Stakeholder memorandum

TO: IT Manager, Stakeholders
FROM: Kasey Chang
DATE: June 1, 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: We are auditing user permissions, controls, and procedures+protocols for following systems: accounting, endpoint detection, firewall, IDS, and SIEM. We are also ensuring the existing user permissions, controls, and procedures+protocol are compliant with needed standards/legal requirements. Finally, we are also accounting for all hardware and system access.

Goals: We want to ensure we are compliant with NIST CSF and other legal compliance requirements. We want to make sure all systems have their respective playbook for policies and procedures. We will implement least permission, and improve system controls to ensure compliance.

Critical findings: We need to implement following playbooks (procedures) immediately in the following areas:

- Disaster recovery plan for business continuity (backups, power, server room, connectivity, applications, restore procedure)
- Audit and reduce all users to “least privilege” needed for company assets/data
- Audit and improve password policy to prevent brute-force or dictionary attacks against individual accounts to compromise data/assets
- Audit and identify duties to ensure all positions have controls in place to prevent single person having too much power
- Install and implement IDS
- Ensure website payment system is compliant with industry standards of encryption regarding credit card payments

- Install and implement full company wide antivirus for all connected devices
- Audit legacy systems still in use, evaluate potential of compromise, and how to monitor for such, as well as policies and procedures
- Audit / Implement locks and access control to prevent physical intrusions

Findings: these items can wait behind the critical findings

- Audit and eliminate ex-employee accounts to limit potential damage from disgruntled ex-employees.
- Encrypt data to make compromise more difficult
- Implement password management system to allow recovery, reset, lockout, and so on
- Time-controlled safe for physical security
- Appropriate lighting and CCTV cameras for proper logs, both store on-site and cloud backup
- Badge control and locks of network equipment such as server room and other networking gear, again, logs on-site and cloud backup
- Fire detection and prevention for both equipment and store inventory

Summary/Recommendations:

Company needs to revamp many procedures and policies ASAP, not only for legal and operational compliance, but to ensure business continuity (in case of disaster) as well as implement security measures to safeguard itself against both physical and online intrusions.