Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Matteo Arnetoli
DATE: 8/9/23
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 for the internal security audit is primarily, assessing current user permissions, controls, procedures, and protocols across varied company's systems (*accounting, end point detection, firewalls, intrusion detection system, security information and event management (SIEM) tool*) and ensuring that these align with necessary compliance requirements.
Additionally, we want to ensure that current technologies, both hardware and software, are accounted for.

Goals: The main goals of the internal security audit are the adherence of Botium Toys to NIFT CSF, which will help to establish a better process for the organization's systems as well as ensuring compliance to current laws and regulations.
A fundamental point is the strengthening of system controls, with the implementation of the concept of least permission when it comes to user credential management.
Finally, it is important to ensure that appropriate internal policies and procedures are in place, with a particular focus on playbooks.

Critical findings (*must be addressed immediately*): We have identified several high-risk priorities concerning mainly Administrative and Technical Controls. The following controls should be implemented with urgency:

- 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
- Fire detection and prevention systems

In addition, internal policies need to be developed and implemented to meet the following regulations:

- GDRP
- PCI DSS
- SOC1 and SOC2

Findings (*should be addressed, but no immediate need*): A series of medium to low-risk priorities have been identified during the audit. These are mainly related to the Physical Controls category. Although, they are not critical, they should be implemented soon:

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

Summary/Recommendations:

We recommend prioritizing the controls highlighted within the Critical Finding section of this document as a matter of urgency as they represent the most significant vulnerabilities for Botium Toys.

The application of the principles of Least Privilege and Separation of Duty will ensure that employees have only access to the assets and data that they need to be able to carry out their usual tasks. This is to prevent any sensitive data being compromised or any abuse of the system for personal gain.

We recommend the implementation of strong password policies, which would reduce the risk of breaches in case of brute force attacks. At the same time, access controls and account management policies are essential to reduce the attack surface as well as potential internal threats.

The creation of appropriate disaster recovery plans as well as having system backups will help business continuity and uninterrupted production in case of severe incidents.

Moreover, having IDS and AV softwares in place will help detect external intrusions and identifying and stopping known threats, such as malware.

Physical controls should also be considered to protect assets that are stored within Botium Toys' offices and factory, with priority given to CCTV cameras, fire detection systems and locks appropriately installed.

We highly recommend implementing policies and procedures for the handling of assets that are compliant with the most updated laws and regulations. Special attention should be given to conformity to GDRP, concerning the handling of data of customers and partners within the European Union; PCI DSS regarding the storing, accepting, processing, and transmission of credit card information; and SOC1 and SOC2.