Stakeholder Memorandum

TO: IT Manager, stakeholders
FROM: Yeison Castillo
DATE: 6/21/2023

Internal IT Security Audit Findings and Recommendations

Dear Colleagues,

Please review the following information regarding the Botium Toys internal audit scope, goals, critical findings, summary and recommendations.

Scope:

- ➢ Ensure both hardware and system access are up-to-date with the latest technology.
- ➢ Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR compliance requirements.
- ➢ Systems in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. The systems will be evaluated for:
  - ○ Current user permissions
  - ○ Current implemented controls
  - ○ Current protocols and procedures

Goals:

- ➢ Adhere to the NIST CSF standards and regulations.
- ➢ Establish better processes for their systems to ensure they are compliant.
- ➢ Adapt to the concept of least privilege when it comes to user credential management.
- ➢ Establish their policies and procedures.

- Ensure they are meeting compliance requirements.

Critical findings (must be urgently addressed):

- Multiple controls need to be developed and implemented to meet the audit goals:
    - Password, access control, and account management policies, including the implementation of a password management system
    - IDS
    - Encryption (for secure website transactions)
    - Control of Least Privilege and Separation of Duties
    - Disaster recovery plans
    - Backups
    - CCTV
    - AV software
    - Locks
    - Manual monitoring, maintenance, and intervention for legacy systems

- Policies and procedures need to be developed and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies and procedures need to be developed and implemented to meet SOC type 1 and SOCtype 2 guidance related to user access policies and overall data safety.

Findings (should be addressed, but no immediately):

- The following controls should be implemented when possible:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets
    - Signage indicating alarm service provider

Summary/Recommendations:

To ensure compliance with PCI DSS and GDPR, it's important for Botium Toys to promptly address any critical findings. Since they accept online payments globally, including the EU, it's crucial to prioritize data security and privacy. Following SOC1 and SOC2 guidance will help establish user access policies and enhance overall data safety. Disaster recovery plans and backups are vital for business continuity in case of incidents. Integrating IDS and AV software will aid in identifying and mitigating potential risks, especially for legacy systems that require manual monitoring. Enhancing physical security through locks, CCTV, and proper asset monitoring is essential. Additionally, implementing encryption, time-controlled safes, adequate lighting, lockable cabinets, and signage indicating alarm services will further bolster Botium Toys' security measures.