Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Ricardo Duran
DATE: 17/07/24
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 included: accounting, endpoint detection, firewall,
- intrusion detection system, SIEM tool. Systems will be evaluated for:
    - Current user permissions
    - Current controls
    - Current procedures and protocols
- Ensure that 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:

- Comply with the National Institute of Standards and Technology (NIST) Cybersecurity Framework.
- Establish a more effective process to ensure systems compliance.
- Strengthen system controls.
- Implement the principle of least privilege in the management of user credentials or identification cards.
- Establish clear policies and procedures, including playbooks.
- Ensure compliance with regulatory compliance requirements.

Critical findings (must be addressed immediately):

- Multiple controls need to be developed and implemented to meet the objectives, including:
    - Least privilege control 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 web site transactions)
    - IDS
    - Backups
    - Antivirus software
    - CCTV
    - Locks
    - Manual monitoring, maintenance and intervention for legacy systems
    - Fire detection and prevention systems
- Policies need to be developed and implemented to meetPCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented to align with SOC1 and SOC2 guidelines related to user access policies and general data security.

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

- Whenever possible, the following controls should be applied:
    - Time-controlled security
    - Adequate lighting
    - Lockable cabinets
    - Signage indicated by the alarm service provider

Summary/Recommendations:

It is recommended that critical findings related to PCI DSS and GDPR compliance be addressed promptly, as Botium Toys accepts online payments from customers around the world, including the EU. In addition, since one of the objectives of the audit is to adapt to the concept of minimum permissions, SOC1 and SOC2 guidance related to user access policies and general data security should be used to develop appropriate policies and procedures.

Having disaster recovery and backup plans in place is also critical because they support business continuity in the event of an incident.

Integrating IDS and anti-virus software into current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, as current legacy systems require manual monitoring and intervention.

For assets housed at Botium Toys' single physical location, locks should be used to protect physical assets (including equipment) and to monitor and investigate potential threats.

Although not immediately necessary, the use of encryption and a time-controlled safe, adequate lighting, lockable cabinets, fire detection and prevention systems, and signage as directed by the alarm service provider will further enhance Botium Toys' security posture.