TO: IT Manager, Stakeholders
FROM: Cristo Plata-Castro
DATE: 07/24/2023
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: The security audit for Botium Toys' internal IT will encompass a comprehensive assessment of user permissions, implemented controls, and established procedures and protocols in critical systems, including accounting, endpoint detection, firewalls, intrusion detection system, and Security Information and Event Management (SIEM) tool. The audit will also verify technology accountability, encompassing both hardware and system access, to ensure proper management and control.

Goals: The primary goals of the security audit are to adhere to the National Institute of Standards and Technology (NIST) Cybersecurity Framework, establish a more compliant process, strengthen system controls, implement the principle of least privilege for user credential management, establish policies and procedures, including playbooks, and ensure adherence to compliance requirements. The audit aims to enhance overall cybersecurity, protect sensitive data, and align the company's IT practices with industry standards and regulations, fostering a secure and compliant IT environment for Botium Toys.

Critical findings (must be addressed immediately): During the audit, critical findings revealed that Botium Toys had inadequate Administrative controls, leaving sensitive data vulnerable to unauthorized access. Additionally, the company lacked essential security controls, such as encryption and monitoring, which increased the risk of data breaches and cyber-attacks. Furthermore, the absence of established policies and procedures, including playbooks, left the organization ill-prepared to handle security incidents effectively, necessitating immediate action to fortify their cybersecurity measures.

Findings (should be addressed, but no immediate need): Some other findings during the audit include inadequate lighting and other physical security controls. While these non-critical findings may not pose an immediate threat, addressing them would contribute to overall IT efficiency and strengthen the company's security posture in the long term.

Summary/Recommendations: The security audit for Botium Toys exposed critical vulnerabilities, including inadequate user permissions, insufficient security controls, and the absence of established policies. To fortify cybersecurity, the company should implement least privilege principles, deploy robust security controls, and develop comprehensive policies and procedures. Addressing these issues promptly will enhance data protection, ensure compliance, and mitigate potential risks, safeguarding the organization from cyber threats.