Botium Toys Memorandum

TO: IT Manager, stakeholders

FROM: Vicente Agricourt Jr  
DATE: September 25, 2024  
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 internal IT audit aimed to evaluate the information security measures and practices at Botium Toys. This audit included examining the company's information systems, as well as its policies and procedures concerning information security.

**Goals:** The audit aimed to pinpoint any gaps or flaws in Botium Toys' information security measures and offer suggestions to enhance the company's security stance.

**Critical Findings** (must be addressed immediately): During the audit, several critical findings were identified that require immediate attention. These findings include:

1. Weak password policies: The current password policies are inadequate for safeguarding the company's sensitive information from unauthorized access. It's essential to enhance and enforce the password complexity rules.
2. Unpatched software and systems: Botium Toys has several systems and software that haven't been updated with the latest patches, exposing the company to known security risks.
3. Lack of backups and disaster recovery plan: Botium Toys lacks a comprehensive backup and disaster recovery plan, which presents a major risk to its operations if a system failure or cyberattack occurs.

**Findings** (should be addressed, but no immediate need): The following findings were also identified during the audit, which should be addressed for overall improvement in the company's security posture:

1. Inadequate monitoring and logging of network activity.
2. Lack of security awareness training for employees.
3. Incomplete inventory of company assets and software licenses

**Summary/Recommendations:** To improve Botium Toys' overall security posture, we recommend the following actions be taken:

1. Implement regular backups and disaster recovery plan.
2. Strengthen password policies and enforce them.
3. Update and patch all systems and software.
4. Provide regular security awareness training for employees.
5. Complete inventory of company assets and software licenses.
6. Implement proper monitoring and logging of network activity.

Botium Toys should urgently address critical PCI DSS and GDPR compliance issues, as it processes online payments globally, including from the E.U. The audit aims to implement least privilege access, so SOC1 and SOC2 guidance on user access and data safety should inform policy development. Disaster recovery plans and backups are essential for business continuity. Integrating IDS and AV software will enhance risk detection and mitigation, especially since current legacy systems rely on manual monitoring. To secure physical assets, locks and CCTV are necessary, while further enhancements like encryption, time-controlled safes, and improved lighting can strengthen security over time.

Thank you for allowing us to conduct this audit and provide recommendations to enhance Botium Toys' information security. If you have any questions or concerns, feel free to reach out to us.

Sincerely,

Vicente Agricourt Jr