Stakeholder Memorandum

TO: IT Manager, Stakeholders
FROM: Michael Shanosky
DATE: May 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, and recommendations.

Scope:
The audit scope for Botium Toys encompassed a comprehensive assessment of the company's cybersecurity program. It included an evaluation of current user permissions, implemented controls, procedures and protocols across various systems such as accounting, endpoint detection, firewalls, intrusion detection system, and Security Information and Event Management (SIEM) tool. The audit also examined compliance requirements and the management of technology assets, including hardware and system access.

Goals:
The goals of the internal IT audit for Botium Toys were as follows:

- Adhere to the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF).
- Establish a better process for systems to ensure compliance.
- Fortify system controls.
- Implement the concept of least privilege for user credential management.
- Establish policies, procedures, and playbooks.
- Ensure compliance with relevant regulations and standards.

Critical Findings (must be addressed immediately):
Based on the audit findings, the following critical issues require immediate attention:

- Inadequate management of assets, including a lack of proper controls and compliance adherence, poses a high risk to Botium Toys.

- Insufficient access controls and user permissions, particularly in systems handling sensitive data, increase the likelihood of unauthorized access and potential data breaches.
- Lack of disaster recovery plans and limited backup mechanisms put the company at risk of significant downtime and potential loss of critical data in the event of an incident.

Findings (should be addressed, but no immediate need):
The audit also identified the following findings that should be addressed to improve the security posture of Botium Toys:

- Incomplete password policies that do not meet recommended strength requirements, increasing the risk of password-related attacks.
- Inadequate monitoring and maintenance of legacy systems, leaving them vulnerable to potential threats and vulnerabilities.
- The need for enhanced vendor access management processes to ensure secure access and minimize risks associated with third-party relationships.

Summary/Recommendations:
In summary, the internal IT audit of Botium Toys has revealed critical findings that require immediate attention to mitigate risks and strengthen the company's security posture. It is recommended that the following actions be taken:

- Develop and implement a comprehensive asset management program to ensure proper control, monitoring, and compliance with regulations and standards.
- Enhance access controls and user permissions across systems, implementing the principle of least privilege to minimize the risk of unauthorized access.
- Establish robust disaster recovery plans and implement regular data backups to ensure business continuity and protect critical data in the event of an incident.
- Strengthen password policies to enforce stronger password complexity and ensure regular password updates.
- Enhance monitoring and maintenance practices for legacy systems to address vulnerabilities and minimize potential risks.
- Improve vendor access management processes to ensure secure and controlled access to Botium Toys' systems and data.

Taking these recommended actions will significantly enhance the security posture of Botium Toys and align it with industry best practices and compliance requirements.

Please let me know if you have any questions or require further clarification on the audit findings and recommendations.

Thank you for your attention to this matter.

Sincerely,
Michael Shanosky