Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: (Sakshi pralhad gajanan jagtap), Cheif Internal Security Auditor
DATE: (5 Aug 2023)
SUBJECT: Internal IT Audit Findings and Recommendations

Dear Colleagues,
I am sharing the findings of the recent internal IT audit conducted at Botium Toys. This audit aimed to assess the effectiveness of our existing controls and identify areas for improvement to ensure the security and protection of our assets and data.

Scope:

- The following things are in scope :
    - Accounting
    - Endpoint
    - Detection
    - Firewalls
    - intrusion detection system
    - Security Information and Event Management (SIEM) Tool.

- The system will evaluate for
    - Current user permissions set
    - Current implemented controls
    - Current procedure and protocols set.

- 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 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 include their playbooks
- Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

- Least Privilege Preventative and Separation of Duties
- Disaster recovery plans Corrective
- Password policies and Password management system
- Encryption
- Access control policies
- Intrusion Detection System (IDS)
- Backups
- Antivirus (AV) software
- Manual monitoring, maintenance, and intervention
- Locks
- Account management policies
- Closed-circuit television (CCTV) surveillance
- 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):

- Time-controlled safe
- Adequate lighting
- Firewall
- Locking cabinets (for network gear)
- Signage indicating the alarm service provider
- Fire detection and prevention (fire alarm, sprinkler system, etc.)

Summary/Recommendations:

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 are also critical because they support business continuity in the event of an incident. Integrating 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 providers will further improve Botium Toys' security posture.