Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Jordan Davis
DATE: 12/08/2023
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: Botium Toys internal IT audit assessed 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:

- To adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF)
- Establish a better process for 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):

- Multiple controls are required to be implemented to meet the goals outlined:
  - Least privilege: Limit authorized access to only the data/assets that are needed so that users/vendors can still perform their duties
  - Disaster recovery plans: Ensure plans are in place so there is limited to no loss of productivity or impacts to the systems/hardware/connectivity/data in the event of an incident
  - Password policies: improve security and reduce the likelihood of account compromise through attacks
  - Access control policies: Increase confidentiality and integrity of data
  - Account management policies: reduce attack surface and limit overall impact from disgruntled/former employees
  - Separation of duties: split access across multiple employees to ensure no one has a level of access that it could be abused
  - Intrusion detection system (IDS): Ensure adequate IDS is in place to allow IT teams to identify possible intrusions quickly
  - Encryption: Make confidential information/data more secure
  - Backups: Backups are needed in the case of an event to support ongoing productivity, this aligns with the disaster recovery plan
  - Antivirus software: required to help detect and quarantine known threats.
  - Manual monitoring, maintenance and intervention:
  - Closed circuit television (CCTV) surveillance: necessary for on site premises to help reduce risk of certain events, also can be used after an event has occurred for investigation purposes
  - Locks: ensure locks are in place to protect physical and digital assets
- Policies need to be developed and implemented to meet both GDPR and PCI DSS compliance requirements

- Policies need to be developed and implemented to align to SOC1 and SOC2 guidance related to user access policies and overall data safety.

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

- These controls should be addressed when possible:
    - Password management system: needs to be implemented to effectively manage password recoveries/resets as well as lock out notifications
    - Time controlled safe: helps to reduce attack surface and reduce impact of physical events
    - Adequate lighting: low priority, well lit areas reduce and deter physical threats
    - Locking cabinets: lock away physical assets such as network gear, prevent unauthorized access or modifications from occurring
    - Signage: adequate and visible signage that indicates the alarm service provider to deter potential attacks by reducing apparent success likelihood.
    - Fire detection and prevention: installation and maintenance of appropriate fire detection/prevention equipment such as fire alarms, sprinkler systems etc

Summary/Recommendations:

It is recommended that the critical findings related to the compliance with GDPR and PCI DSS be addressed immediately, as Botium Toys conducts business with customers from the EU and accepts payments online from multiple countries. Also as one of the goals of the audit consists of adapting to the process of least permissions SOC1 & SOC2 guidelines should also be used to develop appropriate policies and procedures. Having disaster recovery plans and backups is also critical in ensuring business continuity in the event of an incident. Integrating IDS and AV software will support our ability to identify and mitigate potential risks, and could help with intrusion detection especially since existing legacy systems require manual monitoring and intervention. To help secure assets housed at Botiums physical location, CCTV and locks should be installed to help keep the location secure. 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.