Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Jesse O’Connell
DATE: 6/29/2023
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:

- Assess current user permissions, controls, procedures, and protocols for the following systems: accounting, end point detection, firewalls, intrusion detection system, and Security Information and Event Management (SIEM) tool.
- Ensure user permissions, controls, procedures, and protocols in place align with compliance requirements (PCI DSS, GDPR).
- Ensure accountability of both hardware and software systems access.

Goals:

- Adhere to the National Institute of Standards and Technology Cybersecurity framework (NIST CSF).
- Adapt concept of least permissions.
- Comply with international regulation.
- Fortifying both administrative and technical system controls.
- Establishing policies and procedures, to include playbooks.

Critical findings (must be addressed immediately):

- Several controls must be implemented to reach audit goal to include the following:
    - Least Privilege
    - Disaster recovery plan
    - Password Policies
    - Access Control Policies

    - Account management policies
    - Separation of Duties
    - Intrusion Detection System (IDS)
    - Encryption
    - Back Ups
    - Password management system
    - Antivirus Software
    - CCTV Surveillance
    - Manual Monitoring, Maintenance, and intervention
    - Locks
    - Fire detection and prevention Systems
- Botium Toys must implement policies to be compliant with the GDPR and PCI DSS.
- Policies need to be developed and implemented to align with SOC 1 and SOC 2 regarding access policies and overall data safety.

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

- The following controls should be implemented:
    - Time-Controlled Safe
    - Adequate lighting
    - Locking Cabinets
    - Signage indicating alarm service provider

Summary/Recommendations: It is recommended that Botium Toys make immediate changes to be compliant with PCI DSS and the GDPR, as the company accepts online credit card payments to include those living in the E.U. Incident detection systems and antivirus software should be utilized to identify and quickly mitigate potential threats. Encryption software would be beneficial in upholding the integrity of sensitive information and ensuring only those authorized may view said information. SOC1 and SOC2 should be implemented to reach the concept goal of least permission. Additionally, disaster recovery plan policies should be put in place and include back ups of information. This will allow for business continuity in the event of an incident. Lastly, controls, such as cctv, locks, fire protection, etc., should be implemented to protect physical location and assets. A plan and timeline should be created to address lower priority controls. Although not immediately necessary, implementing a time controlled safe, adequate lighting, locking cabinets, and signage indicating the alarm service provider will show an aggressive security posture. These actions will work to deter and prevent threat actors from accessing private information.