TO: IT Manager, Stakeholders

FROM: Beneventi Dario  
DATE: 07/09/2023  
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:**

* 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:**

* 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):

* Controls that need to be developed and implemented to meet the audit goals

*Administrative Controls:*

1. Control of Least Privilege
2. Disaster Recovery Plans
3. Password, Access Control and Account management policies including password management system
4. Separation of Duties

*Technical Controls:*

1. Intrusion Detection System (IDS)
2. Encryption (for web transactions)
3. Backups
4. Antivirus (AV) Software
5. Manual Monitoring and Maintenance

*Physical Controls:*

1. Closed-Circuit Television (CCTV) Surveillance
2. Locks
3. Fire detection and prevention systems

* Development of policies and implementation to meet PCI DSS and GDPR compliance requirements.
* Development of policies and implementation to align to SOC1 and SOC2 guidance related to user access policies and data safety.

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

*Physical Controls:*

1. Time-Controlled Safe
2. Adequate Lighting
3. Locking Cabinets (for Network Gear)
4. Signage Indicating Alarm Service Provider

**Summary/Recommendations:**

To enhance cybersecurity and meet compliance requirements, prompt action is essential. Given Botium Toys' global online payment acceptance, addressing PCI DSS and GDPR compliance is paramount. These regulations demand robust data security and privacy measures for worldwide customers. Adapting to the "Least Privilege" concept aligns with audit goals and requires leveraging SOC1 and SOC2 guidance for user access policies and overall data safety. This approach ensures the principle of minimal user permissions is upheld.

Furthermore, implementing disaster recovery plans and regular backups is crucial for seamless business continuity during potential incidents. Integrating an Intrusion Detection System (IDS) and Antivirus (AV) software will enhance risk identification and mitigation, especially for legacy systems that necessitate manual monitoring and intervention. To bolster physical security at Botium Toys' single location, deploying locks and Closed-Circuit Television (CCTV) surveillance will secure physical assets and facilitate threat monitoring and investigations.

While not immediately imperative, considering encryption, a time-controlled safe, adequate lighting, locking cabinets, fire detection and prevention systems, and signage indicating an alarm service provider will provide further enhancements to Botium Toys' overall security posture.

In conclusion, addressing critical findings promptly, adhering to compliance requirements, and implementing recommended measures will significantly bolster Botium Toys' cybersecurity and overall safety measures.