Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Brent Zitsman
DATE: May 22, 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 established 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 general 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: Botium Toys, an international online retailer accepting payments from customers worldwide, including the E.U., is advised to promptly address critical compliance issues regarding PCI DSS and GDPR. The audit emphasizes adopting the principle of least permissions, and it is recommended to incorporate SOC1 and SOC2 guidelines to develop appropriate user access policies and ensure overall data safety. Disaster recovery plans and backups are crucial for ensuring business continuity during potential incidents. Enhancing the existing systems with Intrusion Detection Systems (IDS) and antivirus (AV) software will bolster risk identification, mitigation, and intrusion detection capabilities, alleviating the need for manual monitoring and intervention in legacy systems. Strengthening physical asset

security at Botium Toys' single location is essential, and measures such as using locks and closed-circuit television (CCTV) for monitoring and investigating potential threats are recommended. While not immediately necessary, additional security measures like encryption, time-controlled safes, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating alarm service providers will further enhance Botium Toys' overall security posture.