Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Ben Zarichny
DATE: June 26th, 2023
SUBJECT: Internal IT 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:

- The following systems are in scope: accounting, end point detection, firewalls, intrusion detection system, SIEM tool. These systems will be evaluated for:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols
- Ensure that current user permissions, controls, procedures, and protocols align PCI DSS and GDPR compliance requirements.
- Ensure technology is accounted for both hardware and system access.

Goals:

- Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for ensuring current systems are compliant.
- Fortify system controls
- Implement the concept of least permissions for user credential management
- Establish policies and procedures, including playbooks
- Ensure Botium Toys is meeting compliance requirements

Critical findings (must be addressed immediately):

- The following controls need to be implemented to meet the audit goals:
    - Control of Least Privilege and Separation of Duties
    - Disaster recovery plans

    - Password, access control, and account management policies, including the implementation of a password management system
    - Encryption (for secure website transactions)
    - IDS
    - Backups
    - AV software
    - CCTV
    - Locks
    - Manual monitoring, maintenance, and intervention for legacy systems
    - Fire detection and prevention systems
- Policies need to be implemented to meet the following compliance requirements:
    - PCI DSS and GDPR compliance requirements
    - SOC1 and SOC2 guidance related to user access policies and overall data safety

Findings (should be addressed, but no immediate need):

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

Summary/Recommendations:

Since Botium Toys accepts online payments worldwide, including the EU, it is recommended that the critical findings relating to compliance with PCI DSS and GDPR be addressed immediately. Additionally, since one of the goals of the audit is to adapt to the concept of least permissions, SOC1 and SOC2 guidance related to user access policies and overall data safety should be used to develop appropriate policies and procedures. Having disaster recovery plans and backups is also critical because they support business continuity in the event of an incident. Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention. To further secure assets housed at Botium Toys' single physical location, locks and CCTV should be used to secure physical assets (including equipment) and to monitor and investigate potential threats. While not necessary immediately, using encryption and having a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating alarm service provider will further improve Botium Toys' security posture.