Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Willie Conway
DATE: May 13, 2023
SUBJECT: Internal IT audit findings and recommendations

Dear Colleagues,

Please evaluate the following details regarding the scope, objectives, key findings, summary, and recommendations of the internal audit conducted at Botium Toys.

Scope:

- The following systems are in scope: accounting, endpoint detection, firewalls, intrusion detection system, and SIEM tool. The systems will be evaluated for:
  - Current user permissions
  - Current implemented controls
  - Current procedures and protocols
- Verify that the user permissions, controls, workflows, and protocols currently in use comply with PCI DSS and GDPR compliance standards.
- Make careful to take into account current hardware and system access technology.

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 include their playbooks.
- Ensure they are meeting compliance requirements.

Critical findings (must be addressed immediately):

- To achieve the audit's objectives, numerous controls must be created and executed, 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
- To achieve the criteria of PCI DSS and GDPR compliance, policies must be created and put into place.
- To align with SOC1 and SOC2 recommendations regarding user access policies and overall data safety, policies must be designed and put into place.

Findings (should be addressed, but no immediate need):

- When practical, the following controls should be used.:
    - Time-controlled safe
    - Adequate lighting
    - Locking cabinets
    - Signage indicating alarm service provider

Summary/Recommendations: Given that Botium Toys accepts online payments from clients all over the world, including those in the EU, it is advised that serious concerns about compliance with PCI DSS and GDPR be addressed right away. Additionally, SOC1 and SOC2 recommendations about user access policies and overall data safety should be used to build suitable policies and processes, as one of the audit's objectives is to adapt to the notion of least permissions. It is also crucial to have backups and disaster recovery plans since they assist business continuity in the case of an occurrence. Since the current old systems need manual monitoring and intervention, integrating IDS and AV software will boost our ability to recognize and reduce potential hazards and could assist with intrusion detection. Locks and CCTV should be employed to secure physical assets (including equipment) as well as to monitor and investigate any threats in order to better secure assets located within Botium Toys' single physical location. Encryption, a time-controlled safe, proper lighting, locking cabinets, fire detection and prevention systems, and signage identifying the alarm service provider will all help to further strengthen Botium Toys' security posture, albeit they are not immediately necessary.