Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Seth Martin
DATE: 7/23/2023
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

Recommendations for PCI DSS and GDPR Compliance

Botium Toys should promptly address the critical findings related to compliance with PCI DSS and GDPR. This is because Botium Toys accepts online payments from customers worldwide, including the European Union (EU).

PCI DSS Compliance

As part of its PCI DSS compliance efforts, Botium Toys should:

- Develop and implement user access policies that align with the concept of least permissions.
- Use SOC1 and SOC2 guidance to develop policies and procedures for data safety.
- Implement disaster recovery plans and backups to ensure business continuity.
- Integrate IDS and AV software into its current systems to identify and mitigate potential risks.
- Use locks and CCTV to secure physical assets at its single physical location.

GDPR Compliance

Botium Toys should also take the following steps to comply with the GDPR:

- Use encryption to protect personal data.
- Have a time-controlled safe for storing sensitive data.
- Provide adequate lighting in its physical location.
- Lock cabinets that contain sensitive data.
- Install fire detection and prevention systems.
- Display signage indicating the presence of an alarm service provider.
- By taking these steps, Botium Toys can improve its security posture and protect the sensitive data of its customers.

Here is a more detailed explanation of each recommendation:

- Develop and implement user access policies that align with the concept of least permissions. This means that users should only have access to the data and systems that they need to do their jobs. This will help to protect sensitive data from unauthorized access.
- Use SOC1 and SOC2 guidance to develop policies and procedures for data safety. SOC1 and SOC2 are frameworks that provide guidance on how to manage information security and financial reporting. By following these frameworks, Botium Toys can ensure that its data is safe and secure.
- Implement disaster recovery plans and backups to ensure business continuity. A disaster recovery plan is a document that outlines how a business will recover its operations in the event of a disaster. Backups are copies of important data that can be used to restore the data in the event of a disaster. By having a disaster recovery plan

and backups in place, Botium Toys can ensure that it can resume its operations quickly and efficiently in the event of a disaster.

- Integrate IDS and AV software into its current systems to identify and mitigate potential risks. IDS (intrusion detection system) and AV (anti-virus) software can help to identify and mitigate potential risks to Botium Toys' systems. IDS software can detect unauthorized access attempts, while AV software can detect and remove malware.
- Use locks and CCTV to secure physical assets at its single physical location. Locks and CCTV can help to deter and prevent theft of physical assets, such as computers and equipment. CCTV can also be used to monitor the physical location for potential threats.
- Use encryption to protect personal data. Encryption is a process of scrambling data so that it cannot be read by unauthorized individuals. Botium Toys should use encryption to protect personal data, such as credit card numbers and social security numbers.
- Have a time-controlled safe for storing sensitive data. A time-controlled safe is a safe that can only be opened during certain hours. This can help to prevent unauthorized access to sensitive data.
- Provide adequate lighting in its physical location. Adequate lighting can help to deter theft and vandalism.
- Lock cabinets that contain sensitive data. Locking cabinets that contain sensitive data can help to prevent unauthorized access.
- Install fire detection and prevention systems. Fire detection and prevention systems can help to protect Botium Toys' physical location from fire damage.
- Display signage indicating the presence of an alarm service provider. This signage can deter criminals from targeting Botium Toys' physical location.
- By following these recommendations, Botium Toys can improve its security posture and protect the sensitive data of its customers.