Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Nehemiah Chandler
DATE: 8/15/23
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:

- 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 advised that critical issues concerning compliance with PCI DSS and GDPR be promptly addressed due to Botium Toys' acceptance of online payments from a global customer base, including the E.U. Furthermore, aligning with the principle of least permissions, incorporating SOC1 and SOC2 guidelines for user access policies and overall data security is recommended to formulate suitable policies and procedures.
Establishing disaster recovery plans and maintaining backups is of paramount importance, as they ensure business continuity in case of unforeseen incidents. To enhance risk management, integrating an Intrusion Detection System (IDS) and Anti-Virus (AV) software into the existing systems is vital, aiding in identifying and mitigating potential threats. This is particularly crucial given that manual monitoring and intervention are required for existing legacy systems.

For bolstering the security of assets housed at Botium Toys' single physical location, implementing measures such as locks and Closed-Circuit Television (CCTV) surveillance can effectively safeguard physical assets, including equipment, and enable active monitoring for potential threats. While immediate implementation might not be necessary, incorporating encryption, a time-controlled safe, adequate lighting, secure locking cabinets, fire detection and prevention systems, as well as displaying signage indicating the alarm service provider, can further enhance the overall security stance of Botium Toys.