Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Siraj A-Shahid
DATE: 6/11/23
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: Assessing the entire security program at Botium Toys.

- 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: The goals for Botium Toys' internal IT audit are:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for their systems to ensure they are compliant
- Fortify system controls
- Implement 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)
During the controls assessment these items were found to be the most critical:
Updates to Administrative Controls

- Updating the accessibility privileges for employees and vendors to ensure they have the least privilege necessary to fulfill their roles.
- Implementing a disaster recovery plan.
- Updating password and access control policies to strengthen security and prevent the likelihood of account compromise (consider updating account management policies as well).

Updates to Technical Controls

- Implementing an Intrusion detection system (IDS) to allow IT team to detect and identify possible intrusions.
- Adding a strong form of Antivirus to assist in detecting and quarantining threats.

Updates to Physical Controls

- Adding a CCTV surveillance system to help deter and investigate events.
- Consider locking cabinets for network gear/equipment.

During the compliance checklist these items were found to be the most critical:
Policies need to be implemented to more closely align with certain standards and regulations. Most importantly being the General Data Protection Regulation (GDPR) and Payment Card Industry Data Security Standard (PCI DSS).

It is also strongly recommended to implement System and Organization Controls (SOC1 & 2) related to user access policies and overall data safety.

Findings (should be addressed, but no immediate need):
During the controls assessment these items were found to be in need:

- Consider updating separation of duty policies to ensure no one has an inordinate amount of access - **Medium Urgency.**
- Consider encrypting data to improve confidentiality and security - **Medium Urgency.**
- Consider creating backups for important data - **Medium Urgency.**
- Consider implementing a password management system in case of lockouts, resets, etc.

- Consider adding/increasing manual monitoring and maintenance for legacy systems.
- Consider adding locks for physical and digital assets.
- Consider a fire detection system to minimize loss in case of fire.

Summary/Recommendations: As a result of this audit it is highly recommended that actions be taken asap to implement the critical findings listed above as well as more closely aligning to the standards and regulations laid out. Compliance with PCI DSS and GDPR should 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.

This will greatly increase the security and reduce the risk of a breach or other security threats should they arise. It will also help the company avoid any fines or lost points if an external audit were to be conducted.