# Botium Toys security audit

**SCOPE**

The internal security audit of Botium Toys will assess the following systems: existent user permissions, existing system controls, ongoing procedures and protocols in accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool. Including the alignment with PCI DSS, GDPR and compliance requirement.

**GOALS**

The goals of the internal security audit are the following ones: to base the security posture adhering to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF), to build a good security posture based on the compliance, reinforce system controls, establish policies and procedures including playbooks.

**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.
* 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, ecommerce and inventory management
* Internet access
* Internal network
* Data retention and storage
* Legacy system maintenance: end-of-life systems that require human monitoring

**RISK ASSESMENT**

***Risk description***

Currently, there is inadequate management of assets. Additionally, Botium Toys does not have all of the proper controls in place and may not be 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.

The potential impact from the loss of an asset is rated as medium, because 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 bullet points for specific details:

* Currently, all Botium Toys employees have access to internally stored data and may be able to access cardholder data and customers’ PII/SPII.
* Encryption is not currently used to ensure confidentiality of customers’ credit card information that is accepted, processed, transmitted, and stored locally in the company’s internal database.
* Access controls pertaining to least privilege and separation of duties have not been implemented.
* The IT department has ensured availability and integrated controls to ensure data integrity.
* The IT department has a firewall that blocks traffic based on an appropriately defined set of security rules.
* Antivirus software is installed and monitored regularly by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans currently in place, and the company does not have backups of critical data.
* 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.
* 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).
* 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.
* While legacy systems are monitored and maintained, there is no regular schedule in place for these tasks and intervention methods are unclear.
* 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.

**CONTROL ASSESMENT CHECKLIST**

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

***Compliance checklist***

Payment Card Industry Data Security Standard (PCI DSS)

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

General Data Protection Regulation (GDPR)

|  |  |  |
| --- | --- | --- |
| Yes | No | Best Practice |
|  | X | E.U. customers’ data is kept private/secured. |
| X |  | There is a plan in place to notify E.U. customers within 72 hours if their data is compromised/there is a breach. |
|  | X | Ensure data is properly classified and inventoried. |
|  | X | 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 |
|  | X | User access policies are established. |
|  | X | Sensitive data (PII/SPII) is confidential/private. |
| X |  | Data integrity ensures the data is consistent, complete, accurate, and has been validated. |
|  | X | Data is available to individuals authorized to access it. |

**CONTROL CATEGORIES ASSESSMENT**

**Administrative Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| Control Name | Type | Purpose | 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 | High |
| Disaster Recovery plans | Corrective | There are no disaster recovery plans, they have to implement then in order to ensure business continuity | High |
| Password policies | Preventative | They have to establish password strength rules for them to improve security of account compromise | High |
| Separation of duties | Preventative | Reduce the amount of access different people have so they can’t abuse the system for personal gain | High |
| Access control policies | Preventative | To increase confidentiality and the integrity of the data | High |
| Account management policies | Preventative | Reduce the surface in case of an attack happening and limits overall impact from former employees | High |

**Technical Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| Control Name | Type | Purpose | Priority |
| Intrusion Detection System (IDS) | Detective | Allows to identify non-wanted intrusions in the system | High |
| Encryption | Deterrent | Changes normal info/data into a more secure and protected data, for example website payment transactions | High |
| Password management system | Corrective | To recover passwords, resets and lockout notifications | High |
| Backups | Corrective | Supports the current productivity in the case of an event | High |
| Firewall | Preventative | They are already in place to prevent and filter malicious traffic from entering the internal network | N/A |
| Antivirus software (AV) | Corrective | Detects and isolates identified threats | High |
| Manual monitoring, maintenance and intervention | Preventative and corrective | There isn’t a regular schedule to do this task even if it is monitored and they have to identify and mitigate potential threats and risks to do so | High |

**Physical Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| Control Name | Type | Purpose | Priority |
| Closed-circuit television surveillance (CCTV) | Preventative and detective | Can be used for investigation and usually prevents from events happening | Medium |
| Locks | Preventative | So the physical and digital assets are more secure for unwanted people | High |
| Fire detection and prevention | Detective and preventative | Identifies the fire and protects the store to prevent damage to the assets | Medium |
| Signage alarm service provider | Deterrent | Stopping threats by making the probabilities of a successful attack seem low | Low |
| Time-controlled safe | Deterrent | Reducing the surface of attack from physical threats | Low |
| Adequate lighting | Deterrent | Limiting hiding places in the store | Medium |
| Locking cabinets for network gear | Preventative | Preventing unauthorized access to this gear | High |

**RECOMMENDATIONS AND FINDINGS**

The audit revealed some findings in every area and some of them must be addressed immediately. For example, the principles of least privilege and separation of duties must be implemented as fast as they could, in that way they could lower the risk of a breach and in case that happens, the field of attack will be smaller. They need to implement a password management system, antivirus software and manual monitoring for legacy systems. Enhance physical controls through closed circuit television surveillance, locks and locking cabinets in the store.

It has to be a priority to address the gaps or lack of compliance related exclusively to GDPR and PCI DSS. It would be helpful using the SOC1 and SOC2 guides to secure user access policies and data or info safety. Implementing easy-going disaster recovery plans and regularly make and check the backups for business continuity. Something that must be addressed would be the fact that integrating intrusion detection systems and updating antivirus software would help to this company’s security posture. Finally, they must implement powerful encryption processes to make sure that the data containing PII and SPII shouldn’t be compromised.