TO: IT Manager, Stakeholders

FROM: Cameron Magliozzi

DATE: 7/14/2023

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 of this security audit includes the evaluation of these systems: accounting, end point detection,firewalls, an intrusion detection system, and an SIEM tool. These systems will be assessed for: current user permissions, current implemented controls, and current procedures and protocols. To make sure that current user permissions, controls, procedures, and protocols that are in place align with PCI DSS and GDPR compliance requirements.

**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.
* Make sure that they are meeting compliance requirements.

**Critical findings (must be addressed immediately):** Many controls need to be made and implemented ASAP in order to meet the goals of this audit. This includes:

* IDS
* Locks
* CCTV
* Encryption
* Extensive password, access control, and account management policies. (password management system)
* Better manual monitoring and maintenance of taking care of/ updating legacy systems.
* AV software
* They need to have systems in place to properly react to catastrophes in the company and properly recover from said catastrophes
* Control of separation of duty and Least Privilege.
* Fire detection and prevention systems.
* Backups
* They also need to develop and implement policies to meet PCI DSS and GDPR

compliance requirements.

* As well as developing and implementing policies to align to SOC1 and SOC2

guidance related to user access policies and overall safety of data.

**Findings (should be addressed, but no immediate need):** These following controls need to be implemented in time but are not of the highest priority.

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

**Summary/Recommendations:** It is highly recommended that the critical findings relating to

compliance with PCI DSS and GDPR are addressed ASAP as Botium Toys is growing internationally and accepts online payments from clients worldwide, including the E.U. On top of that, user access policies need to be developed and implemented in order to align with the control of least permissions, as well as procedures needing to be put in place to help overall data safety and adhere to SOC1 and SOC2 guidelines. There were also no recovery plans in case of a disaster that would promise the protection of business continuity in case of a catastrophe. Digital assets that prepare the company for disasters big or small like IDS and AV need to be integrated as soon as possible in order to identify and mitigate risks and threat actors that could follow as well as helping with intrusion detections. These would help alleviate the workload of the manual monitoring of the legacy systems and automate some tasks to make security of these systems more efficient. When it comes to physical asset improvements, there needs to be more thorough implementation of CCTV and locks around the company HQ in order to protect sensitive hardware harboring extremely valuable data to the company as well as preventing future threats. As far as the findings go, although not needed immediately, these systems should be implemented in due time. These systems include signage indicating alarm service provider, adequate lighting, fire detection and prevention systems, time-controlled safes, and locking cabinets in order to help improve Botium Toys’ security posture further.