TO: IT Manager, Stakeholders
FROM: Moe Dastranj
DATE: 3rd of September 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 scope is defined as the entire security program at Botium Toys.
This means all internal and external assets need to be assessed and audited alongside internal processes and procedures.
Internal criteria include outlined policies, procedures, and best practices.
External criteria include regulatory compliance, laws, and federal regulations.

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.

Botium Toys internal IT audit will assess the following:
● Current user permissions set in the following systems: accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool.
● Current implemented controls in the following systems: accounting, end point detection, firewalls, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Current procedures and protocols set for the following systems: accounting, end point detection, firewall, intrusion detection system, Security Information and Event Management (SIEM) tool.
● Ensure current user permissions, controls, procedures, and protocols in place align with necessary compliance requirements.
● Ensure current technology is accounted for. Both hardware and system access.

Goals:
The goal of an audit is to ensure an organization's information technology (IT) practices are meeting industry and organizational standards. Expecting a report of the current security posture of the organization and recommendations for improving the security posture of the organization, as well as justification to hire additional cybersecurity personnel.

The goals for Botium Toys' internal IT audit are:
● To adhere to the National Institute of Standards and Technology Cybersecurity Framework (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
● Ensure they are meeting compliance requirements

Critical findings (must be addressed immediately):

Administrative	Controls 6 issues
Technical	Controls 6 issues
Physical	Controls 2 issues

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

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

Physical Controls 4 issues
The following controls should be implemented when possible:

- Time-controlled safe
- Adequate lighting
- Locking cabinets
- Signage indicating alarm service provider

Summary/Recommendations:

It is recommended that critical findings relating to compliance with PCI DSS and GDPR be promptly addressed since Botium Toys accepts online payments from customers worldwide, including the E.U. In order to obtain Confidentiality Integrity and Availability triad it is important to have the needed Point's controls implemented right-away.

The assessment identified needed preventive systems to be implemented to reduce risk with PII stored data that can be accessed by unauthorized personnel. Integrating an IDS and AV software into the current systems will support our ability to identify and mitigate potential risks, and could help with intrusion detection, since existing legacy systems require manual monitoring and intervention.
Furthermore it is recommended that a disaster recovery plan should be implemented which allows for business continuation during such event.

Staff members can play a huge roll by reducing risk by participating by creating stronger passwords and the use of 2FA. Access control points increase confidentiality and integrity of data. You can find all related notes to findings on the Controls assessment exemplar.

To further secure assets housed at Botium Toys' single physical location, locks and CCTV should be used to secure physical assets (including equipment) and to monitor and investigate potential threats. While not necessary immediately, using encryption and having a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating alarm service provider will further improve Botium Toys' security posture.

Botium Toys needs to adhere to GDPR because they conduct business and collect personal information from people worldwide, including the E.U.

Botium Toys needs to adhere to PCI DSS because they store, accept, process, and transmit credit card information in person and online.

Botium Toys needs to establish and enforce appropriate user access for internal and external (third-party vendor) personnel to mitigate risk and ensure data safety.