Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Mario David Hernández Pantoja
DATE: 04/29/2024
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 recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. 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.

Sincerely,
Mario David Hernández Pantoja