Botium Toys: Audit scope and goals

Summary: Perform an audit of Botium Toys' cybersecurity program. The audit needs to align current business practices with industry standards and best practices. The audit is meant to provide mitigation recommendations for vulnerabilities found that are classified as "high risk," and present an overall strategy for improving the security posture of the organization. The audit team needs to document their findings, provide remediation plans and efforts, and communicate with stakeholders.

Botium Toys: Risk assessment

Current assets

Assets managed by the IT Department include:

- On-premises equipment for in-office business needs
- Employee equipment: end-user devices (desktops/laptops, smartphones), remote workstations, headsets, cables, keyboards, mice, docking stations, surveillance cameras, etc.
- Management of systems, software, and services: accounting, telecommunication, database, security, ecommerce, and inventory management
- Internet access
- Internal network
- Vendor access management
- Data center hosting services
- Data retention and storage
- Badge readers
- Legacy system maintenance: end-of-life systems that require human monitoring

Controls assessment

Administrative Controls			
Control Name	**Control type and explanation**	**Needs to be implemented (X)**	**Priority**
Least Privilege	Preventative; reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs	X	High
Disaster recovery plans	Corrective; business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment (air conditioning, power supply, etc.); hardware (servers, employee equipment); connectivity (internal network, wireless); applications (email, electronic data); data and restoration	X	High

Password policies	Preventative; establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques	X	High
Access control policies	Preventative; increase confidentiality and integrity of data	X	High
Account management policies	Preventative; reduce attack surface and limit overall impact from disgruntled/former employees	X	High
Separation of duties	Preventative; ensure no one has so much access that they can abuse the system for personal gain	X	High

Technical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented**	**Priority**

		(X)	
Firewall	Preventative; firewalls are already in place to filter unwanted/malicious traffic from entering internal network	NA	NA
Intrusion Detection System (IDS)	Detective; allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly	X	High
Encryption	Deterrent; makes confidential information/data more secure (e.g., website payment transactions)	X	High
Backups	Corrective; supports ongoing productivity in the case of an event; aligns to the disaster recovery plan	X	High
Password management system	Corrective; password recovery, reset, lock out notifications	X	Medium
Antivirus (AV) software	Corrective; detect and quarantine known threats	X	High
Manual monitoring,	Preventative/corrective; required for legacy systems to identify and mitigate	X	High

maintenance, and intervention	potential threats, risks, and vulnerabilities		

Physical Controls			
Control Name	**Control type and explanation**	**Needs to be implemented** **(X)**	**Priority**
Time-controlled safe	Deterrent; reduce attack surface/impact of physical threats	X	Medium
Adequate lighting	Deterrent; limit “hiding” places to deter threats	X	Low
Closed-circuit television (CCTV) surveillance	Preventative/detective; can reduce risk of certain events; can be used after event for investigation	X	Medium

Locking cabinets (for network gear)	Preventative; increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear	X	High
Signage indicating alarm service provider	Deterrent; makes the likelihood of a successful attack seem low	X	Low
Locks	Preventative; physical and digital assets are more secure	X	High
Fire detection and prevention (fire alarm, sprinkler system, etc.)	Detective/Preventative; detect fire in the toy store's physical location to prevent damage to inventory, servers, etc.	X	Low

Compliance checklist

X General Data Protection Regulation (GDPR)

GDPR is a European Union (E.U.) general data regulation that protects the processing of E.U. citizens' data and their right to privacy in and out of E.U. territory. Additionally, if a breach occurs and a E.U. citizen's data is compromised, they must be informed within 72 hours of the incident.

Explanation: Assuming that Botium Toys conducts business in the EU region with customers that derive from the EU. The company must adhere to the GDPR and ensure the personal data of their EU customers are protected. In addition, they also must inform EU customers if their data is compromised within the 72 hour timeframe.

X Payment Card Industry Data Security Standard (PCI DSS)

PCI DSS is an international security standard meant to ensure that organizations storing, accepting, processing, and transmitting credit card information do so in a secure environment.

Explanation: Assuming that Botium Toys conducts online transactions on their websites/domains. The organization is obligated to adhere to the PCI DSS standard to ensure that customer's credit card data and information are being managed and stored correctly. If this standard is not being met, the organization may face severe financial implications if a data breach were to occur.

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

The SOC1 and SOC2 are a series of reports that focus on an organization's user access policies at different organizational levels. They are used to assess an organization's financial compliance and levels of risk. They also cover confidentiality, privacy, integrity, availability, security, and overall data safety. Control failures in these areas can lead to fraud.

Explanation: Though Botium Toys is a toy corporation and is not directly related to the financial industry. With the assumption that Botium Toys has an online presence and conducts business through online transactions, they may be in possession of customer's PII (Name, phone #, etc.) and SPII (credit card #). Therefore, Botium Toys should adhere to these standards to assure to their clients and customers that they are exercising every possible method to ensure their data is secure.

TO: IT Manager, Stakeholder
FROM: Arthur Sahertian
DATE: 5/22/2023
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,

This email is regarding the Botium Toys internal audit that was conducted on 5/22/2023. Please review the following information regarding the internal audit's scope, goals, critical findings, summary and recommendations.

Scope:

The internal audit will primarily focus on aspects regarding the following Botium Toys' systems: (accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool). The audit will review the current procedures, user permissions, controls and protocals that are in place to ensure they are meeting the compliance requirements. In addition, the audit will also review all technologies, both hardware and software that are being utilized in the companies everyday operations, to ensure they are all accounted for.

Goals:

The aim of the audit is to meet specific goals and standards to ensure Botium Toys are adhering to specific security frameworks such as the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF). The audit will review the current controls and ensure that Botium Toys is operating in a manner that complies with specific national/international regulations, such as PCI DSS and GDPR. This is done to avoid unnecessary fines and non-compliance issues in the future. In addition the audit will also aim to include an implementation of the least permission principle in their current systems, to reduce the surface area of potential cyber attacks.

Critical findings:

A glaring issue that Botium Toys needs to address immediately is regarding to their management of assets. Management of asset controls refer to controls that protect an organizations important assets such as access control policies, encryption of data, having an incidence response plan (playbook) etc. This inadequacy of controls results in Botium toys failing to meet specific standards and compliance regulations, which can lead to a number of legal and financial penalties.

Botium Toys needs to reassess their current controls in all domains (administrative,technical, physical) to ensure they are complying with the standards and procedures laid out in relevant regulations such as the PCI DSS and the GDPR.

The following controls are recommended to be developed to meet audit goals:

- Control of Least Privilege and Separation of Duties
- Password, access control, and account management policies, including the implementation of a password management system
- Encryption (secure web transactions)
- IDS
- AV software

- CCTV
- Locking cabinet
- Manual monitoring, maintenance, and intervention for legacy system

Additionally, the audit also revealed that Botium Toys is lacking a backup plan if things were to go awry. Every organization is recommended to have a contingency plan in case specific assets were to become unavailable, to ensure the continuity business operations can return to normal as soon as possible.

The following controls are recommended for developing a continuation plan:

- Disaster recovery plan
- Creating backups

Findings:

On a scale of 1 to 10 on the risk score scale, Botium Toys scored an 8 which is a cause for concern. This highscore is largely due in part to the lack of necessary controls and adherence to the necessary compliance regulations and standards.

A number of physical controls such as implementing adequate lighting, time-lock safe and alarm warning signange are also recommended to provide detterence for potential insider threaths, but in comparisson to the other controls, it is of least importance.

Summary:

Internal audits are important part of an organziations success, Conducting these audits will provide an organization with some insight on the current policies in place and assess improvements and changes that can be made to improve their operations from a security standpoint. The audit revealed a number of vulnerabilities with Botium Toy's security posture and the need for additional controls to be implemented, specifically regarding the management of assets. An inadequate amount of controls in this area means the organization has failed to meet the minimal requirements to be in accordance with specific national and international regulations. This can be catastrophic for any organization and addressing these issues should be of the upmost importance. Recommendations of controls has been provided to improve the overall security portfolio of Botium Toys and it is highly advised that these be applied with the upmost urgency.