**Security Audit- Botium Toys**

Audit created: 06/09/23

Due to increasing pressure to support their online market worldwide, I was designated to conduct an internal security audit and review at Botium Toys. **The purpose of the audit was to assist the IT department in developing a strategy for managing security** to have a solidified plan of action and to ensure business continuity and compliance, as the business grows. In addition, this is also to achieve securing the company’s infrastructure and help them identify and mitigate potential risks, threats, or vulnerabilities to critical assets.

A summary of the recommendations made during the audit is detailed in Section B. The recommendations can be categorised as Administrative Controls, Technical Controls, and Physical Controls.

**Botium Toys’ internal IT audit assessed the following:**

● Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.

● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.

● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.

● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.

● Ensure current technology is accounted for. Both hardware and system access.

**The goals for Botium Toys’ internal IT 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 permissions when it comes to user credential management

● Establish their policies and procedures, which includes their playbooks

● Ensure they are meeting compliance requirements

**Critical Findings:**

**1.) Administrative controls**

* High Priority – Least Privilege, Disaster recovery plans, Account Management policies, Separation of duties.
* High/Medium - Password policies, Access control policies.

**2.) Technical controls**

* High Priority - Firewall, Intrusion Detection System (IDS), Encryption
* High/Medium - Backups, Password management system, Antivirus (AV) software.
* N/A - Manual monitoring, maintenance, and intervention

**3.) Physical controls**

* High Priority - Locks, Fire detection and prevention (fire alarm, sprinkler system, etc.)
* High/Medium - Time-controlled safe, Adequate lighting, Locking cabinets (for network gear)
* Low - Signage indicating alarm service provider
* N/A - Closed-circuit television (CCTV) surveillance

As listed above, all with high priority under each controls is categorised as **critical findings** that require immediate attention and prompt action. **Other findings** would be all stated as High/Medium and Low. **N/A** should not be ignored even though it is considered existinng but instead, this should be maintained according to recommendation and improve as needed. This is in line of what the organisation is aiming to adhere with the scope and goals mentioned in this security Audit.

**Summary/Recommendation**

As the organisations goal for this recommendation is to strengthen and assure stability of its security posture, there is a lot of improvement that has been sighted that needs to be actioned swiftly and execute some improvement the soonest time possible. Personally Identifiable Information (PII) or Sensitive Personally Identifiable Information (SPII) should be the outmost priority specially with financial dealings with online market.

As per compliance checklist, the three major regulation/controls should be implemented immediately as it would cost hefty fines and would ruin the organisation reputation wise if not done properly. This in mind, it is a priority to do regular review to those High and High/Medium controls that was listed in Section B. from time-to-time e.g., weekly or quarterly to ensure if all recommended information is up and running.

This can be reviewed by us upon request and providing us copies of what has been accomplished and will be updated as required. We also strongly advise that we conduct an online training/materials within the organisation to disseminate the information as quickly as possible so the recommendation would be implemented accordingly.