Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Tanner Adler
DATE: 10/24/2024
SUBJECT: Botium Toys Internal Audit Findings and Recommendations

Dear Stakeholders,

Please review the following information regarding the internal audit of Botium Toys, including the scope, goals, critical findings, summary, and recommendations.

Scope:
The following systems are in scope for this audit: accounting, end point detection, firewalls, intrusion detection system, and security information and event management (SIEM) tool. These systems will be evaluated for:

- Current user permissions
- Current implemented controls
- Current procedures and protocols
- Compliance with GDPR, PCI DSS, and other compliance requirements
- Ensuring current technology and assets are 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
- Implement the concept of least permissions when it comes to user credential management
- Establish their policies and procedures, which includes their playbooks

Critical Findings (must be addressed immediately):
- Multiple controls need to be developed and implemented to meet the audit goals, including:
    - Principle of Least Privilege and Separation of duties
    - Disaster recovery plans
    - Password, Access control, and Account management policies
    - Intrusion Detection System (IDS)
    - Encryption (secure website transactions and disk drive(s) containing sensitive information)
    - Backups
    - Implementation of a Password management system
    - Antivirus (AV) software
    - Manual monitoring, maintenance, and intervention for legacy systems
    - Closed-circuit television (CCTV) surveillance
    - Locks
    - Locking cabinets (for network gear)
    - Fire detection and prevention (fire alarm, sprinkler system, etc.)
      To meet PCI DSS and GDPR compliance requirements.
- Policies need to be developed and implemented for the following:
    - To meet PCI DSS and GDPR compliance requirements.
    - To meet SOC1 and SOC2 guidance related to user access policies and overall data safety.

Summary/Recommendations:

- It is recommended that the critical findings relating to compliance with PCI DSS and GDPR be promptly addressed as Botium Toys accepts online payments and is expanding to offer services and handle the data of customers abroad, including the European Union.
- SOC1 and SOC2 guidance related to user access policies should be used to align to the audit goal to adapt to the concept of least permissions to develop the policies and procedures needed to be compliant.
- Disaster recovery plans and backups are recommended as they will support business continuity in the event of an incident occurring, ranging from a physical disaster such as a fire, or worse case scenario of a cyber attack or technical issue impacting business productivity as a part of a data and system resilience strategy.
- A method of fire detection and prevention systems is worth consideration for protecting against physical attacks.
- Integrating an IDS and AV software into current systems will give the ability to assist with intrusion detection and spot and mitigate potential risks while taking into account the existing legacy systems that need manual monitoring and intervention.
- To secure assets at Botium Toys' physical location, locks and CCTV should be used to secure physical assets and to monitor for potential threats. Having a time-controlled safe, adequate lighting, and signage indicating alarm service provider will further improve Botium Toys' security posture.

Thank you for your attention to this matter. Please let me know if you have any questions or concerns.