**Botium Toys Internal Audit (Fictitious Company Auditing Exercise)**

Summary: Perform an internal audit of Botium Toys’ cybersecurity program. The audit will need to align with the current business model and industry standards. The purpose of the audit is to provide mitigation strategies for vulnerabilities classified as high risk and present a framework for improving the security posture of the organization. The audit team will document findings, provide remediation recommendations, and communicate with stakeholders.

Scope: The Botium Toys internal audit will assess the following:

* Current user permissions are set in the following systems: accounting, end point detections, firewalls, intrusion detection system, security information and event management tool.
* Curent implemented controls in the following systems: accounting, end point detections, firewalls, intrusion detection system, security information and event management tool.
* Current procedures and protocols in the following systems: accounting, end point detections, firewalls, intrusion detection system, security information and event management tool.
* Ensure current user permissions, controls, procedures, and protocols align with compliance requirements.
* Ensure current technology is accounted for including hardware and system access.

Goals: The goals for the Botium Toys’ internal audit are:

* To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
* Establish a better process for their systems to ensure they are compliant.
* Fortify system controls.
* Implement the concept of least permission to user credential management.
* Establish their policies and procedures including their playbooks.
* Ensure the meeting of compliance requirements.

Current assets: Assets managed by the IT department include the following:

* On premises equipment for office business needs.
* Employee equipment includes end-user devices such as desktops, laptops, and smartphones, remote workstations, headsets, cables, keyboards, mice, docking stations, and surveillance cameras.
* Management of systems, software, and services: accounting, telecommunications, 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.

Risk Description: Currently, there is inadequate management of assets, Additionally, Botium Toys does not have proper controls in place and may not be compliant with U.S. and international regulations and standards.

Control best practices: The first of the five functions of the NIST CSF are Identify. Botium Toys will need to dedicate resources to managing assets. Additionally, they will need to determine the impact of the loss of existing assets, including systems on the business continuity.

Risk Score: On a scale of 1 to 10, the risk score is 8 which is high. This is due to a lack of controls and adherence to necessary compliance regulations and standards.

Additional comments: Several critical issues require immediate attention:

* 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 in current use to ensure confidentiality of customer credit card information that is accepted, processed, transmitted, and stored in the company 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 appropriate defined set of security rules.
* Antivirus software is installed and monitored by the IT department.
* The IT department has not installed an intrusion detection system (IDS).
* There are no disaster recovery plans in place including no backups for critical data.
* The IT department has established a plan to notify E.U. customers within 72 hours if there is a security breach. Privacy policies, procedures, and processes have been developed and enforced among the IT department and other employees to properly document and maintain data.
* Password policy exists but requirements are not in line with current minimum password complexity needs which includes at least eight characters, a combination of letters and at least one number, and one special character.
* There is no centralized password management system that enforces the password policy minimum requirements which affects productivity when employees submit a ticket to the IT department to recover or reset a password.
* Legacy systems are monitored and maintained but there is no regular schedule in place for these tasks and intervention methods are unclear.
* Physical locations which include Botium Toys’ main offices, store front, warehouse has sufficient locks, an up-to-date CCTV surveillance systema and a functioning fire detection and prevent system.

**Administrative Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Name** | **Type & Explanation** | **Implementation Currently Yes/No** | **Priority** |
| Least Privilege | Preventative.  Reduce risk as each staff member will only have access to assets/data needed to perform job. | No. Currently all employees have access to data. Privileges need to be restricted. | High |
| Disaster Recovery Plans | Corrective.  To ensure business systems continue during an incidental event with limited loss of productivity and downtime to system components including computer rooms, hardware, internal wireless network, email, and data. | No. Currently no disaster recovery plan is in place. These need to be implemented to protect business downtime during an event and to backup critical data. | Medium |
| Password Policies | Preventative.  Establish password strength rules to improve security and reduce account compromise. | No. Currently password policies are minimal and do not follow current minimum password complexity requirements. Improving password policy will prevent a threat actor to easily access important data. | High |
| Access Control Policies | Preventative.  Increase confidentiality and integrity of data. | No. Currently there is no access control policy in place as all employees have access to internally stored data and may access customer SPII/PII. | High |
| Account Management Policies | Preventative.  Reduce attack surface and limit impact from disgruntled and former employees. | No. Currently the account management policy in place is minimal and needs updating to protect the internal data. | High |
| Separation of Duties | Preventative.  Ensure no one person has excessive access that they can abuse system for personal gain. | No. There is no current policy in place to separate payroll from signed checks as CEO runs day to day operations, does payroll, and signs checks. | High |

**Technical Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Name** | **Type & Explanation** | **Implementation Currently Yes/No** | **Priority** |
| Firewall | Preventative.  Firewalls are already in place to filter malicious traffic from entering internal network. | Yes. Current firewall is adequate to block traffic based on a set of defined security rules. | NA |
| Intrusion Detection System | Detective.  Assist IT team to identify possible intrusions quickly. | No. The IT department needs an IDS system to identify threat actor intrusions. | High |
| Encryption | Deterrent.  Improves confidential information security. | No. There is no current encryption of internally stored data to ensure confidentiality of customers credit card information. | High |
| Backups | Corrective.  Supports productivity in the case of an event. Aligns with the disaster recovery plan. | No. The company does not have any backup in place for critical data in case of an event. | Medium |
| Password Management System | Corrective.  Password recovery, reset, and lockout notifications. | No. There is no centralized password management system in place to enforce the company’s password policy. This can affect productivity, as when an employee submits a ticket to the IT department to recover a password. I would recommend implementation of MFA also for extra security layer. | High |
| Antivirus Software | Corrective.  Detect and quarantine known threats. | Yes. There is antivirus software installed and monitored by the IT department. | NA |
| Manual Monitoring, Maintenance, and Intervention | Preventative & Corrective.  Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities. | No. There is a legacy system in place to monitor and maintain but no regular schedule and method in place for these interventions. | High |

**Physical Controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Control Name** | **Type & Explanation** | **Implementation Yes/No** | **Priority** |
| Closed-Circuit  Television (CCTV)  Surveillance | Preventative & detective.  Reduce risk of certain events and  can be used after event for  investigation. | Yes. Sufficient CCTV surveillance at the physical locations is adequate. | NA |
| Locks | Preventative.  Physical and digital assets are more secure. | Yes. The company’s physical location has adequate locks. | NA |
| 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 and hardware. | Yes. Sufficient and functioning fire detection and prevention system is in place. | NA |

**Payment Card Industry Data Security Standard (PCI DSS)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Best Practice** | **Explanation** | **Implementation Yes/No** | **Priority** |
| Build and Maintain a Secure Network. | Maintain a firewall and change default passwords and settings. | Yes & No. There is an adequate firewall protection in place, but password policy and implementation are inadequate. | High |
| Protect Cardholder Data. | Encryption of cardholder data during transit and at rest is needed to protect SPII/PII. | No. Credit card information is not encrypted, and all employees have access to SPII/PII. | High |
| Maintain a Vulnerability Management Program. | Use and regularly update anti-virus software. | Yes. The company has an adequate anti-virus software installed and monitored by IT department. | NA |
| Implement Strong Access Control Measures | Restriction of cardholder data to authorized users. User accounts should be assigned to real individuals and avoidance of shared accounts should be implemented. | No. All employees have access to the company’s internal data. | High |

**General Data Protection Regulation (GDPR)**

|  |  |  |  |
| --- | --- | --- | --- |
| **Best Practice** | **Explanation** | **Implementation Yes/No** | **Priority** |
| Data Minimization. | Only collect and process data that is necessary for the intended purpose. Data that is no longer necessary should be deleted. | No. No policy and implementation is in place to restrict only necessary data collection and to delete data once it is no longer necessary to keep. | High |
| Confidentiality to protect sensitive data. | No current encryption protocol is in place which would improve confidentiality of SPII/PII. | No. Credit card information is not encrypted, and all employees have access to SPII/PII. | High |
| Data Breach Reporting. | A data breach must be reported to authorities and individuals within 72 hours. | Yes. The company has a plan in place to notify E.U. customers in case of data breach. | NA |

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Best Practice** | **Explanation** | **Implementation Yes/No** | **Priority** |
| Processing Integrity | The company systems operate in a way as intended. | Yes. Integrity is in place to ensure complete, accurate, and validated data. | NA |
| Confidentiality | Protect confidential information by limiting who can access it, how it is stored, and how it is used. | No. The company does not have a current encryption tool to protect PII/SPII and the data is available to all employees without limitation of access. | High |
| Security. | Protect information from vulnerabilities and unauthorized access. | No. Controls of least privilege and separation of duties are not in place. | High |

Recommendations: Multiple controls need to be implemented to improve Botium Toys’ security posture. This includes the following: least privilege, disaster recovery plan and backup, access control policy, separation of duties, an IDS, improved legacy system monitoring and scheduling, encryption of SPII/PII, and improved password management system.

To address the gaps the following is most relevant to improve security posture.

* Implement the principle of least privilege across the company. Integration of Role-Based Access Control (RBAC) in which permissions are associated with specific roles and responsibilities.
* Develop a disaster recovery plan which outlines procedures for data recovery in the case of an event. Also, automate regular backups of important data.
* Establish an access control policy that defines who and under what circumstances can access data. Communicate the new strategy to all employees.
* Implement a separation of duty policy to prevent a single user from having excessive control.
* Deploy an intrusion detection system (IDS) which monitors network traffic and can alert the IT team to suspicious activities.
* Create a schedule for regular legacy system monitoring and updates to keep it secure and functioning.
* An encryption tool should be implemented to protect sensitive personal identifiable information and personally identifiable information during transit and at rest.
* Implement an improved password management system through policy updates, and higher-level password complexity and expiration. Encourage multi-factor authentication to provide an extra layer of protection.
* Conduct regular security training for all employees to improve best practice and encourage prompt reporting of suspicious activities.