William Castro

Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: William Castro
DATE: 06/11/2023
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:

- 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:

Being a global online payment processor that serves clients from all over the world, including the E.U., Botium Toys should act quickly to address PCI DSS and GDPR compliance issues. This ensures adherence to relevant regulations. Additionally, it is important to employ SOC1 and SOC2 guidance for creating suitable policies and procedures for user access regulations and overall data protection to adopt the principle of least permissions. Plans for backups and disaster recovery are crucial for ensuring business continuity in the event of an unanticipated disasters. It is also advised to incorporate antivirus (AV) software and an intrusion detection system (IDS)

into the current systems. Given the manual monitoring and intervention that the existing legacy systems demand, this integration will improve risk identification and mitigation capabilities.

Botium Toys should also think about employing locks, closed-circuit television (CCTV), and conducting investigations when necessary to improve the protection of physical assets and to keep an eye on potential dangers. Even though they are not immediately necessary, adding extra security precautions like encryption, time-controlled safes, adequate lighting, locking cabinets, fire detection and prevention systems, and signage identifying the alarm service provider will improve Botium Toys' overall security posture.