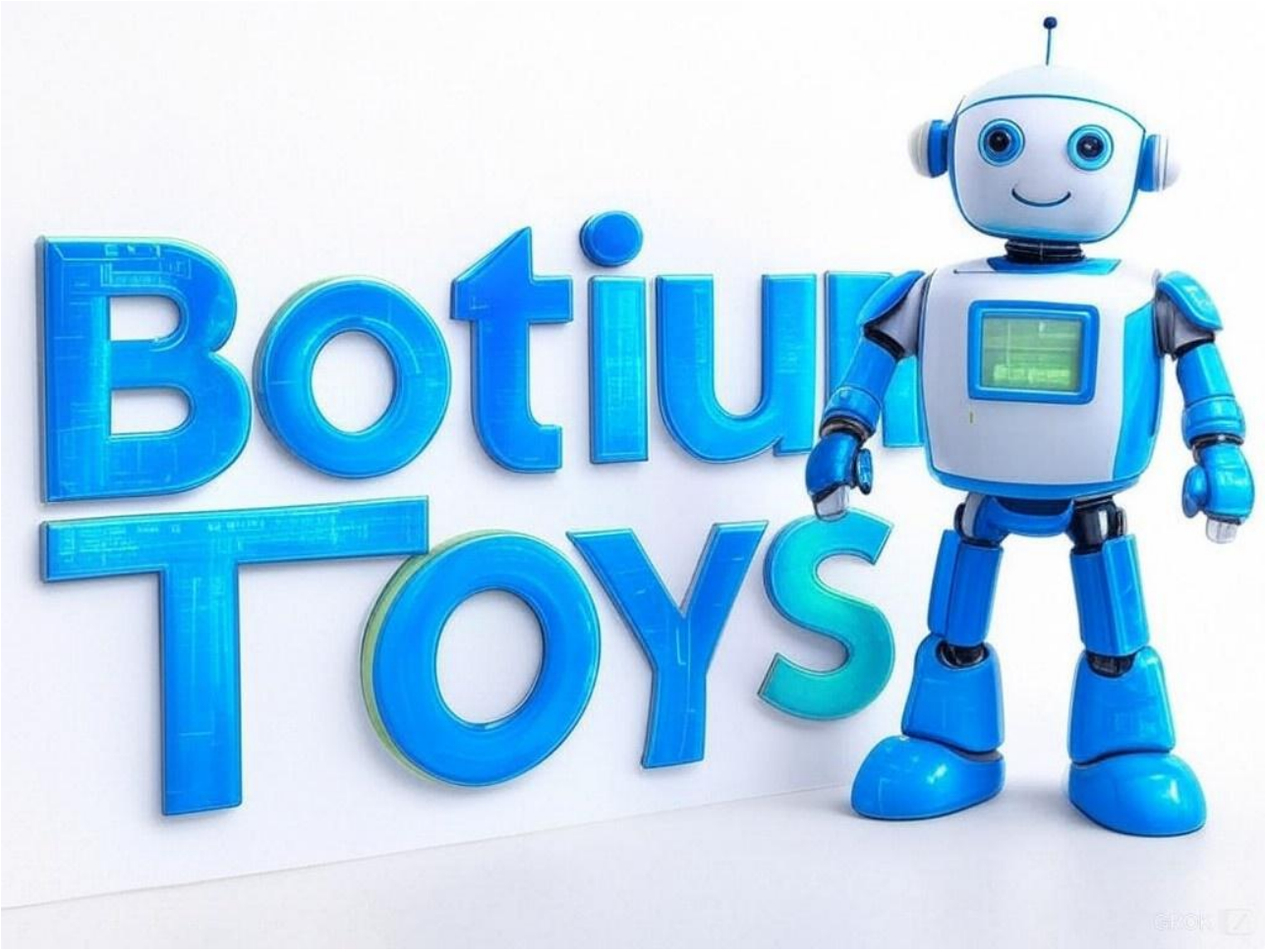
Botium Toys' Security Audit Report



Introduction

This Security Audit Report focuses on delivering the findings from an assessment conducted on January 2nd, 2025, of Botium Toys' information security environment. With the scope, goals, and risk assessment already outlined in separate documents, this report concentrates on presenting the detailed findings from our examination.

The digital threat landscape is ever-changing, making it essential for Botium Toys to continually evaluate and strengthen its cybersecurity defenses. This audit has been designed to identify specific vulnerabilities, assess compliance with established security policies, and highlight areas where security measures can be enhanced to safeguard against cyber threats.

Table of Contents:

Controls assessment checklist

Yes	No	Control	*Explanation*
	X	Least Privilege	*Currently, all employees have access to customer data; privileges need to be limited to reduce the risk of a breach.*
	X	Disaster recovery plans	*There are no disaster recovery plans in place. These need to be implemented to ensure business continuity.*
	X	Password policies	*Employee password requirements are minimal, which could allow a threat actor to more easily access secure data/other assets via employee work equipment/the internal network.*
	X	Separation of duties	*Needs to be implemented to reduce the possibility of fraud/access to critical data, since the company CEO currently runs day-to-day operations and manages the payroll.*
X		Firewall	*The existing firewall blocks traffic based on an appropriately defined set of security rules.*
	X	Intrusion detection system (IDS)	*The IT department needs an IDS in place to help identify possible intrusions by threat actors.*
	X	Backups	*The IT department needs to have backups of critical data, in the case of a breach, to ensure business continuity.*
X		Antivirus software	*Antivirus software is installed and monitored regularly by the IT department.*
	X	Manual monitoring, maintenance, and intervention for legacy systems	*The list of assets notes the use of legacy systems. The risk assessment indicates that these systems are monitored and maintained, but there is not a regular schedule in place for this task and procedures/ policies related to intervention are unclear, which could place these systems at risk of a breach.*
	X	Encryption	*Encryption is not currently used; implementing it would provide greater confidentiality of sensitive information.*

	X	Password management system	*There is no password management system currently in place; implementing this control would improve IT department/ other employee productivity in the case of password issues.*
X		Locks (offices, storefront, warehouse)	*The store's physical location, which includes the company's main offices, store front, and warehouse of products, has sufficient locks.*
X		Closed-circuit television (CCTV) surveillance	*CCTV is installed/functioning at the store's physical location.*
X		Fire detection/prevention (fire alarm, sprinkler system, etc.)	*Botium Toys' physical location has a functioning fire detection and prevention system.*

Actionable Insights:

To fortify cybersecurity, enforcing least privilege access, developing disaster recovery plans, and enhancing password policies are essential. These measures prevent unauthorized access, ensure business continuity, and protect against data breaches. Implementing separation of duties and regular backups further safeguards against internal fraud and data loss. Encryption, intrusion detection, and updated firewalls are crucial for data integrity and network security. A password management system and robust physical security measures, including CCTV, protect against both digital and physical threats, ensuring comprehensive security. Neglecting these could lead to severe data breaches, financial loss, and operational downtime, jeopardizing the business's reputation and legal standing.

Compliance checklist

Payment Card Industry Data Security Standard (PCI DSS)

Yes	No	Best practice	*Explanation*
	X	Only authorized users have access to customers' credit card information.	*Currently, all employees have access to the company's internal data.*
	X	Credit card information is accepted, processed, transmitted, and stored internally, in a secure environment.	*Credit card information is not encrypted and all employees currently have access to internal data, including customers' credit card information.*
	X	Implement data encryption procedures to better secure credit card transaction touchpoints and data.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
	X	Adopt secure password management policies.	*Password policies are nominal and no password management system is currently in place.*

Actionable Insights:

To adhere to the Payment Card Industry Data Security Standard (PCI DSS), it's imperative to restrict access to customer credit card information to only authorized personnel, currently a risk as all employees have access. Encrypting credit card data during acceptance, processing, transmission, and storage is crucial for security, yet currently, this data is not encrypted, exposing it to potential breaches. Implementing encryption for credit card transactions at all touchpoints is vital for maintaining data confidentiality, which is not currently practiced. Lastly, adopting secure password management policies and systems is essential for safeguarding access to sensitive data, an area where current practices are inadequate. Failure to address these could lead to data breaches, financial penalties, and loss of customer trust, highlighting the urgent need for compliance with PCI DSS standards to protect both the business and its customers.

General Data Protection Regulation (GDPR)

Yes	No	Best practice	*Explanation*
	X	E.U. customers' data is kept private/secured.	*The company does not currently use encryption to better ensure the confidentiality of customers' financial information.*
X		There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach.	*There is a plan to notify E.U. customers within 72 hours of a data breach.*
	X	Ensure data is properly classified and inventoried.	*Current assets have been inventoried/listed, but not classified.*
X		Enforce privacy policies, procedures, and processes to properly document and maintain data.	*Privacy policies, procedures, and processes have been developed and enforced among IT team members and other employees, as needed.*

Actionable Insights:

To comply with the General Data Protection Regulation (GDPR), it is essential to encrypt E.U. customers' data to ensure privacy, which is currently lacking as encryption is not used. Having a plan to notify E.U. customers of data breaches within 72 hours is a step in the right direction, but proper data classification and inventory are still needed, as current assets are listed but not categorized. Additionally, enforcing comprehensive privacy policies and procedures is crucial for secure data handling, an area well-addressed with developed and enforced policies among the IT team. Non-compliance could lead to severe penalties, loss of customer trust, and legal repercussions, emphasizing the need for immediate action to align with GDPR requirements for data security and privacy.

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

Yes	No	Best practice	*Explanation*
	X	User access policies are established.	*Controls of Least Privilege and separation of duties are not currently in place; all employees have access to internally stored data.*
	X	Sensitive data (PII/SPII) is confidential/private.	*Encryption is not currently used to better ensure the confidentiality of PII/SPII.*
X		Data integrity ensures the data is consistent, complete, accurate, and has been validated.	*Data integrity is in place.*
	X	Data is available to individuals authorized to access it.	*While data is available to all employees, authorization needs to be limited to only the individuals who need access to it to do their jobs.*

Actionable Insights:

To align with System and Organization Controls (SOC) standards, it's critical to establish and enforce user access policies to ensure least privilege and separation of duties, which are currently absent, allowing all employees access to sensitive data. Encrypting sensitive data (PII/SPII) is necessary for privacy, which is not currently practiced. Data integrity, ensuring data is consistent, accurate, and validated, is in place, which is positive. However, data availability needs enhancement to ensure access is appropriately authorized, not universally available. Non-compliance with these controls could lead to data breaches, operational inefficiencies, and loss of stakeholder trust, underlining the urgency for implementing robust access controls, encryption, and authorization protocols to meet SOC compliance.

Strategic Recommendations

To enhance Botium Toys' security and compliance posture, it's recommended that the company implement a multifaceted strategy focusing on access control, data protection, and compliance adherence. This includes enforcing strict access controls through the principle of Least Privilege to minimize unauthorized access, developing robust disaster recovery plans to ensure operational continuity, and strengthening password policies alongside implementing a secure password management system. Further, ensuring separation of duties, particularly in financial operations, will mitigate risks of fraud. Installing an Intrusion Detection System (IDS) will provide early threat detection, while regular maintenance and monitoring of legacy systems will safeguard against vulnerabilities.

Additionally, encrypting all sensitive data enhances confidentiality, and classifying and inventorying data assets will aid in understanding what needs protection under regulations like GDPR. Adopting secure data sharing and access policies ensures that sensitive information is available only to those who absolutely need it, enhancing data security. The company should also focus on reviewing and updating firewall configurations and network security rules regularly to adapt to new threats, ensuring robust protection against external attacks. This comprehensive approach will not only improve Botium Toys' cybersecurity but also align with regulatory compliance standards, thereby protecting both its operations and its customers' data effectively.