ARAIZ NAQVI

SECURITY AUDIT

BOTIUM TOYS INC.

25TH SEPTEMBER, 2024

2024-2025

ARAIZ NAQVI

TABLE OF CONTENT

2024-2025

ARAIZ NAQVI

DISCLAIMER

This audit is a project-based simulation for the fictional organization Botium Toys, as part of the "Fundamentals of Cybersecurity" course on Google's Coursera platform.

While the details may resemble real-world scenarios, all data, systems, and findings are entirely fictitious and created for educational purposes. This audit does not reflect any actual incidents or vulnerabilities affecting any real organization, including BOTIUM TOYS Inc.

Though based on NIST and OWASP frameworks, the assessments are conducted in a simulated environment and should not be considered representative of any real entity's security posture.

2024-2025

ARAIZ NAQVI

EXECUTIVE SUMMARY

Date of Audit: 25th September, 2024

Organization: Botium Toys, Inc

Auditor(s): Araiz Naqvi

Purpose of Audit: To ensure that Botium Toys, Inc. has implemented effective security controls and is in compliance with relevant security regulations.

Scope of Audit: The audit covers the entire security program at Botium Toys, Inc., including all assets such as employee equipment, devices, internal networks, and systems.

Goal of Audit: Assess existing assets and complete the controls and compliance checklist to identify necessary improvements for enhancing Botium Toys' security posture.

ARAIZ NAQVI

ASSESSMENT OVERVIEW

Current Assets

- 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.
- Storefront products available for retail sale on site and online stored in the company’s adjoining warehouse.
- Management of systems, software, and services: accounting, telecommunication, database, security, e-commerce, and inventory management.
- Internet access.
- Internal network
- Data retention and storage.
- Legacy system maintenance: end-of-life systems that require human monitoring.

2024-2025

ARAIZ NAQVI

RISK ASSESSMENT

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.

Risk Description

Currently, assets are being managed inadequately. Additionally, Botium Toys does not have all the proper controls in place and may not fully comply with U.S. and International regulations and standards.

The next page includes checklists offering an overview of security control implementation and compliance with security regulations (Please Turn Over).

ARAIZ NAQVI

Does Botium Toys currently have this control in place?

Controls assessment checklist

Yes	No	Control
☐	■	Least Privilege
☐	■	Disaster recovery plans
■	☐	Password policies
☐	■	Separation of duties
■	☐	Firewall
☐	■	Intrusion detection system (IDS)
☐	■	Backups
■	☐	Antivirus software
☐	■	Encryption
☐	■	Password management system
■	☐	Locks (offices, storefront, warehouse)
■	☐	CCTV surveillance
■	☐	Fire detection/prevention

Does Botium Toys currently adhere to this compliance best practice?

Payment Card Industry Data Security Standard (PCI DSS)

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

ARAIZ NAQVI

General Data Protection Regulation (GDPR)

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

ARAIZ NAQVI

RISK CLASSIFICATION

Security Risks are classified based on their impact on Organization operations, Finances, and Reputation in case of a data breach or compromise.

High Security Risk

Information protected by law if compromised can cause severe Financial, Operational and Reputational Damage to the organisation.

Medium Security Risk

Information that's not publicly available, can affect reputation, halt operations and cause financial damage.

Low Security Risk

Information that is publicly available and has very little to no impact on reputation, operations and finances of the organisation.

2024-2025

High Security Risk

- Absence of Least Privilege.
- Open Access to PII and SPII.
- Lack of Encryption on sensitive data.
- No Intrusion Detection System.
- No Intrusion Prevention System.
- Absence of Asset Inventory/Knowledge.
- Lack of compliance with US and International Law.

Impact on Organisation and Recommendations

1. ***Absence of Least Privilege***

The absence of a least privilege policy increases the risk of unauthorized access to sensitive data and systems, potentially leading to data breaches and insider threats.

Implementing a least privilege policy and conducting regular access reviews can ensure users only have the access necessary for their job functions.

2. **Absence of Least Privilege**
Open access to personally identifiable information (PII) and sensitive personally identifiable information (SPII) raises the likelihood of data breaches, resulting in financial penalties and reputational damage.

Educating employees on the importance of data protection and establishing clear access controls can significantly reduce risks, complemented by tools like Symantec Data Loss Prevention.

3. ***Lack of Encryption on Sensitive Data***
Without encryption on sensitive data, there is a heightened risk of interception during transmission and storage, making it easier for attackers to exploit this information.
Implementing a strong encryption policy and utilizing tools like VeraCrypt can ensure sensitive data is encrypted both at rest and in transit.

4. ***No Intrusion Detection System (IDS)***
The lack of an intrusion detection system increases the risk of undetected intrusions and attacks, potentially leading to data loss or system compromise.
Deploying Cisco Firepower for robust monitoring is essential, but regular training for IT staff on threat detection is equally important for enhancing overall security.

5. ***No Intrusion Prevention System (IPS)***
Not having an intrusion prevention system leaves the organization vulnerable to attacks as there are no proactive measures to block identified threats. Installing Palo Alto Networks can actively monitor and block potential threats while developing incident response protocols can enhance the organization's ability to respond to incidents.

6. ***Absence of Asset Inventory/Knowledge***
The absence of asset inventory compromises the organization's ability to manage and secure its assets effectively, leading to vulnerabilities and compliance issues.
Establishing a regular process for asset discovery and using SolarWinds for tracking can create a comprehensive asset inventory that is routinely updated.

7. ***Lack of Compliance with US and International Law***
Failure to comply with US and international regulations can result in legal penalties and reputational damage.
Conducting compliance audits with tools like OneTrust is beneficial, but fostering a culture of compliance through employee training and awareness programs is crucial for ongoing adherence to legal requirements.

Medium Security Risk

- Absence of Disaster Recovery Plans.
- No Backup was found.
- Password Policy does not meet Complexity Standards.
- No Centralized Password Management System.
- Irregular Monitoring of Legacy Systems.

Impact on Organisation and Recommendations

1. ***Absence of Disaster Recovery Plans***

The absence of disaster recovery plans can leave the organization unprepared for unexpected events, leading to prolonged downtime and data loss. Developing and regularly updating a comprehensive disaster recovery plan, along with conducting regular training and drills for employees, can significantly enhance preparedness.

2. ***No Backups Found***

The lack of regular backups increases the risk of permanent data loss due to system failures or cyber incidents.
Implementing a structured backup policy that includes automated backups using solutions like Acronis or Veeam can ensure data is consistently backed up. Regularly training staff on backup processes can further reinforce its importance.

3. ***Password Policy Does Not Meet Complexity Standards***

A weak password policy increases the likelihood of unauthorized access through easily guessable passwords.
Strengthening the password policy to enforce complexity requirements and conducting training sessions for employees on creating strong passwords can enhance security.
Consider using a tool like LastPass or 1Password to help users manage complex passwords.

4. No Centralized Password Management System
The absence of a centralized password management system can lead to password fatigue, resulting in insecure practices.
Implementing a centralized password management solution like Dashlane can streamline password management and improve security.
Additionally, educating employees on the benefits of using such systems can foster better password practices.

5. ***Irregular Monitoring of Legacy Systems***
Irregular monitoring of legacy systems increases vulnerabilities and can lead to security breaches.
Establishing a regular monitoring schedule for these systems, combined with tools like Nagios or ManageEngine, can help identify issues promptly.
Training IT staff on the importance of consistent monitoring can further mitigate risks associated with legacy systems.

CONCLUSION

The identified security risks and corresponding recommendations align with the weaknesses and vulnerabilities uncovered to date.

By implementing these measures, the organization can effectively realign itself with various NIST, OWASP, and CISSP frameworks and controls, thereby enhancing its resilience against potential breaches.

It is important to note that the identification of undiscovered risks will be an ongoing process.

Additionally, adherence to these recommendations will ensure compliance with US and international laws.

ABOUT ME :)

Hello, I'm Araiz Naqvi! I've delved into the world of machine learning and explored the fascinating terrain of AI. However, my growing concerns about the security risks posed by this rapidly advancing technology led me to transition into cybersecurity.

To my surprise, I've discovered a genuine enthusiasm for this field, one that I never anticipated! I recall telling a friend how I could never see myself working in cybersecurity. But look at me now, diving into the basics and embracing the idea that to learn something new, you often have to start from scratch. I'm immersing myself in the essentials of networking, the Linux system, and the frameworks and controls that underpin cybersecurity.

And the journey doesn't stop here! I'm excited to pursue further education in this field in Australia. So, Australia, here I come!