Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Niteesh Deshmukh
DATE: 06/08/2023
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:

- **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):

- Least Privilege : Reduces risk by making sure vendors and non-authorized staff only have access to the assets/data they need to do their jobs
- Disaster Recovery Plans : Business continuity to ensure systems are able to run in the event of an incident/there is limited to no loss of productivity downtime/impact to system components, including: computer room environment, hardware, applications
- Access control policies : Increase confidentiality and integrity of data
- Separation of duties : Ensure no one has so much access that they can abuse the system for personal gain
- Password policies : Establish password strength rules to improve security/reduce likelihood of account compromise through brute force or dictionary attack techniques
- Intrusion Detection System : Allows IT team to identify possible intrusions (e.g., anomalous traffic) quickly
- Encryption : Makes confidential information/data more secure (e.g., website payment transactions)
- Antivirus Software : Detect and quarantine known threats
- Manual monitoring : Required for legacy systems to identify and mitigate potential threats, risks, and vulnerabilities
- Time-controlled safe : Reduce attack surface/impact of physical threats
- CCTV surveillance : Can reduce risk of certain events; can be used after event for investigation
- Locks : Physical and digital will be more secure
- Fire detection and prevention : Detect fire in the toy store's physical location to prevent damage to inventory, servers, etc.

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

- Account management policies : Reduce attack surface and limit overall impact from disgruntled/former employees
- Password Management System: password recovery, reset, lock out notifications
- Firewalls :
- Adequate Lighting: Limit "hiding" places to deter threats
- Locking Cabinets : Increase integrity by preventing unauthorized personnel/individuals from physically accessing/modifying network infrastructure gear

- Signage indicating alarm service provider : Makes the likelihood of a successful attack seem low

Summary/Recommendations:
It is important to adhere to the proper administrative controls and ensure they are in place followed by implementation of adequate technical controls. In the scenario of an attack or breach, impact should be minimal on the organization's business and assets, in order to accomplish this disaster recovery and backup plans must be in place to ensure the business continuity. The aforementioned critical findings must be addressed as soon as possible to ensure compliance with NIST CSF.