Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Christopher Myers
DATE: 07/04/2023
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 implement controls in the following systems. Current procedures and protocols set for the following systems. 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. 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): What requires immediate remediation is the administrative and technical controls. Also new compliance regulations and standards must be implemented due to the expansion of sales internationally.

Findings (should be addressed, but no immediate need): The physical controls need to be addressed in the future. It's not an immediate need.

Summary/Recommendations: The scope of the cybersecurity audit covered user permissions in the accounting, end point detection, firewalls, intrusion detection system, and security information and event management (SIEM) tool systems. The audit assessed the current implementation of controls and procedures in these systems. The primary goal was to ensure

that user permissions, controls, procedures, and protocols align with necessary compliance requirements. The audit also aimed to account for current technology, including both hardware and system access. To adhere to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, a better process was established to ensure compliance and fortify system controls. The concept of least permissions for user credential management was emphasized for enhanced security. The organization's policies and procedures, including playbooks, were established and reviewed for compliance. Critical findings that require immediate attention include the remediation of administrative and technical controls, as well as the implementation of new compliance regulations and standards for international sales expansion. Findings regarding physical controls were identified as an area for future attention, without an immediate need for remediation. Overall, the audit aimed to strengthen the organization's cybersecurity posture and ensure compliance with applicable regulations and standards.