Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Jacob King
DATE: 05/20/2023
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:
Botium Toys internal IT audit will assess the following:

- Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
- Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event
- Management (SIEM) tool.
- Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
- Ensure current user permissions, controls, procedures, and protocols in place align with necessary 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 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 immediately addressed):
A list of security implementations to meet audit goals:

- Controls of Least Privilege and Separation of duties.
- Disaster Recovery Plans
- Password, Access Control, and Account Management policies
- Password Management System
- Intrusion Detection System (IDS)
- Data Backups
- Antivirus (AV) Software
- Manual Monitoring, Maintenance, and Intervention for legacy systems
- Physical Locks
- Transaction Encryption
- CCTV
- Fire Detection and Prevention

Development of policies to meet business/data-security standards and regulations (PCI DSS, GDPR, SOC1, and SOC2)

Findings (Should be addressed but no immediate need):

- Time-Controlled Safe
- Adequate Lighting
- Locking Cabinets (for network equipment)
- Signage Indicating Security System

Summary/Recommendations:

We find that Botium Toys' current security measures may be inadequate to secure company assets and may not be within relevant security regulations and standards. We recommend the implementation of several changes to the business' regular security controls as well as major changes to the overall security framework ASAP. This includes administrative, technical, and physical safeguards to ensure the security of company assets and customer information's safety. It is highly recommended that critical findings relating to compliance with PCI DSS and GDPR be immediately addressed due to the company's use of online transactions worldwide (including the E.U.).

Following guidelines listed in SOC1 and SOC2, related to user access policies and overall data security should be used to develop appropriate policies and procedures, such as the concepts of ‘least permission’ and ‘separation of duties’. The implementation of IDS and AV software should be immediately used to identify and mitigate potential risks toward user and company data. This will assist Botium Toys’ security greatly as legacy systems require manual monitoring and intervention.

The use of security tools should immediately be installed to ensure the safety of Botium Toys’ physical location/assets. The addition of CCTV monitoring, fire detection and prevention, time-controlled safe, and physical locks on both entry points and equipment storage is recommended immediately. It is also recommended to install preventative security measures, such as better lighting in and around physical location as well as signage indicating the use of security alarms. If followed and swiftly acted upon, these recommendations will greatly improve Botium Toys’ security posture.