**WORKSHEET**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **CONTROL NAME** | **CONTROL TYPE** | **CONTROL PURPOSE** | | Least Priviledge | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts | | Disaster recovery plans | Corrective | Provide business continuity | | Password policies | Preventative | Reduce likelihood of account compromise through brute force or dictonary attack techniques | | Access control policies | Preventative | Bolster confidentiality and integrity by defining which groups can access or modify data | | Account management policies | Preventative | Managing account lifecycle,reducing attack surface and limiting overall impact from disgruntled former employees and default account usage | | Seperation of duties | Preventative | Reduce risk and overall impact of malicious insider or compromised accounts |   **ADMINISTRATIVE/MANAGERIAL CONTROLS** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **CONTROL NAME** | **CONTROL TYPE** | **CONTROL PURPOSE** | | Firewall | Preventative | To filter unwanted or malicious traffic from entering the network | | IDS/IPS | Detective | To detect and prevent anomalous traffic that matches a signature or rule | | Encyrption | Deterrent | Provide confidentiality to sensitive information | | Backups | Corrective | Restore/recover from an event | | Password management | Preventative | Reduce password fatique | | Antivirus AV software  Manual monitoring, maintenance and intervention | Corrective  Preventative | Detect and quarantine known threats  Necessary to identify and manage threats, risks or vulnerabilities to out-of-date systems |   **TECHNICAL CONTROLS** |

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  | | --- | --- | --- | | **CONTROL NAME** | **CONTROL TYPE** | **CONTROL PURPOSE** | | Time-controlled safe | Detterent | Reduce attack surface and overall impact from physical threats | | Adequate lighting | Detterent | Deter threats by limiting “hiding” places | | Closed-circuit television (CCTV) | Preventative/Detective | CCTV is both a preventative and detective control because its prevence can reduce risk of certain events from occuring and can be used after an event to inform on event conditions | | Locking cabinets (for network gear) | Preventative | bolster integrity by preventing unauthorized personnel and other individuals from physically accessing or modifying network infrastructure gear | | Signage indicating alarm service provider | Deterrent | Deter certain types of threats by making the likelihood of a succesful attackseem low | | Fire detection and prevention  (fire alarm,sprinkler system etc)  Locks | Detective/Preventative  Detective/Preventative | detect fire in physcial location & prevent damage to physical assets like severs,inventory etc  Bolster integrity by deterring and preventing unauthorized personnel, individuals from physical accessing assets |   **PHYSICAL/OPERATIONAL CONTROLS** |

**CONTROLS AND COMPLIANCE CHECKLIST**

Controls Assessment Checklist

Does Botium Toys currenly have the following controls in place?

|  |  |  |
| --- | --- | --- |
| **YES** | **NO** | **CONTROL** |
|  | NO | Least Privilige |
|  | NO | Disaster recovery plan |
|  | NO | Password policies |
|  | NO | Seperation of duties |
| Yes |  | Firewall |
|  | NO | Intrusion detection system IDS |
| No |  | Backups |
| YES |  | Antivirus software |
| Yes |  | Manual montoring,maintenance and intervention for legacy systems |
|  | NO | Encyrption |
|  | NO | Password management system |

**Compliance Checklist**

Does Botium Toys currenly adhrere to this compliance best practice?

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

|  |  |  |
| --- | --- | --- |
| **Yes/ No** | **Best Practice** | **Explanation** |
| No | Authorized users can access to customer's credit card. | At the moment, all employees have access to it which is a bad practice in the business. |
| No | Credit card is stored in a secure environment. | It is not encrypted and violates the law and regulations. |
| No | Encryption is secured. | No, the encryption has not taken place yet. |

* **GDPR**

|  |  |  |
| --- | --- | --- |
| **Yes/ No** | **Best Practice** | **Explanation** |
| No | EU customers are kept secured. | The organization does not apply GDPR practice. Thus, it puts them at risk of being fined by the EU government. |
| Yes | Privacy policies are maintained properly. | According to the scenario, it has been enforced by the IT Team members and other staff. |

* **System and Organizations Controls**

|  |  |  |
| --- | --- | --- |
| **Yes/ No** | **Best Practice** | **Explanation** |
| No | User access policies are established | Employees have access to internally stored data which means the access policy has not been applied. |
| Yes | Data integrity is consistent, complete, accurate | Data integrity is in place. |
| No | Data is available to authorized users | Currently, all the employees can access all the data. |

**Recommendations**

After researching Botium Toys's security posture, the analysts agreed that the security practice is far from the expectation. It lacks of protection of confidentialiy of sensitive information. The following are:

* Least priviledge
* Disaster recovery plan
* Passoword policies
* Encryption
* Password management system

To address gaps in compliance, Botium needs to implement and establish the policies that can address the following above. Botium also needs to update its assets so the additional control can be identified as soon as possible to improve their security practice.