Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Yazeed Alshehri
DATE: June 1, 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. The systems will be evaluated for:
    - Current user permissions
    - Current implemented controls
    - Current procedures and protocols
- Ensure current user permissions, controls, procedures, and protocols in place align with PCI DSS and GDPR compliance requirements.
- Ensure current technology is accounted for both hardware and system access.

Goals:

- Adhere to the NIST CSF.
- Establish a better process for their systems to ensure they are compliant.
- Fortify system controls.
- Adapt to 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 (must be addressed immediately):

- Multiple controls need to be developed and implemented to meet the audit goals, including:
    - 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 developed and implemented to meet PCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align to 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:

It is strongly recommended to promptly address critical findings related to compliance with PCI DSS and GDPR, given that Botium Toys accepts online payments from customers worldwide, including the E.U. Furthermore, as one of the audit goals is to implement the concept of least permissions, it is highly recommended to leverage SOC1 and SOC2 guidance for the development of appropriate policies and procedures regarding user access policies and overall data safety. The establishment of disaster recovery plans and regular backups is of utmost importance as they significantly contribute to business continuity during unforeseen incidents. Integrating an intrusion detection system (IDS) and antivirus (AV) software into the existing systems is highly recommended to enhance risk identification and mitigation, particularly for the manual monitoring and intervention required by legacy systems. To reinforce the security of physical assets at Botium Toys' location, it is strongly recommended to utilize locks, closed-circuit television (CCTV), and implement additional measures such as encryption, a time-controlled safe, adequate lighting, locking cabinets for equipment, fire detection and prevention systems, as well as signage indicating alarm service provider. While not immediately necessary, these recommended measures will further bolster Botium Toys' overall security posture.