Stakeholder memorandum

TO: IT Manager, stakeholders
FROM: Abdullah Hassan
DATE: July 5, 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: In light of Botium Toys' acceptance of online payments from customers worldwide, including the E.U., it is crucial that we promptly address critical findings related to compliance with PCI DSS and GDPR. These measures will help ensure the security of customer data and maintain regulatory compliance.

To align with the concept of least permissions, we recommend leveraging SOC1 and SOC2 guidance to develop robust user access policies and enhance overall data safety. It is essential to establish appropriate policies and procedures that limit access rights to authorized individuals only.

In order to support business continuity in the event of an incident, it is imperative that disaster recovery plans and backups be established. These measures will enable a quick recovery and minimize potential downtime.

To enhance our ability to identify and mitigate potential risks, we propose integrating an Intrusion Detection System (IDS) and Antivirus (AV) software into our current systems. The implementation of these tools will streamline the process of detecting intrusions and facilitate timely intervention, particularly in legacy systems that currently rely on manual monitoring.

To strengthen the security of physical assets housed at Botium Toys' single location, we recommend utilizing locks and closed-circuit television (CCTV) surveillance. These measures will enhance asset protection and enable effective monitoring and investigation of potential threats.

While not an immediate priority, additional security measures can further improve Botium Toys' security posture. Encryption should be considered for sensitive data, and implementing a time-controlled safe, adequate lighting, locking cabinets, fire detection, and prevention systems are all worthwhile steps. Visible signage indicating the alarm service provider will serve as a deterrent and raise awareness of security measures.

By addressing these recommendations, we can bolster the security of Botium Toys, protect customer data, and minimize the risk of potential breaches. Please review these suggestions and take the necessary steps to implement them accordingly.

If you have any questions or require further clarification, please do not hesitate to reach out.

Thank you for your attention to this matter.